Краснодарский университет МВД России

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XIV Всероссийской научно-практической конференции
(15 июня 2018 г.)

Краснодар
2018

УДК 004, 51, 53
ББК 60.8
М34

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Редакционная коллегия:
И. Н. Старостенко, кандидат физико-математических наук, доцент
(председатель);
Е. В. Михайленко, кандидат физико-математических наук, доцент
(заместитель председателя);
А. К. Назаров, кандидат физико-математических наук;
А. А. Хромых, кандидат физико-математических наук.

М34 **Математические методы и информационно-технические средства** : материалы XIV Всерос. науч.-практ. конф., 15 июня 2018 г. / ред. кол. : И. Н. Старостенко, Е. В. Михайленко, А. К. Назаров, А. А. Хромых. – Краснодар : Краснодарский университет МВД России, 2018. – 344 с.

ISBN 978-5-9266-1370-1

В сборнике представлены материалы XIV Всероссийской научно-практической конференции, которая проводилась 15 июня 2018 г. в Краснодарском университете МВД России.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 004, 51, 53
ББК 60.8

ISBN 978-5-9266-1370-1

© Краснодарский университет
МВД России, 2018

Ажмухамедов И.М.
Астраханский государственный университет
Мачуева Д.А.
Грозненский государственный нефтяной технический университет имени акад. М.Д. Миллионщикова

МОДЕЛИРОВАНИЕ ПРОЦЕССА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СОЦИАЛЬНЫХ СИСТЕМАХ С ЦЕЛЬЮ ВЫРАБОТКИ МЕР ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ЭКСТРЕМИЗМУ

Экстремизм в различных формах проявления представляет серьезную угрозу жизнедеятельности и развитию современного общества. В широкой трактовке под экстремизмом понимают «приверженность к крайним, радикальным взглядам», и в настоящее время к экстремистской деятельности относят различные как по целевой направленности, так и по выбору средств противозаконные деяния, выделяя идеологический, националистический, гендерный, политический, религиозный, духовный, криминальный экстремизм [2].

К проявлениям экстремизма могут быть отнесены [4,6]:

– возбуждение социальной, расовой, национальной или религиозной розни и призывы к дискриминации людей по тому или иному признаку;

– осуществление массовых беспорядков, хулиганских действий и актов вандализма на основании ненависти и вражды в отношении какой-либо социальной группы;

– призывы к насилию и противоправной деятельности, основанные на психологии нетерпимости, предубеждений, предрассудков, этноцентризма, дискриминации, ксенофобии, национализма;

– унижение национального достоинства;

– усвоение радикальных религиозных воззрений, отрицание культурных, духовно-нравственных основ своей нации;

– пропаганда и публичное демонстрирование нацистской атрибутики или символики;

– осуществление террористической деятельности;

– финансирование или пропаганда террористической деятельности, либо иное содействие ее осуществлению;

– инспирирование протестной активности с намерением дестабилизации политической системы.

Можно отметить следующую тенденцию: все большее распространение наряду с актами открытой агрессии получают ненасильственные скрытые формы экстремизма, основанные на использовании современных средств коммуникации и доступа к информационным ресурсам. Вербальные формы экстремизма начинают превалировать над физическими [2]. Так называемый информационный экстремизм становится одной из наиболее острых проблем современного социума.

Прогресс информационно-коммуникационных технологий, повлиявший на процессы социального общения, обмена данными, образования и социализации личности, пополнил арсенал экстремистов такими средствами воздействия, как информационно-психологические диверсии, манипуляция сознанием, распространение слухов, подмена представлений и культурных ценностей. Современная технико-технологическая среда обладает значительным потенциалом влияния на сознание социальных групп путем организации и направления процессов массовой коммуникации.

Значительно способствуют распространению идей экстремизма следующие особенности Интернет-коммуникации [5,7,9]:

– резкое ухудшение качества информации;

– увеличение объемов ненужной человеку, «фоновой» информации, что приводит к разрушению барьеров восприятия вредоносной, антисоциальной информации;

– сложность для отдельного индивида или группы объективно оценить получаемые сведения;

– информационные «фантомы» – возможность распространения слухов в виртуальной среде;

– проблема Интернет-зависимости, особенно актуальная в молодежной среде.

Для выработки мер противодействия деструктивным информационным акциям экстремистов необходимо правильно представлять механизмы распространения информации. Исходя из этого, актуальной задачей является разработка алгоритмов и моделей, позволяющих исследовать закономерности информационного взаимодействия, проводить мониторинг «информационного фона» и прогнозировать настроения в обществе.

Математическая модель процесса информационного взаимодействия

Для моделирования процесса информационного взаимодействия (ПИВ) необходимо охарактеризовать социальную систему, в которой происходит обмен информацией. Социальная система (СС) – это сложноорганизованное упорядоченное целое, включающее отдельных индивидов и социальные общности, объединенные разнообразными связями и взаимоотношениями. Значимыми параметрами СС являются связность, коммуникабельность и восприимчивость ее элементов к внешним воздействиям [8].

Поскольку социальным системам имманентно присуща субъективная неопределенность, моделирование происходящих в них процессов превращается в слабо формализуемую проблему [1]. В качестве инструментария для анализа субъективных факторов целесообразно использовать аппарат теории нечетких множеств.

Так, для формализации субъективных данных предлагается определить лингвистическую переменную «Уровень фактора» и задать терм-множество ее значений из трех или пяти элементов:

{низкий; средний; высокий} (1)

{сильно отрицательный; отрицательный; нейтральный; положительный; сильно положительный} (2)

Процесс распространения информации проходит следующим образом. Любая информация вносится в СС в начальный момент времени t=0 некоторым конечным числом ее представителей (назовем их инициирующим множеством). Если информационное воздействие производится осознанно и целенаправленно, члены инициирующего множества, как правило, имеют или активно демонстрируют сильно выраженное положительное или отрицательное мнение относительно этой информации. Дальнейший межличностный информационный обмен обеспечивает доведение информации до сведения остальных участников коммуникации. Целью моделирования ПИВ является определение доли информированных членов СС, а также распределения мнений в терминах множества (2) на каждом шаге t=t+1.

Количество K информированных членов социальной системы на шаге t=t+1 представляет собой зависимость:

$$K_{(t+1)} = K_{(t+1)}\left(L, \bar{b}, q_t, K_{(t)}\right), \quad (3)$$

где L – объем инициирующего множества, $\bar{b}$ – коэффициент связности СС (усредненное количество связей между участниками взаимодействия в системе), q_t – доля участников на шаге t, готовых дальше распространять информацию (делать «репост»).

Значение коэффициента q_t зависит от двух факторов – доли участников с высоким уровнем общительности и актуальности распространяемой информации на временном шаге t. Уровень общительности является постоянным свойством членов СС, однако ак-

туальность информации со временем снижается. Исходя из этого, для определения q_t предложена следующая формула:

$$q_t = Com \cdot Act_t = Com \cdot Act_0 \cdot e^{-\alpha \cdot t / \tau_{act}}, \quad (4)$$

где *Com* – доля участников с высокой коммуникабельностью, Act_0 – начальное значение актуальности информации при t=0 (обычно принимается равным 1); α – коэффициент падения актуальности (согласно многочисленным исследованиям, α=2,3 [3]); τ_{act} – максимальное время сохранения актуальности информации (время ее жизненного цикла).

Исходные данные о количестве связей в системе, коммуникабельности, а также восприимчивости (или, напротив, консерватизме) ее членов для больших СС могут носить характер статистических распределений. То же относится и к имеющемуся начальному распределению мнений в системе по тематике распространяемой информации. Для получения этих данных рекомендуется метод репрезентативного социологического опроса на основе выборочной совокупности, позволяющий экстраполировать выводы на всю социальную систему.

Показатель «уровень восприимчивости» характеризует склонность человека менять свою точку зрения, ориентируясь на мнение окружающих. Значению «низкая восприимчивость» соответствует способность сохранять свое мнение под воздействием информационного фона, а значению «высокая» – значительная степень конформности.

Учитывая все сказанное, можно сформулировать правила информационного обмена и формирования мнений в СС, допускающие формализацию и автоматизацию математического расчета:

1. Делятся информацией только участники:

а) с высокой степенью коммуникабельности;

б) с сильно выраженным собственным отношением к этой информации (положительным или отрицательным);

2. Мнение участников с низкой восприимчивостью не меняется, тогда как участники со средней и высокой восприимчивостью, получая эмоционально окрашенные отзывы, меняют мнение.

3. Участники со средней восприимчивостью умеренно поддаются стороннему влиянию: переходят от нейтрального мнения – к положительному или отрицательному (или наоборот), от положительного или отрицательного – к сильно выраженному позитивному или негативному отношению, получая соответствующие отзывы.

4. Участники с высокой восприимчивостью легко поддаются давлению окружающих: их мнение «скачет» от отрицательного к положительному, от нейтрального к сильно положительному или отрицательному.

Введем следующие обозначения:

– $\omega^{\text{Н}}, \omega^{\text{С}}, \omega^{\text{В}}$ – доли членов СС с низкой, средней и высокой восприимчивостью;

– K_t^{++} и ν_t^{++} – соответственно количество и доля участников с сильно положительным отношением к обсуждаемой информации на момент времени t;

– K_t^{+} и ν_t^{+} – количество и доля участников с положительным мнением;

– $K_t^{\text{Н}}$ и $\nu_t^{\text{Н}}$ – количество и доля участников с нейтральным отношением;

– K_t^{-} и ν_t^{-} – участники с отрицательным мнением;

– K_t^{--} и ν_t^{--} – участники, у которых на момент t сложилось сильно отрицательное мнение.

Тогда количество информированных членов СС определяется по формуле:

$$K_{t+1} = K_t + q_t \cdot \left(\frac{N-K_t}{N}\right) \cdot (K_t^{++} + K_t^{--}) \cdot \bar{b}, \quad (5)$$

где N – общая численность СС, а коэффициент $\frac{N-K_t}{N}$ отражает долю остававшихся неинформированными участников на предыдущем шаге.

Количество участников с положительным мнением можно рассчитать следующим образом:

$$K_{t+1}^{+} = K_t^{+} + (K_{t+1} - K_t) \cdot [\nu_t^{+} - \nu_t^{+} \cdot (\omega^{\text{С}} + \omega^{\text{В}}) \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right) - \nu_t^{+} \cdot (\omega^{\text{С}} + \omega^{\text{В}}) \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}}\right) + \nu_t^{++} \cdot \omega^{\text{С}} \cdot \left(\frac{K^{--}}{K^{++} + K^{--}}\right) + \nu_t^{-} \cdot \omega^{\text{В}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right) + \cdot \nu_t^{\text{Н}} \cdot \omega^{\text{С}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right)] \quad (6)$$

Множители $\frac{K_t^{++}}{K_t^{++} + K_t^{--}}$ и $\frac{K_t^{--}}{K_t^{++} + K_t^{--}}$ отражают доли участников информационного обмена, делящихся сильно выраженным положительным и отрицательным мнением соответственно. По формуле можно видеть, как поддаются их влиянию и меняют мнение в ту или иную сторону (вычитаются или прибавляются) участники со средней и высокой восприимчивостью.

В свою очередь, количество членов СС с сильно позитивным отношением к распространяемой информации вычисляется так:

$$K_{t+1}^{++} = K_t^{++} + (K_{t+1} - K_t) \cdot [\nu_t^{++} - \nu_t^{++} \cdot (\omega^{\text{С}} + \omega^{\text{В}}) \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}}\right) + \nu_t^{+} \cdot (\omega^{\text{С}} + \omega^{\text{В}}) \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right) + \nu_t^{\text{Н}} \cdot \omega^{\text{В}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right)] \quad (7)$$

Количество нейтрально настроенных участников:

$$K_{t+1}^{\text{Н}} = K_t^{\text{Н}} + (K_{t+1} - K_t) \cdot [\nu_t^{\text{Н}} - \nu_t^{\text{Н}} \cdot (\omega^{\text{С}} + \omega^{\text{В}}) + \nu_t^{-} \cdot \omega^{\text{С}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right) + + \nu_t^{+} \cdot \omega^{\text{С}} \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}}\right) + \nu_t^{++} \cdot \omega^{\text{В}} \cdot \left(\frac{K_t^{--}}{K_t^{++} + K_t^{--}}\right) + \nu_t^{--} \cdot \omega^{\text{В}} \cdot \left(\frac{K_t^{++}}{K_t^{++} + K_t^{--}}\right) \quad (8)$$

Количество участников СС с отрицательным и сильно отрицательным мнением определяется аналогично.

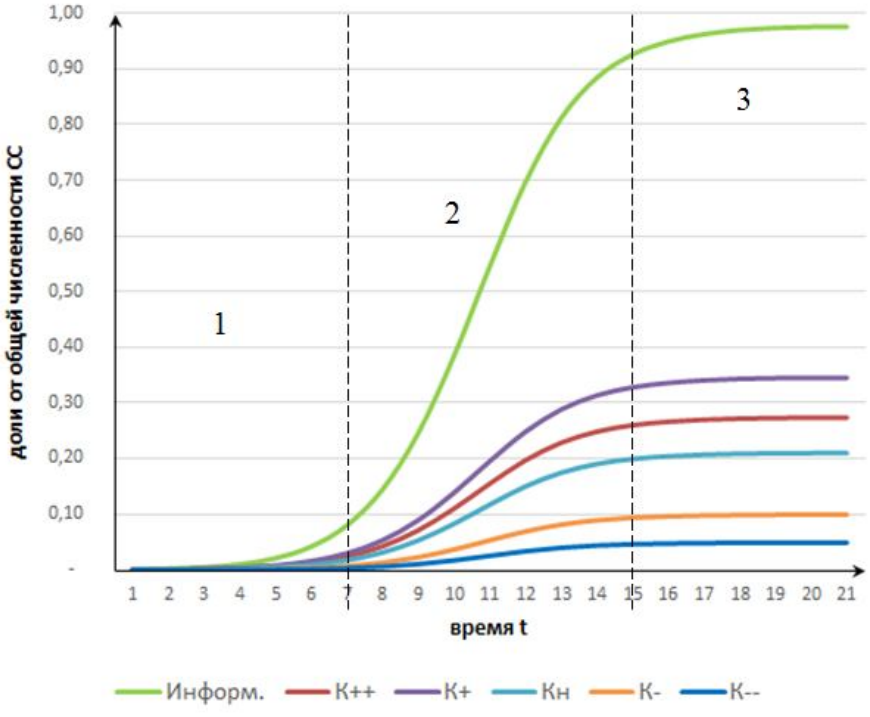


Рис. 1. Графики нарастания количества информированных участников и распределения их мнений

Расчетный пример

Для выявления закономерностей ПИВ приведем пример социальной системы объемом 10 млн человек, характеризуемой следующими показателями:

а) количество связей: от 1 до 5 – у 82% участников, от 6 до 30 – 17%, свыше 30 и менее 100 – 1%; среднее число контактов на одного человека – 6,2;

б) восприимчивость: $\omega^{\mathrm{H}} = 0{,}2, \omega^{\mathrm{C}} = 0{,}55, \omega^{\mathrm{B}} = 0{,}25$;

в) начальное отношение к исследуемой тематике: $\nu_0^{++} = \nu_0^{--} = 0{,}05$, $\nu_0^{+} = \nu_0^{-} = 0{,}15$, $\nu_0^{\mathrm{H}} = 0{,}6$ (преимущественно нейтральная равновесная среда);

г) готовность распространять полученную информацию: $q_0 = 0{,}4$.

Информационный блок «внедряется» в систему через инициирующее множество объемом 0,01% от генеральной совокупности (1000 человек с сильно положительным отношением к информации).

Динамика процесса информационного взаимодействия показана на рисунке 1. Графики имеют форму сигмоиды, что позволяет условно выделить три стадии ПИВ. На первом этапе количество информированных членов СС нарастает медленно. Затем с определенного момента начинается резкий лавинообразный рост количества получивших информацию участников. Процесс замедляется и переходит в третью стадию, когда дальнейшая передача информации практически прекращается. Важно отметить, что полная информированность СС не достигается. Обмен мнениями между участниками может продолжаться еще некоторое время, однако установившийся баланс мнений заметно не меняется.

Практическая ценность модели заключается в возможности прогнозировать развитие ситуации и предсказывать реакцию общества при проведении различных информационных акций (в том числе деструктивных), а также, что более важно, рассматривать возможности и последствия целевого вмешательства в процесс распространения информации с целью управленческого воздействия.

Например, уменьшение показателя q_0 до 0,35 заметно снижает общую информированность членов социальной системы, хотя и не оказывает влияния на относительное распределение их мнений (рис. 2).

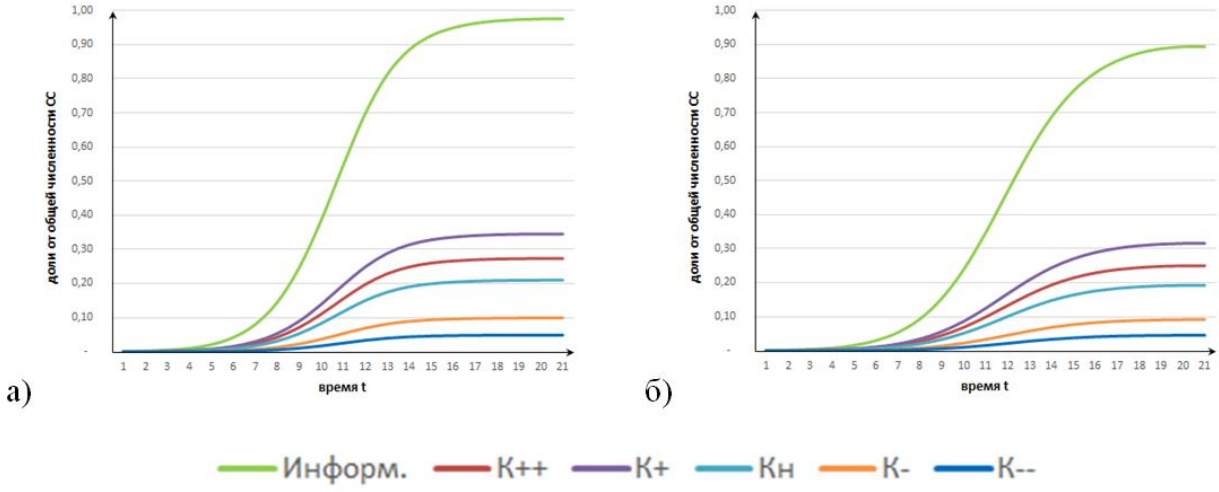


Рис. 2. Графики ПИВ: а) при q_0=0,4; б) при q_0=0,35

Уменьшение восприимчивости СС к информационному фону приводит как к снижению информированности, так и к изменению соотношения мнений участников относительно полученной информации (графики количества нейтральных и сильно положительных мнений на рис. 3).

Можно, например, предложить следующие направления воздействия на социальную систему с целью изменения ее параметров:

1. Дискредитация источника распространяемой деструктивной информации, что повлечет уменьшение доверия и восприимчивости к ней;

2. Инициирование и запуск другого информационного блока, обсуждение которого отвлечет участников коммуникации от изначально деструктивной информации, снижая ее актуальность и готовность ее распространять.

Очевидно, что наибольший эффект меры противодействия будут оказывать на начальном этапе распространения вредоносной информации, пока процесс не перешел в стадию резкого роста.

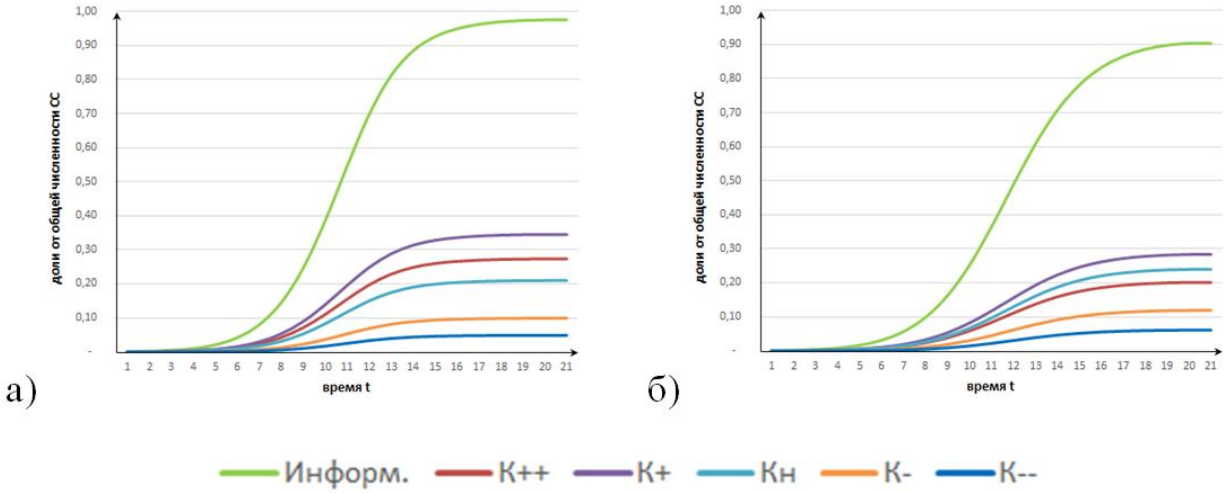


Рис. 3. Графики ПИВ: а) при $\omega^{\mathrm{H}} = 0{,}2, \omega^{\mathrm{C}} = 0{,}55, \omega^{\mathrm{B}} = 0{,}25$;
б) при $\omega^{\mathrm{H}} = 0{,}3, \omega^{\mathrm{C}} = 0{,}5, \omega^{\mathrm{B}} = 0{,}2$

Заключение

Прогресс коммуникативных технологий значительно разнообразил варианты подачи информации обществу. На сегодняшний день достижения науки и техники служат не только во благо, но и активно применяются для осуществления противоправной деятельности различных экстремистских и террористических организаций. Адекватным ответом на вызываемые ими деструктивные процессы должны стать меры информационного управления. Планирование и организация информационных акций требует практически ориентированного научного подхода для создания жизнеспособных эффективных моделей. Имитационное моделирование процесса информационного взаимодействия позволяет предсказывать реакцию общества на обнародование той или иной информации и принимать меры для регулирования и стабилизации информационного фона, что, в свою очередь, помогает снизить проявления антисоциального поведения.

Литература:

1. Ажмухамедов И.М. Синтез управляющих решений в слабо структурированных плохо формализуемых социотехнических системах / И.М. Ажмухамедов // Управление большими системами. – 2013. – № 42. – С. 29-54.

2. Громова Н.С. Профилактика молодежного экстремизма как угрозы безопасности региона / Н.С. Громова // Вестник Прикамского социального института. – 2017. – № 2 (77). – С. 16-23.

3. Деревяшко В.В. Влияние фактора старения информации на ее ценность для организации / В.В. Деревяшко // Математические и инструментальные методы экономики. Экономические науки. – 2010. – 1(62). – С. 425-427.

4. Ильичев И.Е. О понятии и классификации проявлений экстремизма / И.Е. Ильичев, С.А. Лазарева // Вестник Казанского юридического института МВД России. – 2017. – Т. 7, № 3. – С. 126 - 134.

5. Казарин О.В. Социально-правовые и технологические аспекты проблемы выявления деструктивных информационных воздействий в сети Интернет / О.В. Казарин,

В.П. Охапкин, Е.П. Охапкина, Р.А. Шаряпов // Вестник Российского государственного гуманитарного университета. – 2017. – № 3 (9). – С. 132-147.

6. Карнаушенко Л.В. Деструктивное информационно-психологическое воздействие на массовую аудиторию: правовые аспекты противодействия / Л.В. Карнаушенко // Вестник Краснодарского университета МВД России. – 2017. – № 2 (36). – С. 157-161.

7. Куликов Е.М. Экстремизм как социально-управленческая проблема трансформирующегося российского общества / Е.М. Куликов, Е.О. Кубякин, В.В. Плотников // Общество и право. – 2016. – № 4 (58). – С. 230-234.

8. Мачуева Д.А. Моделирование процесса информационного взаимодействия в социальных системах / Д.А. Мачуева, И.М. Ажмухамедов // Системы управления, связи и безопасности. – 2018. – № 2. – С. 18-39. URL: http://sccs.intelgr.com/archive/2018-02/02-Machueva.pdf

9. Мозговой В.Э. Информационный экстремизм как инновационная девиация социума начала XXI века / В.Э. Мозговой // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 1. – С. 61-65.

Акапьев В.Л., Дрога А.А., Савотченко С.Е.
Белгородский юридический институт
МВД России имени И.Д. Путилина

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРОГНОЗНОГО МОДЕЛИРОВАНИЯ В ПРАВЕ

В праве моделирование используется во многих областях. Доктринально оно является средством познания государственно-правовых явлений и процессов, в практической деятельности выступает как средство увеличения качества юридических действий от принятия и реализации нормативно-правовых актов и отдельных предписаний до выявления и расследования преступлений. В российские научные разработки в области правового моделирования сосредоточены в основном вокруг нескольких вопросов [1]. Наиболее всеобъемлющие правовые модели созданы в сфере борьбы с преступностью. Важную роль здесь играет наличие существенным образом развитой системы уголовно-правовой статистики [2].

Моделирование в криминалистике применяется для извлечения новой информации о совершенном преступлении и лицах, его совершивших [3]. В криминологии существуют множество разнообразных моделей преступного поведения и моделей на основе социальных явлений и преступности [4, 5]. Во многих отраслях права, к примеру, страхового права и права социального обеспечения, существенное значение имеют модели для оценивания рисков и их прогнозирования, которые применяются для расчетов тарифных ставок в страховании. В последние годы время в правовой охране окружающей среды стали использоваться аналогичные принципы моделирования [6].

Не говоря уже о том, что оценка риска является необходимым элементом социального контроля, который имеет основное значение при прогнозировании последствий принимаемых решений. Моделирование риска в целом и юридического в частности - это отдельное, динамично развивающееся направление теоретического моделирования, который характеризуется определенным предметом, методами, концепциями. С уверенностью можно сказать, что наблюдается устойчивая тенденция роста применения разработок в области моделирования правовых рисков [7].

Однако в теории права ситуация с перспективами применения разработок в сфере моделирования не на столько является оптимистичной, где моделирование выступает, в основном, как метод познания. Следует отметить, что последние значительные результаты моделирования в области теории права отмечены в 1980-х годах прошлого столе-

тия [8]. И это несмотря на то, что потребность в новых теоретических разработках давно назрела и ощущается все больше и больше [9].

В теории права методы моделирования зачастую приравниваются к абстрагированию – логическим методом познания, который позволяет формулировать научные понятия и категории, и правовые модели, соответственно, с абстракциями – понятиями и категориями, которые отражают универсальные свойства исследуемых явлений и процессов [10]. Получается, что два различных понятия получают одинаковое значение, а это явное противоречие в логике.

Понятие правовой модели зачастую считают тождественным понятию правовой теории. Однако, несмотря на то, что коммуникация теории и моделей очевидна, в их взаимоотношениях не так просто разобраться. Моделирование социальных процессов не может не опираться на теорию для объяснения некоторых общественных явлений. Теория вводит для моделирования определенные когнитивные ограничения, обеспечивающих его категориальный аппарат и другие образовательные инструменты.

Наиболее всеобъемлющие теории содержат различные модели, позволяющие, к примеру, прогнозировать динамику явлений, происходящих в обществе. В то же время, моделирование часто вынуждено выходить за рамки одной теории, обращаясь к остальным. Оно имеет по отношению к теории относительную самостоятельность. Потому что истина в какой-либо социальной теория подтверждается фактами, а моделирование, ориентированное на моделирование действительности, также может быть средством доказательства или опровержения теории. Трудно не согласиться с мнением, что в моделировании теория выступает в качестве инструмента для создания модели, а модель выступает в качестве посредника между формальной теорией и объективным положением дел [11].

Одним из тормозящих механизмов для широкого применения моделирования в праве становится узкое, формально-догматическое (нормативное) толкование норм закона, трактующее право как систему правовых понятий, выраженную в официальном регламенте. Например, по мнению А.С. Безрукова юридическая модель определяется как «созданная в результате абстракции, идеализации (для теоретических и метатеоретических моделей) или наблюдения (для материальных моделей) форма отражения правовой (или окружающей) действительности, находящаяся в отношении соответствия с исследуемым объектом, служащая средством отвлечения и выражения внутренней структуры сложного явления (или наглядности в описании объектов материального мира), дающая информацию об объекте или выполняющая специальную описательную (демонстрационную) задачу» [8].

Из данного определения вытекает, что здесь не ожидается формулировка теоретической модели на основе наблюдений. Для него закон - это не социальный факт, который можно изучать с помощью наблюдений или другим эмпирическим путем, а логическая система, которая постигается за счет абстрагирования и идеализации. Эта система, видимо, не развивается, поскольку определение относится к возможности для формулировки структурных и функциональных моделей, но не содержат указания на возможность разработки прогностических и причинно-следственных моделей.

Если оставаться в рамках узконаправленного толкования права и продолжать дискутировать по поводу правового моделирования, то можно прийти к следующим выводам: если модели представляют собой юридические понятия, то в течение моделирования правовых явлений, понимаемых как юридические понятия, получается, что разрабатываются не сами модели, а только их макеты. Образуется замкнутый круг. Такой когнитивный результат приходит в своих исследованиях А.С. Безруков [8]. Он отмечает, что одно и то же правовое явление можно рассматривать как модель по отношению к другому явлению (или группы явлений), которые, в свою очередь, представ-

ляют модель для предыдущей модели, только на другом иерархическом уровне. В конце концов, исследователь делает закономерный вывод об «относительном характере правовой модели». Это, на наш взгляд, поставить жирную точку в теории правового моделирования, в котором все является относительным, каковым является само правовое моделирование.

Однако, такие трудности не возникают в области криминологии и управления рисками. Создание правовой модели является не абстрактным понятием, а реальностью – деликвентного и рискованного поведения.

Перспективы в области моделирования смогут открыться в теории государства и права, если мы изменим подход к праву с нормативного на социологический и рассмотрим моделирование как не абстрактное построение описательных категорий и моделей, а модели, содержащие в том числе числовые значения, связанные с эмпирическими данными. Само по себе моделирование включает в себя гораздо больше, чем мыслительные операции обобщения и идеализации, поскольку основная цель моделирования - это моделирование реальной системы, чтобы выявить его свойства, которые включают, как минимум, наблюдения поведения системы в определенных условиях и передачу этих параметров в соответствующие значения в модели. Модели должны быть богаче по содержанию, чем абстрактные понятия, особенно динамические модели, которые объясняют любые процессы.

Похоже, что такие исследования являются наиболее актуальными в прогностических целях для прогнозирования действия нормативно-правовых актов. Прогностические модели нормативно-правовых актов, созданных на этапе обсуждения и принятия решения, могут в конечном итоге сократить количество неэффективных, нерациональных и общественно-политических правовых норм, добиться повышения качества законодательства [12].

Частично прогнозное моделирование реализуется как минимум в двух видах вспомогательного к законотворчеству прогнозирования: оценка регулирующего воздействия (далее – ОРВ), а также антикоррупционная экспертиза. Оно также может быть использовано как часть правового мониторинга комплексной оценки системы подготовки, принятия и прогнозирования, по мнению некоторых авторов [13, 14], действия нормативно-правовых актов.

Для разработки прогнозов моделирование применяется вместе с такими математическими методами как экстраполяция, статистические и вероятностные методы, экспертные оценки, сравнительно-правовые и интуитивным методами.

С целью попыток предсказания рисков появления отрицательных реакций, возникающих вследствие управления ОРВ, предлагается проведение социологических опросов, открытых консультаций с активными предпринимателями и менеджерами ведущих и крупных компаний, экономический расчет возможных последствий, которые могут проявиться после вступления в силу нормативных правовых актов и правовых действий. Цели проведения ОРВ конкретные: следует обнаружить в тексте проектов нормативных правовых актов формулировки, которые приводят к появлению избыточных ограничений и обязанностей для субъектов предпринимательской и иной деятельности или способствуют появлению у них и у бюджетов всех уровней необоснованных расходов. В процессе ОРВ, таким образом, моделируются не все последствия вступления в силу нормативного правового акта, а только те, которые актуальны для этих целей.

Перед специалистом по ОРВ стоит задача не только смоделировать, как будет действовать нормативный акт (и будет ли он вообще действовать), но в основном, чтобы решить, как он будет подходить к заданной системе приоритетов экономической политики. Поэтому моделирование в ОРВ избирательно и ориентировано на экономические последствия.

Самая известная в настоящее время отечественная методика антикоррупционной экспертизы законов была разработана в начале 2000-х годов экспертами Центра стратегических разработок. После этого она была использована Комиссией по борьбе с коррупцией Государственной Думы Федерального Собрания Российской Федерации и легла в основу официальных методик проведения антикоррупционной экспертизы проектов нормативных правовых актов и иных документов в целях выявления в них положений, способствующих созданию условий для проявления коррупции, утвержденной Постановлением Правительства Российской Федерации от 5 марта 2009 г. № 196 (далее – Методика). Методика направлена на выявление коррупционных факторов – положений проектов документов, которые могут способствовать проявлениям коррупции.

Разработка данной Методики и консолидация Министерства юстиции и Генеральной прокуратуры с целью выполнения обязанности осуществлять экспертизу проектов нормативно-правовых актов следует рассматривать как важный шаг на пути повышения качества законов. В то же время, метод имеет очевидные недостатки, основным из которых является упрощение антикоррупционного анализа, сводящегося к поиску так называемых коррупциогенных факторов, многие из которых определяются текстуально. Однако коррупция может скрываться как за всей целостностью нормативного правового акта, так и за теми частями, которые с помощью Методики не обнаруживаются. В таких случаях трудно ожидать успешного результата экспертизы. Следует отметить, что непосредственно сами коррупциогенные формулировки далеко не всегда однозначно свидетельствуют о коррупционной составляющей акта. Для реального функционирования антикоррупционных составляющих нормативно-правовых актов требуется систематический, комплексный анализ коррупционных рисков.

Таким образом, можно утверждать, что предметом анализа прогнозного моделирования должно являться правовое поведение. Также можно констатировать, что свойство «правовое» по отношению к поведению означает не его урегулированность правом, а потенциальную возможность быть таковым. Основным здесь выступает фактор именно правового воздействия. Правовое поведение в прогнозном моделировании – это возможное поведение, развивающееся в будущем, и которое станет результатом воздействия права на определенные общественные отношения.

Она может или соответствовать или противоречить правовым нормам, но также выйти за пределы правового регулирования, т.е. не регулируются правом. Такая широкая смысловая трактовка позволяет создавать реалистичные прогнозные модели, не ограниченные в своих прогностических возможностях искусственным (для случая юридического моделирования [15]) теоретическим различием между поведением на регулируемое и не регулируемое правом. Прогностическая модель правового поведения, таким образом, выражает в вербальной или иной символической форме систему знаний о возможном поведении субъектов права, изменяющемся в результате правовых действий.

Литература:

1. Берзинь О.А. Криминалистические подходы к моделированию преступной деятельности // Право. Журнал Высшей школы экономики. 2011. № 4. С. 133–143.

2. Варчук Т.В. Виктимологическое моделирование в теории детерминации преступности // Вестник Московского университета МВД России. 2012. № 10. С. 112–116.

3. Аршинский Л.В., Проблемы применения информационного и логико-математического моделирования в судебной экспертизе и криминалистике [Текст] / Л.В. Аршинский, Н.Ю. Жигалов, Ц.Б. Мункожаргалов // Российский следователь. 2013. № 3. С. 44 – 52.

4. Астафьев Е.Р. Методы корреляционного и регрессионного анализа обработки статистических данных / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарская академия МВД России, 2006. – 68 с.

5. Губанищев В.В. Общая модель механизма преступной деятельности в сфере экономики: условия формирования // Экономическая безопасность России. 2009. № 1. С. 82–88.

6. Kuran T., Sunstein C.R. Availability Cascades and Risk Regulation // Stanford Law Rev. 1999. 51:683–768; Slovic P. The Perception of Risk, Earthscan Publications Ltd. London UK and Sterling, VA, USA, 2000/

7. Щербаков В.А. О криминологическом моделировании эффективного предупреждения преступности в современных условиях // Вестник Московского университета МВД России. 2012. № 10. С. 132–135.

8. Безруков А.С. Моделирование в праве // Вестник Владимирского юридического института. 2008. № 1. С. 90–92.

9. Скурко Е.В. Метод социальноправового моделирования в решении задач правотворчества // Государство и право. 2003. № 1. С. 103–106.

10. Алексеев С.С. Общая теория права: учеб. 2-е изд., перераб. и доп. – М.: Проспект, 2009. С. 185–186.

11. Morgan M.S., Morrison M. (eds) Models as Mediators: Perspectives on the Natural and Social Sciences. Cambridge: Cambridge University Press, 2000; Suárez M., Cartwright N. Theories: Tools Versus Models // Studies in the History and Philosophy of Modern Physics. 2008. № 39. P. 62–81.

12. Салыгин Е.Н. Моделирование в праве: проблемы и перспективы // Пра-во: журн. Высш. шк. экономики. 2013. № 3. С. 12-35.

13. Арзамасов Ю.Г., Наконечный Я.Е. Мониторинг в правотворчестве: теория и методология. – М., 2009. С. 118.

14. Бойченко А.А. О разработке приложения для автоматизированной обработки данных, определяющих криминогенную обстановку / А.А. Бойченко, Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XII Всерос. науч.-практ. конф. 17 июня 2016 г. / редкол.: И.Н. Старостенко, Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодарский университет МВД России, 2016. – С. 43 – 48.

15. Плетников В.В. Понятие и виды моделей в современной отечественной юриспруденции: теоретико-правовое исследование // Научный ежегодник института философии и права уральского отделения российской академии наук. 2016. Т. 16. № 2. С. 121-135.

Алымов Н.Л.
Академия ФСО России, г. Орел

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МЕТРОЛОГИЧЕСКОГО НАЗНАЧЕНИЯ

В состав современных технических средств (ТСр), в том числе входящих в автоматизированные системы управления (АСУ), практические всегда, в том или ином виде входит специализированное программное обеспечение метрологического назначения (ПО МН). Это позволяет повысить оперативность обработки измерительной информации и существенно расширить их функциональные возможности.

В качестве ПО МН будем понимать компьютерную программу или совокупность программ, осуществляющих сбор, передачу, обработку, хранение и представление измерительной информации, а также электронной документации, необходимой для при-

менения этих программ. Метрологическое ПО может применяться как автономно, так и в составе ТСр. Вместе с тем, использование ПО, совместно с большими возможностями и преимуществами, может привести к появлению ошибок, погрешностей, связанных с применением самого ПО.

О возможности проявления таких рисков говорится в статье 9 Федерального закона «Об обеспечении единства измерений».

Большинство решаемых сегодня нами задач довольно не требовательны к величине этих погрешностей. Но очевидно, что с развитием науки и техники, перспективных информационных технологий, с практически обязательными требованиями к автоматизации процессов измерения, обработки результатов измерения и принятия решения, с необходимостью объединения ТСр в различные интегрированные информационно-измерительные системы с возможностью удаленного управления и в связи с этим появившуюся возможность враждебного воздействия на систему из вне − величина допустимой погрешности постоянно будет уменьшаться, а ущерб от этой погрешности и ответственность будут только увеличиваться.

На сегодняшний момент, уже на стадии приемки, в рамках ОКР в интересах нашего ведомства разрабатывается аппаратная технического обеспечения, диагностики и оперативного восстановления полевых комплексов связи. Основу аппаратной составляет информационно измерительная система, состоящая из компьютера, крейта с VXI модулями средств измерений и программного обеспечения, разработанного непосредственно для функционирования данной аппаратной.

Предварительные метрологическая экспертиза и испытание аппаратной показали, что несоответствие требованиям по метрологическому обеспечению были заложены уже на стадии ТТЗ. А вопросы, касающиеся программного обеспечения метрологического назначения (ПО МН), рассматривались вообще формально. Анализ причин этих событий выявил недостаточную проработанность нормативно-технической документации, пригодной для практического применения и недостаточную осведомленность персонала по вопросам общих и специальных требований к программному обеспечению метрологического назначения. Так же, до сих пор неразрешенными вопросами остаются критерии соответствия ПО МН установленным требованиям.

В связи с этим важно знать основные моменты, связанные с применением ПО МН. К основным источникам ошибок ПО МН можно отнести источники, связанные с погрешностью, вносимой ПО при обработке данных, а также источники, связанные с искажением ПО и данных вследствие недостаточной защищенности.

Источники ошибок схематично изображены на рисунке 1.

В случае недостаточной защищенности ПО основными объектами уязвимости могут являться: данные измерений, накопленные или поступающие на обработку в процессе измерений; динамический вычислительный процесс обработки измерительных данных; код программы; результаты обработки исходных данных и измерений, выдаваемых на исполнительные механизмы или пользователям.

Угрозы безопасности ПО могут быть как внутренними, так и внешними. При этом под внутренними угрозами понимают случайные или непреднамеренные воздействия, приводящие к отрицательным последствиям.

Чаще всего именно злоупотребление или неправильное использование ПО МН приводит к критической ситуации, когда результаты обработки измерительной информации могут оказаться недостоверными. В ряде случаев пользователи даже не знают, когда это случилось.

В качестве примера внешних угроз можно выделить преднамеренное разрушение и искажение ПО МН и данных. В данном случае подразумевается наличие злоумышленников, осуществляющих доступ к программам и данным для их искажения, хищения или уничтожения.

В качестве примера внешних угроз можно выделить преднамеренное разрушение

и искажение ПО МН и данных. В данном случае подразумевается наличие злоумышленников, осуществляющих доступ к программам и данным для их искажения, хищения или уничтожения.

Рис. 1. Источники ошибок, вносимых программным обеспечением метрологического назначения

Подытожив вышесказанное, необходимо отметить, что использование ПО в общем случае сопряжено с проявлением целого ряда рисков. В литературе различают группы рисков, связанные с проблемами управления, неправильным использованием ПО МН; неправильной поддержкой данных; нефункциональностью, неадекватностью и неполнотой ПО МН; некорректностью кода.

ПО МН обладает определенным жизненным циклом, и его параметры могут с течением времени изменяться по разным причинам. Эти изменения приводят к появлению ошибок управления. При управлении и контроле ПО МН различными пользователями, могут появляться такие негативные явления как несовместимость различных частей ПО МН, неаттестованные версии, некорректная сопроводительная документация и др.

Программная поддержка данных в свою очередь тоже имеет значительное влияние на погрешность результатов измерений. Незначительные изменения данных, обусловленные, главным образом, их преобразованием, имеет самое решающее значение для конечного результата измерения. Помимо этого, вследствие их математической обработки, они могут быть подвержены искажению при обмене данными, в результате преобразования в различных средах, системах, а также персоналом.

Нефункциональность, неадекватность и неполнота ПО МН проявляются, когда ПО МН начинают использовать не в тех условиях, на которые оно предварительно рассчитано, прежде всего, на уровне разработки математической модели измерительной задачи, математических алгоритмов, (т.е. математического обоснования измерительных процедур). Особенно эти недостатки ПО МН начинают оказывать влияние в тех случаях, когда необходима высокая воспроизводимость результатов измерений, т.е. при неизменных исходных данных должны получаться одинаковые результаты.

Исходный код ПО МН пишется людьми, поэтому нельзя исключить небрежность, и даже систематические ошибки при написании кода. Даже большое количество программ и тестов, позволяющих обнаруживать и исправлять ПО, абсолютную правильность кода сегодня не гарантируют.

С этим сложно бороться, но можно постараться предупредить. Для этого, при разработке ПО МН собственными силами или сторонней организацией особое внимание должно

быть уделено следующим аспектам: разработке полного описания и четкой спецификации всех требований, предъявляемых к ПО; описания и спецификации модели функционирования ТСр совместно с ПО, модели функционирования управляющего системой ПО; оценке степени риска, установление соответствующих технических средств защиты и защиты кода программы и данных от искажений, в том числе учет фактора надежности; оценка алгоритмов с точки зрения пригодности к решению измерительной задачи с требуемой точностью.

Если же осуществляется закупка готовой продукции с ПО МН, то необходимо убедиться соответствует ли данный продукт необходимому уровню требований.

При этом следует учитывать отличия от требований к другим программным продуктам. Помимо удовлетворения общим требованиям, к ПО МН дополнительно должны предъявляться следующие требования:

1. Использование ПО МН не должно искажать измерительную информацию, т.е. не должно влиять на метрологические характеристики ТСр или это влияние должно быть незначительным и оцениваемым.

2. ПО МН должно иметь защиту от преднамеренных и случайных изменений объектного кода программы, данных результатов измерений, параметров ТСр.

3. ПО МН должно иметь возможность идентификации для проверки соответствовать ПО, установленному в ТСр.

Более подробно можно ознакомиться с национальным стандартом, посвященным описанию требований к программному обеспечению метрологического назначения. (ГОСТ Р 8.654-2009).

Для подтверждения соответствия ПО МН установленным требованиям проводится аттестация, которая, конечно, стоит не малых денег. Поэтому уже перед испытаниями мы должны быть уверенными, что данное ПО эти испытания успешно пройдет.

Все это дает основание говорить о необходимости проведения предварительных (дополнительных) экспертиз разрабатываемого программного обеспечения метрологического назначения на всех стадиях: проектирования, разработки и испытаний.

Для этого, в частности, необходимо разработать проверочные стенды или рабочие места, содержащие основные (наиболее распространенные) методы аттестации ПО МН.

Большинство специалистов, работающих в этой области, считают, что основным должен быть метод «черного ящика». Однако единодушия в этом вопросе нет. Наряду с существующими подходами к решению проблемы проверки ПО предлагаются методы оценки неопределенности измерений с помощью программного обеспечения и методы метрологической аттестации программных продуктов, используемых при решении измерительных задач. Практически все специалисты согласны, что наиболее эффективным методом тестирования является метод, основанный на использовании опорного («эталонного») программного продукта. Отметим, что поскольку в настоящее время не сформулированы критерии отнесения программных продуктов к опорным («эталонным»), отсутствуют и какие-либо нормативные документы, регламентирующие эту процедуру.

Реализация данного предложения позволит повысить надежность функционирования ТСр, свести к минимуму риски, связанные с использованием ПО МН, и в конечном итоге будет способствовать оптимизации затрат на эксплуатационные расходы, связанные с обеспечением бесперебойного и надежного функционирования АСУ в целом.

Литература:

1. Левин С.Ф. Статистические методы и метрологическая аттестация программного обеспечения измерительных систем // Измерительная техника. − 2008. − № 11.

2. Дудыкин А.А., Кудеяров Ю.А., Паньков А.Н. Проблемы аттестации встроенного программного обеспечения средств измерений // Законодательная и прикладная метрология. − 2007. − № 1.

3. Алымов Н.Л., Корнев А.С. Общие подходы к оценке соответствия программного обеспечения метрологического назначения установленным требованиям // 39 Международная научно-техническая конференция молодых ученых «Проблемы метрологическое обеспечения ВВТ» сборник научных трудов ФГКУ «Главный научный метрологический центр» Минобороны России, г. Мытищи. −2014

Астафьев Е.Р
Краснодарское высшее военное авиационное
училище летчиков им. А.К. Серова

ПРОВЕРКА ЭФФЕКТИВНОСТИ МЕТОДИКИ ОБУЧЕНИЯ БЕГА НА 60 МЕТРОВ С ПРИМЕНЕНИЕМ ПАРАМЕТРИЧЕСКОГО КРИТЕРИЯ

Эффективность методики обучения может быть исследована различными научными методами. В настоящее время для проверки и оценки результатов воздействия на обучающихся новыми методиками обучения широко применяются методы количественного и качественного анализа, основанные на использовании математического аппарата [1, 6].

При статистической обработке результатов научных исследований одной из основных задач является проверка выдвигаемой статистической гипотезы, т.е. проверка достоверности различий между полученными результатами [2]. Для получения решения такой задачи проводится сравнительный эксперимента с выделением экспериментальных и контрольных групп [3].

При исследовании были выполнены следующие этапы:

1) выбрана статистическая модель;

2) сформулирована оцениваемая гипотеза (изменились ли результаты обучения в зависимости от применяемой методики);

3) использован критерий оценки для рассматриваемой статистической модели;

4) определен уровень значимости;

5) рассчитано значение выбранного статистического критерия для полученных данных;

6) рассчитанное значение критерия сравнено с граничным (табличным) значением и решен вопрос о достоверности различий.

В данной статье рассмотрена задача проверки эффективности новой методики обучения бега на 60 метров. Уровень значимости был принят равным 5%, т.е. различия считались достоверными при утверждении того, что ошибка в исследовании допускается не более чем в 5 случаях из 100.

Бег на 60 м (с высокого старта) проводится на стадионе. Отмеряется расстояние 60 м, обозначается «Старт», «Финиш». Обучающимся дается задание пробежать всю дистанцию с максимально возможной скоростью, не замедляя движения. Забег проводится парами. При поднятой руке с флажком испытуемые принимают стартовое положение: толчковая нога впереди, маховая сзади. По взмаху флажка обучающиеся устремляются вперед, максимально быстро. Измерение времени осуществляется вручную (секундомером). Результат: время пробега отрезка 60 м. Показ наглядно. Тест позволяет выявить скоростные способности обучающихся.

Для расчета достоверности различий использован t – критерий Стьюдента. В работе проведен сравнительный эксперимент, где одна группа (экспериментальная), со-

стоящая из 5 человек, занималась по предлагаемой экспериментальной методике, а другая (контрольная) – по традиционной, общепринятой. Рабочая гипотеза заключена в том, что новая, предлагаемая методика окажется более эффективной. Итогом эксперимента является контрольное исследование, по результатам которого (табл. 1) рассчитана достоверность различий и проверена правильность выдвинутой гипотезы [4].

Для расчета задачи выполняются следующие действия.

1. Вычисляется средние арифметические величины $\left(\overline{X}\right)$ для каждой группы в отдельности по следующей формуле:

$$\overline{X} = \frac{\sum_{i=1}^{n} X_i}{n}, \tag{1}$$

где $X_i -$ значение отдельного измерения; $n -$ общее число измерений в группе.

Таблица 1.

Определение времени бега в группах

Группа	n	Время (сек)				
Экспериментальная	5	8,03	8,12	9,00	8,14	8,12
Контрольная	5	8,45	9,16	9,65	9,86	9,58

При подстановке в формулу фактических значений из табл. 1, получено:

$$\overline{X_э} = \frac{8{,}03 + 8{,}12 + 9{,}00 + 8{,}14 + 8{,}12}{5} \approx 8{,}28;$$

$$\overline{X_к} = \frac{8{,}45 + 9{,}16 + 9{,}65 + 9{,}86 + 9{,}58}{5} \approx 9{,}34.$$

Сопоставление средних арифметических величин показывает, что в экспериментальной группе данная величина $\left(\overline{X_э} = 8{,}28\right)$ меньше, чем в контрольной $\left(\overline{X_к} = 9{,}34\right)$. Однако для окончательного утверждения о том, что новая методика более эффективна, следует убедиться в статистической достоверности различий t между рассчитанными средними арифметическими значениями [8].

2. Для этого было вычислено в обеих группах стандартное (квадратическое) отклонение σ по формуле:

$$\sigma = \pm \frac{X_{i\max} - X_{i\min}}{K}, \tag{2}$$

где $X_{i\max} -$ наибольший показатель; $X_{i\min} -$ наименьший показатель; $K -$ табличный коэффициент [5]. Значение коэффициента K найдено по таблице (приложение 1), который соответствует числу измерений в группе (пять). Получим, что $K = 2{,}33;$

$$\sigma_э = 0{,}4163 \text{ и } \sigma_к = 0{,}6052.$$

3. На следующем этапе проведено вычисление стандартной ошибки среднего арифметического значения m по формуле:

$$m = \pm \frac{\sigma}{\sqrt{n-1}}, \tag{3}$$

когда $n < 30$ и

$$m = \pm \frac{\sigma}{\sqrt{n}}, \tag{4}$$

когда $n \geq 30$ [9].

В исследовании использована первая формула, так как $n < 30$. Для каждой группы найдены значения m.

$$m_э = \pm \frac{0{,}4163}{\sqrt{5-1}} = \frac{0{,}4163}{2} \approx 0{,}2082; \; m_к = \pm \frac{0{,}6052}{\sqrt{5-1}} = \frac{0{,}6052}{2} \approx 0{,}3026.$$

4. Вычислена средняя ошибка разности по формуле:

$$t = \pm \frac{\overline{X}_э - \overline{X}_к}{\sqrt{m_э^2 + m_к^2}}. \tag{5}$$

В результате получено

$$t = \pm \frac{8{,}28 - 9{,}34}{\sqrt{0{,}2082^2 + 0{,}3026^2}} \approx \frac{1{,}06}{0{,}3673} \approx 2{,}8808.$$

5. По специальной таблице (приложение 2) определена достоверность различий. Для этого полученное значение t сравнено с граничным при 5%-ном уровне значимости $t_{0,05}$ при числе степеней свободы:

$$f = n_э + n_к - 2, \tag{6}$$

где $n_э$ и $n_к -$ общее число индивидуальных результатов соответственно в экспериментальной и контрольной группах. Если полученное в эксперименте t больше граничного значения $t_{0,05}$, то различия между средними арифметическими двух групп считаются ***достоверными*** при 5%-ном уровне значимости, и наоборот, в случае, когда полученное t ***меньше*** граничного значения $t_{0,05}$, считается, что различия ***недостоверны***, и разница в среднеарифметических показателях групп имеет случайный характер, либо требуется дополнительное исследование [7].

В рассмотренной задаче $f = 5+5-2 = 8$ и табличное значение $t_{0,05} = 2{,}31$. При сравнении табличного значения с вычисленным, получим $t = 2{,}88 > t_{0,05} = 2{,}31$. Следовательно, различия между полученными в эксперименте средними арифметическими значениями считаются достоверными, значит, предлагаемая методика обучения оказалась более эффективной, чем предыдущая.

Приложение 1

Значение коэффициента *K*

n	0	1	2	3	4	5	6	7	8	9
0	–	–	1,13	1,69	2,06	**2,33**	2,53	2,70	2,85	2,97
10	3,08	3,17	3,26	3,34	3,41	3,47	3,53	3,59	3,64	3,69
20	3,74	3,78	3,82	3,86	3,90	3,93	3,96	4,00	4,03	4,06
30	4,09	4,11	4,14	4,16	4,19	4,21	4,24	4,26	4,28	4,30
40	4,32	4,34	4,36	4,38	4,40	4,42	4,43	4,45	4,47	4,48
50	4,50	4,51	4,53	4,54	4,56	4,57	4,59	4,60	4,61	4,63
60	4,64	4,65	4,66	4,68	4,69	4,70	4,71	4,72	4,73	4,74

70	4,76	4,76	4,78	4,79	4,80	4,81	4,82	4,82	4,84	4,84
80	4,85	4,86	4,87	4,88	4,89	4,90	4,91	4,92	4,92	4,93
90	4,94	4,95	4,96	4,96	4,97	4,98	4,99	4,99	5,00	5,01
100	5,02	5,02	5,03	5,04	5,04	5,05	5,06	5,06	5,07	5,08
110	5,08	5,09	5,10	5,10	5,11	5,11	5,12	5,13	5,13	5,14

Приложение 2

Граничные значения *t*-критерия Стьюдента
для 5%-ного уровня значимости в зависимости от числа степеней свободы

Степень свободы (*f*)	Граничные значения *p*=0,05	Степень свободы (*f*)	Граничные значения *p*=0,05	Степень свободы (*f*)	Граничные значения *p*=0,05
1	12,71	13	2,16	25	2,06
2	4,30	14	2,15	26	2,05
3	3,18	15	2,13	27	2,05
4	2,78	16	2,12	28	2,05
5	2,57	17	2,11	29	2,04
6	2,45	18	2,10	30	2,04
7	2,37	19	2,09	40	2,02
8	2,31	20	2,08	50	2,01
9	2,26	21	2,08	60	2,00
10	2,23	22	2,07	80	1,99
11	2,20	23	2,07	100	1,98
12	2,18	24	2,06	120	1,98

Литература:

1. Астафьев, Е.Р. Статистические методы обработки экспериментальных данных: учеб. пособие / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарская академия МВД России, 2006. – 105 с.

2. Астафьев, Е.Р. Методы корреляционного и регрессионного анализа обработки статистических данных / Е.Р. Астафьев, Е.В, Михайленко. – Краснодар: Краснодарская академия МВД России, 2006. – 68 с.

3. Астафьев, Е.Р. Оценка эффективности методики обучения подтягивания на перекладине / Е.Р. Астафьев // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф (16 июня 2017 г.). – Краснодар: Краснодарский университет МВД России, 2017. – С. 14-17.

4. Астафьев, Е.Р. Основы теории вероятностей и математической статистики: учеб. метод. пособие / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарская академия МВД России, 2004. – 58 с.

5. Астафьев, Е.Р. Математика: курс лекций / Е.Р. Астафьев, В.В. Василенко, Е.В. Михайленко, И.Н. Старостенко. – Краснодар: Краснодарский университет МВД России, 2006. –347 с.

6. Астафьев, Е.Р. Временные ряды и прогнозирование: лекция / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарский университет МВД России, 2007. – 24 с.

7. Михайленко, Е.В. Теория вероятностей и математическая статистика: учеб. пособие / Михайленко Е.В., Жукова М.А, Бараненко Ф.Ф. – Краснодар: Краснодарский университет МВД России, 2011. – 142 с.

8. Михайленко, Е.В. Технологии исследования характеристик вариационного ряда в среде VBA / Е.В. Михайленко, А.В. Новосельцева // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16

июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 204.

9. Михайленко, Е.В. Методы решения задачи построения рейтинговых оценок качества функционирования социально-экономических систем / Е.В. Михайленко // Математические методы и информационно-технические средства: Труды Всерос. науч.-практ. конф, 23 июня 2006 г. – Краснодар: Краснодарский университет МВД России, 2006. – С. 68 – 74.

Баранова Е.М., Кочкин К.Ю.
Тульский государственный университет

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ КОДИРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ И РАСЧЕТА ХАРАКТЕРИСТИК ЭФФЕКТИВНОСТИ КОДА

В работе представлено описание процесса разработки программы для формирования эффективного кода текстовой информации, а также для расчета показателей, оценивающих, насколько разработанный код эффективен

Ключевые слова: текстовая информация, символьная информация, программное обеспечение, алгоритмизация, схема работы программы.

С целью автоматизации процессов кодирования текстовой информации была разработана программа «Эффективный_код_2.0».

Эта программа предназначена для:

– декомпозиции текста;
– подсчета частот встречаемости каждого символа;
– подсчета вероятности появления каждого символа в тексте;
– равномерного кодирования каждого символа;
– кодирования методом Шеннона-Фано;
– кодирования методом Хаффмана;
– подсчета метрик проведенного кодирования (энтропии(H), средней длины кодовой последовательности (Ncp) и среднего количества информации (Icp) по каждому методу кодирования).

Ниже рассмотрен процесс построения эффективного код Шеннона-Фано и Хаффмана.

Для кодирования текстовой информации по методу Шеннону-Фано необходимо выполнить следующие действия:

– расположить элементы по убыванию вероятностей;
– разбивать элементы на группы с примерно равной суммарной вероятностью, элементам одной из групп приписывать «1», другой «0» и повторять это действие для получившихся групп до тех пор, пока в каждой группе не останется по одному элементу;
– записать получившиеся комбинации.

Сообщ.	Вероятность	Группы и подгруппы				Код.	n_i
a_i	$p(a_i)$	1-я	2-я	3-я	4-я	комбинация	
a_1	0,25	0	0			00	2
a_4	0,25		1			01	2
a_5	0,125	1	0	0		100	3
a_7	0,125			1		101	3
a_2	0,0625		1	0	0	1100	4
a_3	0,0625				1	1101	4
a_6	0,0625			1	0	1110	4
a_8	0,0625				1	1111	4

Рис. 1. Построение кода Шеннона-Фано

Непосредственно перед программной реализацией был разработан алгоритм, который определяет суть поиска двоичного кода для каждого символа или для последовательностей символов текста, подлежащего эффективному кодированию.

После получения эффективного кода программа в соответствии с предложенным алгоритмом определяет ряд метрик, а именно:

– энтропию на один символ;

– общую энтропию;

– среднее количество символов в коде.

На рисунке 2 показана схема работы процедуры кодирования текста программы «Эффективный_код_2.0».

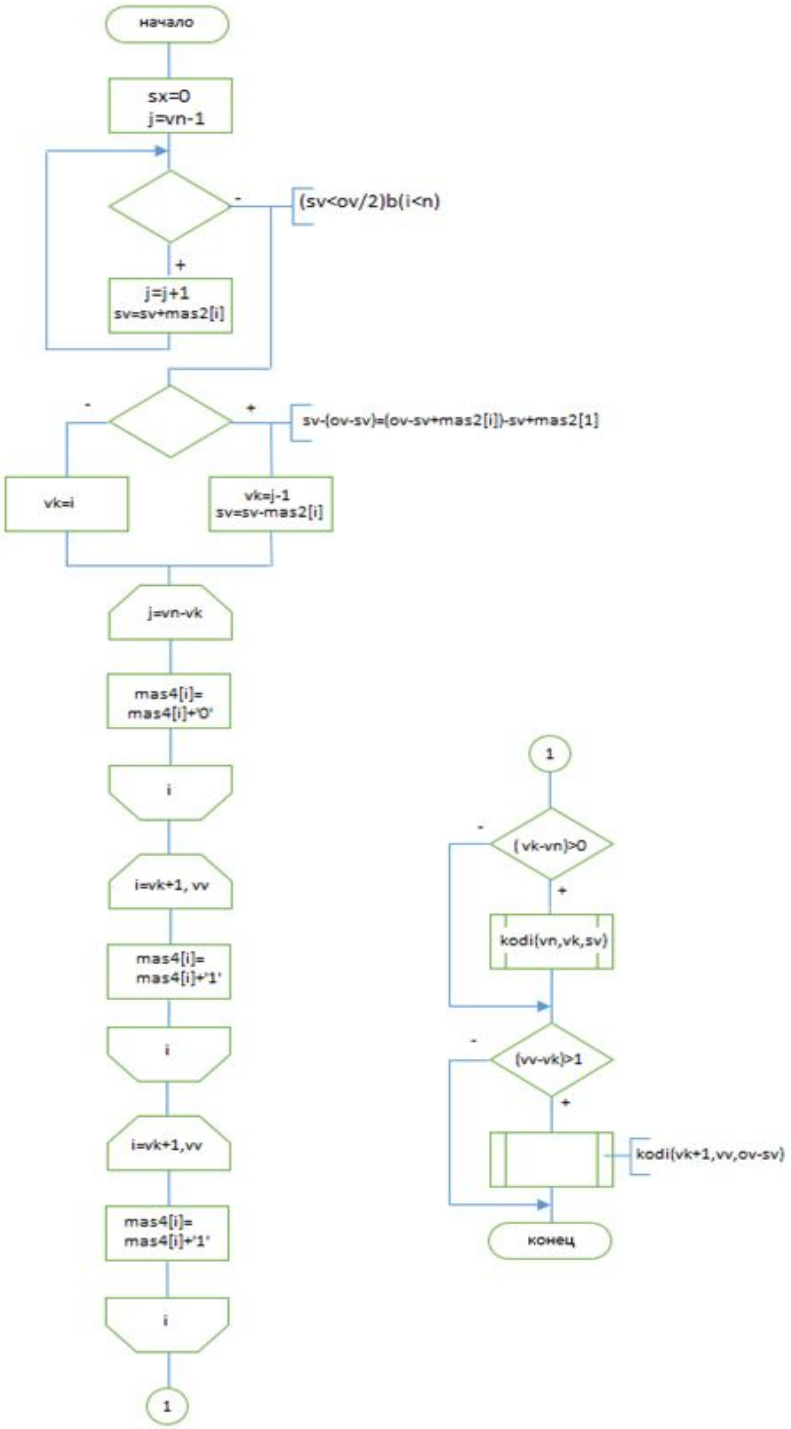


Рис. 2. Схема работы процедуры кодирования текста методом Шеннона-Фано

На рисунке 3 показана программная реализация процедуры. На рисунке 4 показано дерево Хаффмана. На рисунке 5 показана схема работы кодирования текста методом Хаффмана.

```
rocedure kodi(vn,vv:integer; ov:real);
   var
      vk,i:integer;
      sv:real;
   begin
      sv:=0;
      i:=vn-1;
      while (sv<ov/2) and (i<n) do
         begin
         inc(i);
         sv:=sv+mas2[i];
         end;
      if (sv-(ov-sv))+0.0000000001>=((ov-sv+mas2[i])-sv+mas2[i])
then begin vk:=i-1; sv:=sv-mas2[i] end else vk:=i;
      for i:=vn to vk do mas4[i]:=mas4[i]+'0';
      for i:=vk+1 to vv do mas4[i]:=mas4[i]+'1';
      if vk-vn>0 then kodi(vn,vk,sv);
      if vv-vk>1 then kodi(vk+1,vv,ov-sv);
   end;

rocedure kodirovkaSHF;
   var
      i,m:integer;
   begin
      for i:=1 to n do mas4[i]:='';
      kodi(1,n,1);
      nsr:=0;
      for i:=1 to n do nsr:=nsr+mas2[i]*length(mas4[i]);
      for i:=1 to n do
         begin
            m:=length(mas4[n])-length(mas4[i]);
            for g:=1 to m do mas4[i]:=mas4[i]+' ';
         end;
   end;
```

Рис. 3. Программная реализация процедуры

Кодирование по Хаффману выполняется следующим образом:

1) упорядочивание элементов по убыванию частот;

2) объединение частот, которое осуществляется в следующей последовательности:

а) две последние частоты списка складываются, а иные символы исключаются из списка;

б) оставшийся после исключения символов список пополняется суммой частот и вновь упорядочивается;

в) предыдущие шаги повторяются до тех пор, пока ни получится единица в результате суммирования и список ни уменьшится до одного символа.

3) построение двоичного кодового дерева, что осуществляется по следующему алгоритму:

а) корнем его является вершина, полученная в результате объединения частот, равная 1;

б) листьями – исходные вершины;

в) остальные вершины соответствуют либо суммарным, либо исходным частотам, причем для каждой вершины левая подчиненная вершина соответствует большему слагаемому, а правая – меньшему;

г) ребра дерева связывают вершины-суммы с вершинами-слагаемыми.

д) ребра дерева кодируются: каждое левое кодируется единицей, каждое правое – нулем;

4) формирование кода: для получения кодов кодируемых символов продвигаются от корня к нужной вершине и «собирают» веса проходимых ребер.

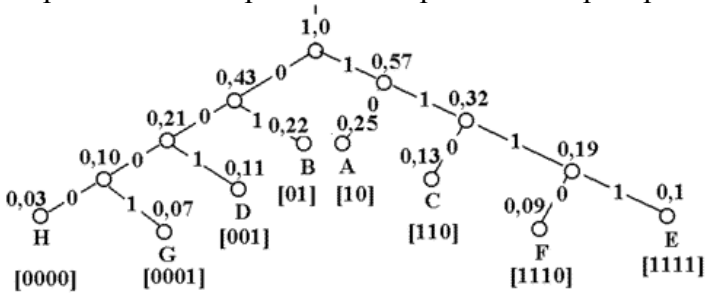


Рис. 4. Дерево Хаффмана

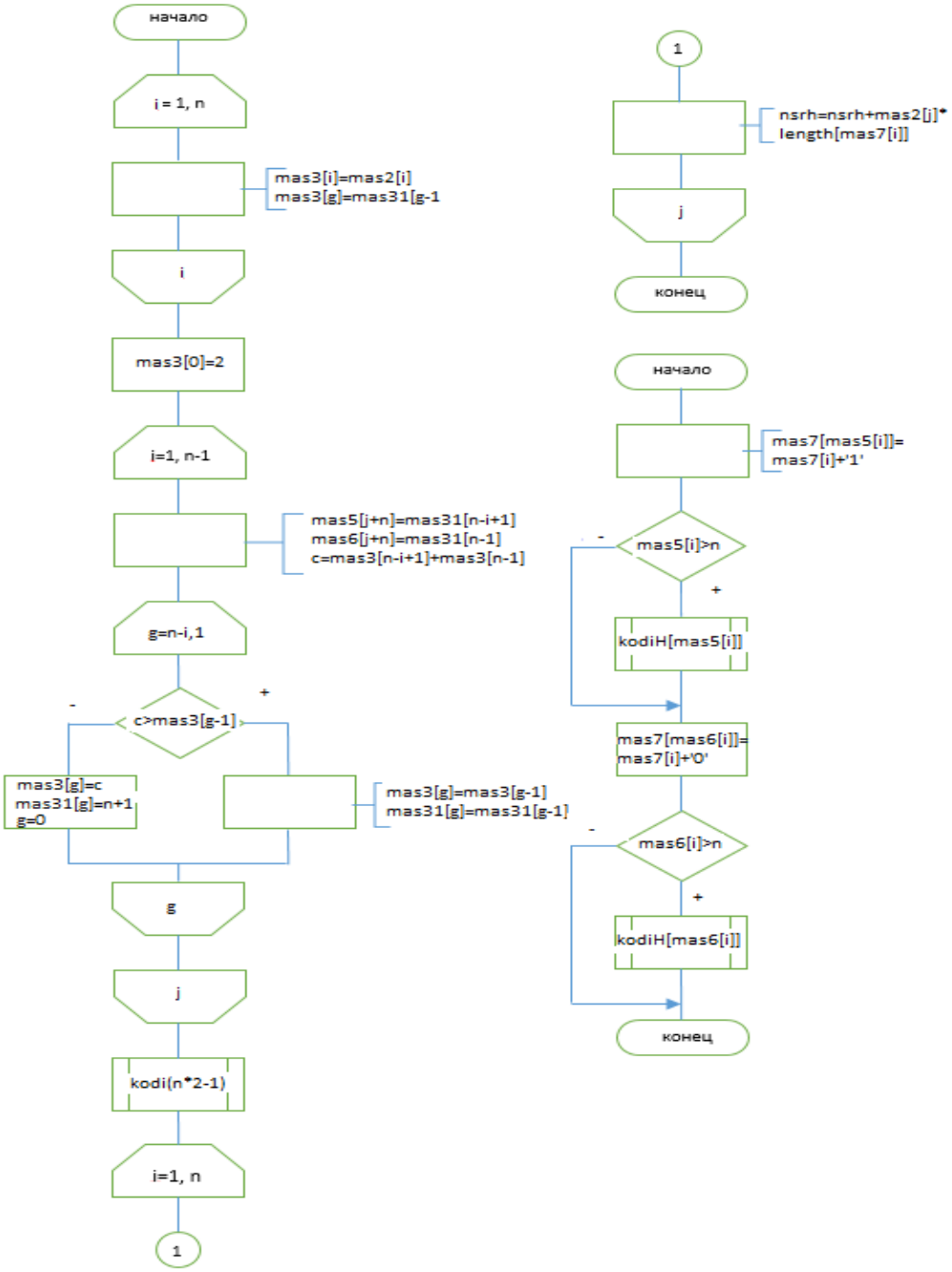


Рис. 5. Схема работы процедуры кодирования текста методом Хаффмана

На рисунке 6 показана программная реализация процедуры кодирования текста методом Хаффмана.

```
procedure kodih(i:integer);
    begin
       mas7[mas5[i]]:=mas7[i]+'1';
       if mas5[i]>n then kodih(mas5[i]);
       mas7[mas6[i]]:=mas7[i]+'0';
       if mas6[i]>n then kodih(mas6[i]);
    end;
procedure kodirovkaH;
    var
       i,g:integer;
       c:real;
       mas3:array[0..1000] of real;
       mas31:array[1..1000] of integer;
    begin
       for i:=1 to n do begin mas3[i]:=mas2[i]; mas31[i]:=i; end;
       mas3[0]:=2;
       for i:=1 to n-1 do
          begin
             mas5[i+n]:=mas31[n-i+1];
             mas6[i+n]:=mas31[n-i];
             c:=mas3[n-i+1]+mas3[n-i];
             for g:=n-i downto 1 do
                begin
                   if c>mas3[g-1] then begin mas3[g]:=mas3[g-1];
                mas31[g]:=mas31[g-1]; end
                  else begin mas3[g]:=c; mas31[g]:=n+i; break; end;
                end;
       end;
    for i:=1 to n do mas7[i]:='';
    kodih(n*2-1);
    nsrh:=0;
    for i:=1 to n do nsrh:=nsrh+mas2[i]*length(mas7[i]);
end;
```

Рис. 6. Реализация метода в программе

Таким образом, автоматизация процесса эффективного кодирования позволяет быстро и точно получить кодовую последовательность каждого символа текста и определить метрики эффективности полученного кода в сравнении с методом равномерного кодирования текстовой и текстово-символьной информации.

Литература:

1. Кочкин К.Ю., Баранова Е.М. Разработка программы для эффективного кодирования текстовой информации и комбинаций в комбинаторных задачах//Мехатроника, автоматика и робототехника. 2018. № 2. С. 224-229.

2. Самсонов Л.О. Эффективное кодирование данных. Спб., Нева, 2016 – 188 с.

3. Таев К.И. Сжатие данных, изображений и звука. М., Наука, 2014 – 320 с.

Басан Е.С., Михайлов Н.В.
Институт компьютерных технологий и информационной безопасности
Инженерно-технологическая академия г. Таганрог

ИССЛЕДОВАНИЕ, ПОИСК И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ДЛЯ СЕТИ МОБИЛЬНЫХ РОБОТОВ С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

Обзор применимости требований по безопасности ФСТЭК к сети мобильных роботов.

1. Идентификация и аутентификация субъектов доступа и объектов доступа.

Каждый пользователь входящий в информационную систему, к примеру, сеть служебного пользования, должен указать пароль и, если стандарт, по которому функционирует сеть предоставляет возможность аутентификации, логин.

Усиление 1а: В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов) с использованием сети связи общего пользования, в том числе сети Интернет.

Вывод: Если говорить о беспроводных сетях, то смысл усиления 1а представлен в пользователе, который имеет доступ к Wi-Fi роутеру, которому необходимо вести аудит происшествий в информационной системе [1].

Усиление 2а: В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, в том числе сети Интернет.

Вывод: Данное усиление стоит применять, если поднимается сеть для служебного пользования, в которой каждому пользователю определена роль, на основании которой ему присваиваются права.

Усиление 3: В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);

Усиление 4: В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);

Вывод: В третьем и четвертом усилениях должны использоваться только локальные сети для сужения спектра атак. Тогда злоумышленнику необходимо будет находится на территории организации.

2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.

Информационная система предусматривает использование сторонних устройств, но существует необходимость вести аудит этих средств. Тогда определяются необходимые протоколы в сети, учет и присваивание идентификаторов для этих устройств, в случае необходимости осуществляется блокировка этих средств, определяется пользователь с правами администратора, организацией составляются руководящие документы.

Усиление 1б: Оператором должно быть исключено повторное использование идентификатора пользователя в течение не менее трех лет;

Вывод: Данный способ защиты запрещает пользователям иметь несколько устройств, которые в информационной системе значатся как одно, что не дает злоумышленнику вектора атак через сторонние устройства, которые неправильно сконфигурированы [2].

Усиление 2б: Оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 45 дней;

Вывод: К примеру, администратор потерял устройство, которое он редко использует в рамках информационной системы, но MAC-адрес этого устройства значится в базах, тогда по истечению 45 дней данный адрес будет заблокирован, и если он когда-нибудь будет обнаружен в какой-то резервной копии, он не будет представлять из себя вектор для атаки.

3. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Перед доступом в информационную систему пользователям должны быть выданы их логины и пароли, которые могут быть в любой момент времени изменены. Большой критике подвергается пароль, его длина, алфавит, количество неверно введенных данных. Организация составляет приказ или документ на основании которого оговариваются параметры и период их корректировки.

Усиление 1г: данное усиление определяет длину пароля не менее чем 8 символов, алфавит не менее из 70 символов, максимальное количество неверно введенных данных не более чем 4 раза, блокировка устройства случае истечения попыток входа на 15-60 минут, период смены не должен превышать 60 дней.

Вывод: Во всемирной паутине полно способов, с помощью которых каждый рядовой пользователь может перебрать пароль при помощи стороннего ПО, онлайн-сервисов, встроенного ПО, различие есть только в быстродействии [3]. Данное усиление способно увеличить время проведения атаки, но стоит отметить, что, к примеру, перехват рукопожатия и подбор хеш-суммы к нему выполняется на оборудовании злоумышленника и здесь бесполезны параметр количества неверных попыток ввода.

4. Управление доступом субъектов доступа к объектам доступа.

Каждый пользователь, входящий в информационную систему должен иметь запись в базе данных, которая содержит в себе ее тип, группы, в которых состоит пользователь, права доступа [4]. Как правило, данное требование осуществляется в интерфейсе операционной системы, в котором формируется матрица доступа для ее сопоставления с таблицей пользователей.

Усиление 1: Оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей.

Вывод: Аудит за учетными данными ведется с помощью ПО, функционал которого позволяет удалять, добавлять, объединять пользователей в группы [5]. Это необходимо не сколько для осуществления порядка, сколько для четкого формирования структуры информационной сети.

Усиление 2: В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

Вывод: В информационной системе должен присутствовать компонент, отвечающий за блокирование пользователей, иначе база данных либо просто переполнится и случится сбой, либо через устаревшую запись можно будет осуществить доступ к информационной системе.

Усиление 3б: В информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования: более 45 дней.

Вывод: В информационной системе не должно присутствовать неиспользованных записей, т.к. их наличие – это дополнительный вектор атаки для злоумышленника.

Заключение. В мире не придумано такого стандарта, по которому возможно создать неуязвимую информационную систему, ведь любую защиту можно сломать, уделив достаточно времени для этого.

В данной статье были рассмотрены требования, предъявляемые к информационной системе, из документа «ПРОГРАММА И МЕТОДИКИ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ». Если использовать этот документ в полном объеме и реализовать все усиления для каждого требования, то возможно реализовать защищенную и стойкую информационную систему, но не стоит забывать, что защита продукта не должна стоит больше, нежели сам продукт.

Работа выполнена при поддержке Гранта РФФИ 18-07-00212 Разработка метода и протокола принятия решений для обнаружения аномального поведения узла в системах группового управления автономными мобильными роботами.

Литература:

1. А.С. Басан, Е.С. Басан, О.Б. Макаревич. Анализ проблем обеспечения безопасности в мобильных автономных робототехнических системах. Материалы Двенадцатой Всероссийской научно-практической конференции и Восьмой молодежной школы-семинара «Управление и обработка информации в технических системах». Ростов-на-Дону. 2017. С 75-84.

2. Банк данных угроз безопасности информации [Электронный ресурс]. URL: http:// www.bdu.fstec.ru Банк данных угроз безопасности информации ФСТЭК России (дата обращения 18.04.2016).

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год.

4. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5. Абрамов Е.С., Басан Е.С. Разработка модели защищенной кластерной беспроводной сенсорной сети. / Известия ЮФУ. Технические науки. / № 12(149) 2013 г. Тематический выпуск Информационная безопасность. Издательство ТТИ ЮФУ в г. Таганроге. С. 48-56.

Валиахметова Е.Д., Хромых А.А.
Краснодарский университет МВД России

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ОПТИМИЗАЦИИ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

В настоящее время все чаще возникают задачи, связанные с обслуживанием потоков событий, носящие случайный характер. Подобные задачи возникали всегда, однако в простейших случаях они решались без применения методов математического моделирования. Применение ЭВМ позволяет значительно упростить решение задач системы массового обслуживания (СМО).

Основной задачей данной работы было создание программного продукта в среде Visual Basic for Application, позволяющего определять эффективность работы СМО и предлагать рекомендации для увеличения вероятности приема сигнала.

Для решения поставленной задачи была разработана форма для внесения данных пользователем (рис. 1). В зависимости от выбранных условий, форма может видоизменяться (рис. 2).

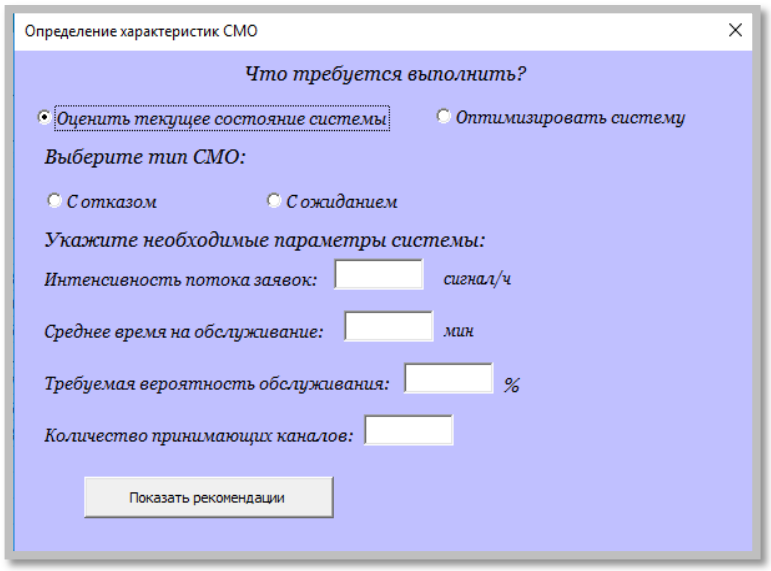


Рис. 1. Вид формы для оценки текущего состояния

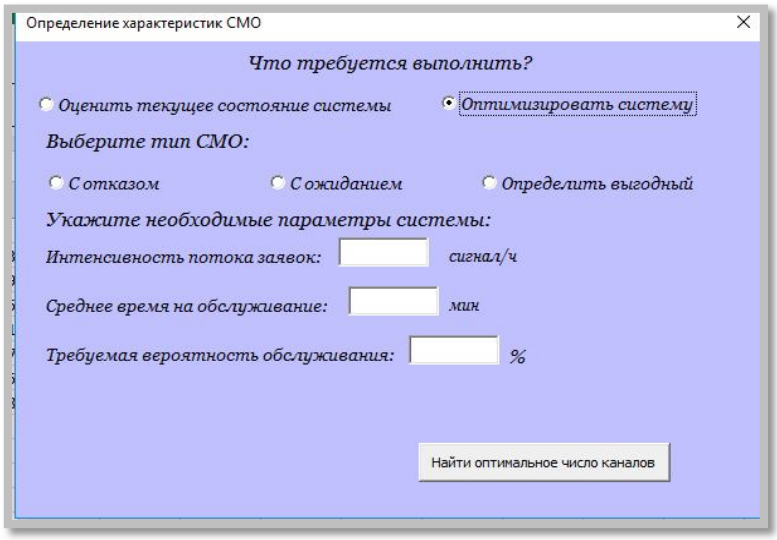


Рис.2. Вид формы для оптимизации

С помощью разработанного программного продукта была решения следующая задача:

В дежурной части (ДЧ) отдела полиции «Кировский» Управления МВД России по г. Кемерово поступающие сигналы принимают два сотрудника. Если звонок поступает в момент, когда обе линии заняты обслуживанием дозвонившихся ранее граждан, то звонок сбрасывается без ожидания. Статистика показывает, что среднее число сигналов, поступающих в дежурную часть в течение часа, равно 25. Среднее время, которое сотрудник затрачивает на обработку сигнала, равно 8 мин.

Необходимо оценить характеристики работы данной дежурной части как СМО с отказами. Найти оптимальное количество сотрудников, которые могут принимать сигналы с вероятностью реагирования выше 85%.

Перед тем как решить задачу с помощью разработанной программы, оценим характеристики исследуемой СМО:

1) в системе работают 2 сотрудника – ДЧ представляет собой 2х- канальную СМО, т.е. n=2;

2) сигнал покидает линию, не ожидая обслуживания – СМО с отказами;

3) среднее число сигналов, поступивших в ДЧ в течение часа, равно 25 – поток заявок простейший с интенсивностью $\lambda = 25$;

4) среднее время на обслуживание равно 8 мин. или 1/ 7,5 часа;

5) интенсивность длительности обслуживания: μ=1, t=7,5.

Заполним форму программы согласно условию задачи (рис. 3).

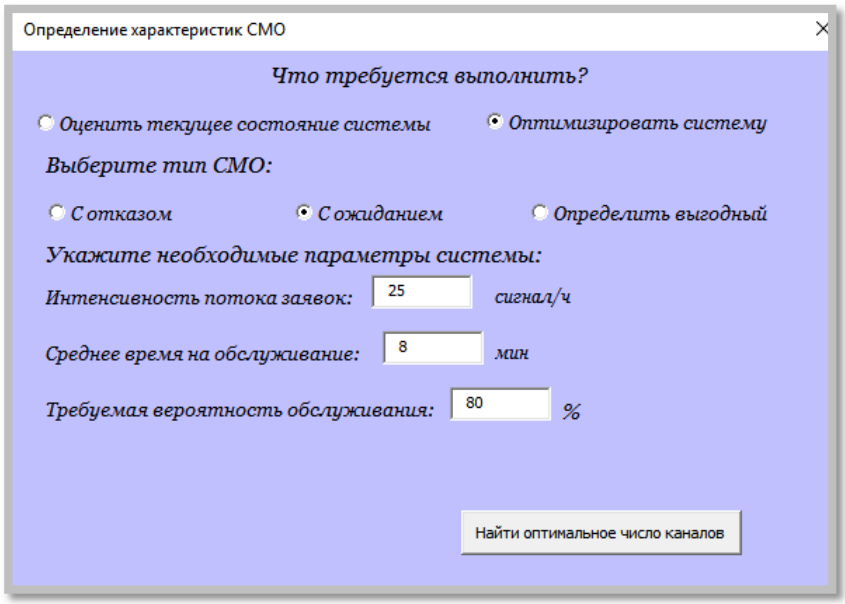


Рис. 3. Заполненная форма для оценки текущего состояния

Программный код для задачи «Оптимизация» выглядит следующим образом:

```
Private Sub chanels_Click()
    lm = Val(intensive.Value)
    m = Round(60 / Val(time.Value), 1)
    pn = Val(theory.Value) / 100
    a = Round(lm / m, 1)
        While p < pn                        'Расчет оптимального количества
            n = n + 1                           'каналов для СМО с ожиданием
                For i = 0 To n
                    p0 = p0 + a ^ i / fact(i)
                Next i
            p0 = Round(p0 ^ (-1), 2)
            p = Round(1 - (p0 * a ^ n / fact(n)), 2)
        Wend
        n1 = n
        n = 0: p = 0: p0 = 0
        While p < pn                            'для СМО с отказами
               n = n + 1
                   For i = 0 To n
                       p0 = p0 + a ^ i / fact(i)
                   Next i
               p0 = Round((p0 + a ^ (n + 1) / fact(n) / (n - a)) ^ (-1), 2)
               p = Round(1 - p0 * a ^ (n + 1) / fact(n) / (n - a), 2)
        Wend
        n2 = n
    If отказ.Value = True Then MsgBox "Оптимальное число принимающих каналов: " & n1
    If ожидание.Value = True Then MsgBox "Оптимальное число принимающих каналов: " & n2
    If определить.Value = True Then
        If n1 > n2 Then MsgBox "Оптимальное число каналов: " & n2 & "(СМО с ожиданием)"
        If n1 = n2 Then MsgBox "Оптимальное число каналов: " & n1 & ", независимо от типа СМО"
        If n1 < n2 Then MsgBox "Оптимальное число каналов: " & n1 & "(СМО с отказами)"
    End If
End Sub
```

Программный код для оценки текущего состояния системы имеет следующий вид:

```
Private Sub help_Click()
    lm = Val(intensive.Value)
    m = Round(60 / Val(time.Value), 1)
    pn = Val(theory.Value) / 100
    a = Round(lm / m, 1)
    n = Val(ch.Value)
    p0 = 0
    If отказ.Value = True Then
        For i = 0 To n
            p0 = p0 + a ^ i / fact(i)
        Next i
        p0 = p0 ^ (-1)
        p = 1 - p0 * a ^ n / fact(n)
        If p >= pn Then answer = "Система работает нормально, вероятность обслуживания: " & Round(p, 2) & vbCr
        If p < pn Then
            answer = "Вероятность обслуживания меньше требуемой: " & Round(p, 2) & vbCr & "Способы оптимизации: " & vbCr
            p = 0
            n1 = n
            While p < pn
               n1 = n1 + 1
                   For i = 0 To n1
                       p0 = p0 + a ^ i / fact(i)
                   Next i
               p0 = Round(p0 ^ (-1), 2)
               p = Round(1 - (p0 * a ^ n1 / fact(n1)), 2)
            Wend
            answer = answer + "1) Увеличить количество принимающих каналов до " + Str(n1) + vbCr
            p = 0
            t = Val(time.Value)
            While p < pn
                t = t - 1
                 m = Round(60 / t, 1)
                 a = Round(lm / m, 1)
                    For i = 0 To n
                        p0 = p0 + a ^ i / fact(i)
                    Next i
                p0 = Round(p0 ^ (-1), 2)
                p = Round(1 - (p0 * a ^ n / fact(n)), 2)
            Wend
            answer = answer + "2) Уменьшить время обработки заявки до" + Str(t)
        End If
    Else
        For i = 0 To n
            p0 = p0 + a ^ i / fact(i)
        Next i
        p0 = Round((p0 + a ^ (n + 1) / fact(n) / (n - a)) ^ (-1), 2)
        p = Round(1 - p0 * a ^ (n + 1) / fact(n) / (n - a), 2)
        If p >= pn Then answer = "Система работает нормально, вероятность обслуживания: " & p & vbCr
        If p < pn Then
            answer = "Вероятность обслуживания меньше требуемой: " & Round(p, 2) & vbCr & "Способы оптимизации: " & vbCr
            p = 0
            n1 = n
            While p < pn
               n1 = n1 + 1
                   For i = 0 To n1
                       p0 = p0 + a ^ i / fact(i)
                   Next i
               p0 = Round((p0 + a ^ (n1 + 1) / fact(n1) / (n1 - a)) ^ (-1), 2)
               p = Round(1 - p0 * a ^ (n1 + 1) / fact(n1) / (n1 - a), 2)
            Wend
            answer = answer + "1) Увеличить количество принимающих каналов до " + Str(n1) + vbCr
            p = 0
            t = Val(time.Value)
            While p < pn
                t = t - 1
                 m = Round(60 / t, 1)
                 a = Round(lm / m, 1)
                 For i = 0 To n
                       p0 = p0 + a ^ i / fact(i)
                 Next i
                 p0 = Round((p0 + a ^ (n + 1) / fact(n) / (n - a)) ^ (-1), 2)
                 p = Round(1 - p0 * a ^ (n + 1) / fact(n) / (n - a), 2)
            Wend
             answer = answer + "2) Уменьшить время обработки заявки до" + Str(t)
        End If
    End If
    MsgBox answer

End Sub
```

После обработки внесенных в форму данных, программа выдает результат (рис. 4, 5).

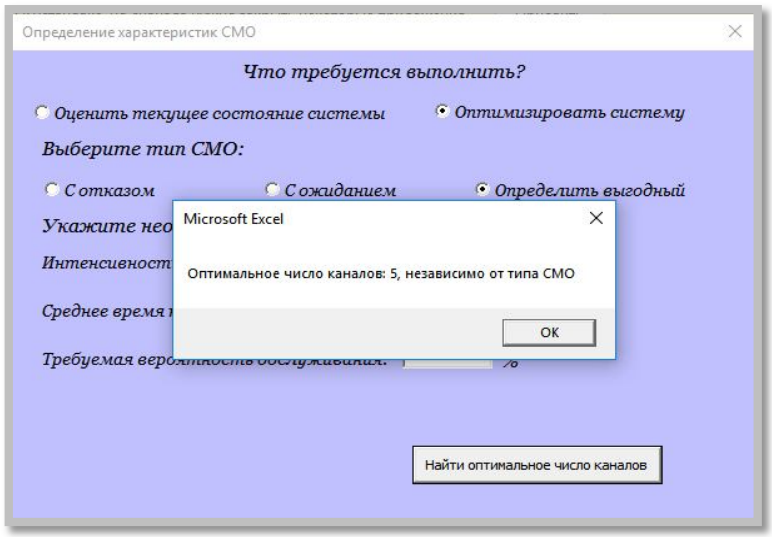


Рис. 4. Результат задачи «Оптимизация»

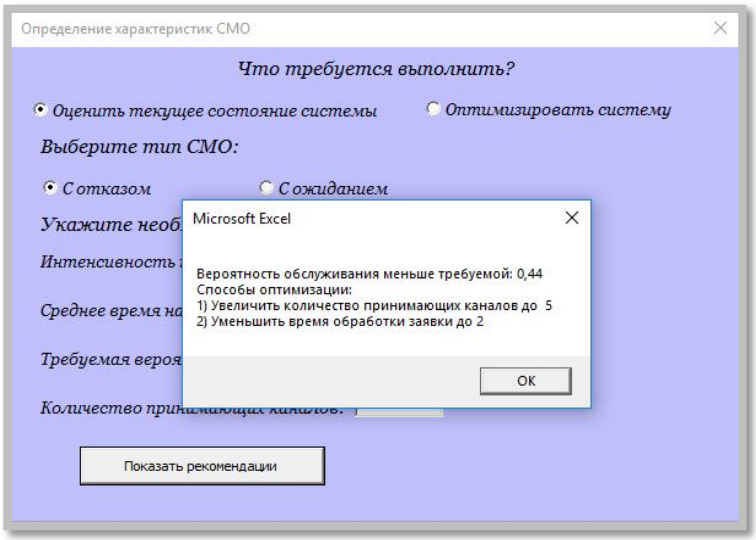


Рис. 5. Результат оценки текущего состояния системы

Таким образом, разработанная программа позволяет гораздо быстрее решать задачи без потери данных. К тому же можно выделить ряд преимуществ:

1) данная программа позволяет решать одновременно две различные задачи, а именно «оптимизация СМО» и «анализ системы»;

2) возможно выбрать оптимальный тип системы: с отказами или с ожиданием, с указанием количества каналов;

3) для анализа системы на выходе программы появляется сообщение о способах организации СМО для повышения уровня ее производительности.

Литература:

1. Фомин Г.П. «Математические методы и модели в коммерческой деятельности».

2. Кошуняева Н.В., Патронова Н.Н. Теория массового обслуживания (практикум по решению задач) / САФУ имени М.В. Ломоносова. – Архангельск; САФУ, 2013.

3. Информационные ресурс «Математический форум» [Электронный ресурс]. – Режим доступа: http://mathhelpplanet.com/

4. Михайленко Е.В. Прикладная математика: курс лекций / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2014. – 192 с.

5. Михайленко Е.В. Методы оптимизации: сборник задач / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2015. – 140 с.

Гавришев Алексей Андреевич
Северо-Кавказский федеральный университет

КАЧЕСТВЕННЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ РАСПРОСТРАНЕННОЙ СИСТЕМЫ СВЯЗИ, ОСНОВАННОЙ НА МЕТОДЕ ПЕРЕКЛЮЧЕНИЯ ХАОТИЧЕСКИХ РЕЖИМОВ

В настоящее время идет активное развитие защищенных систем связи в гражданских и военных сферах применения. Одним из самых перспективных направлений в области защищенных систем связи является использование хаотических сигналов. Хаотические сигналы по сравнению с классическими шумоподобными сигналами обладают следующими преимуществами: большое потенциальное число кодовых конструкций, сплошной спектр мощности, непредсказуемость на больших интервалах времени, повышенная защищенность от несанкционированного доступа [1]. В настоящее время значительный интерес представляет количественное и качественное исследование защищенных систем связи на основе хаотических сигналов [2, 3]. Одним из основных методов качественного исследования защищенных систем связи является анализ временных диаграмм сигналов, передаваемых в канале связи.

Целью данной статьи является качественный анализ защищенности распространенной системы связи, основанной на методе переключения хаотических режимов.

В настоящее время одной из самых распространенных систем связи на основе хаотических сигналов является система связи, основанная переключение хаотических режимов [4.]. В простейшем случае она основана на использовании наличия или отсутствия хаотического импульса на информационной позиции (chaotic on-off keying – далее «COOK») [5]: на временной оси выделяются позиции, присутствие импульса на которых означает, что передается «1», а отсутствие импульса – передачу «0» (рис. 1).

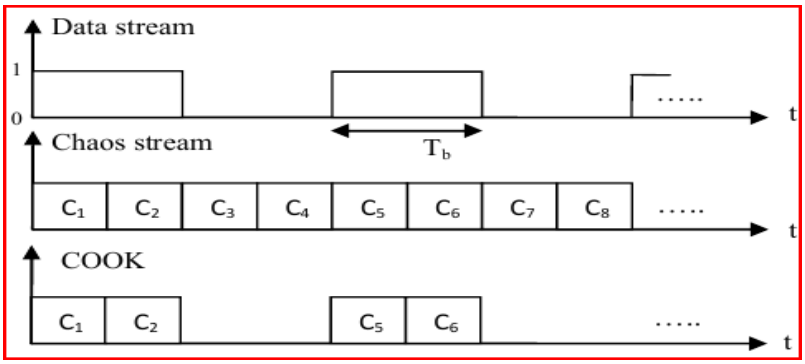


Рис. 1. Схема, поясняющая основные принципы работы системы связи COOK

Обобщенная схема передатчика и приемника системы связи COOK приведены ниже (рис. 2, 3) [5]:

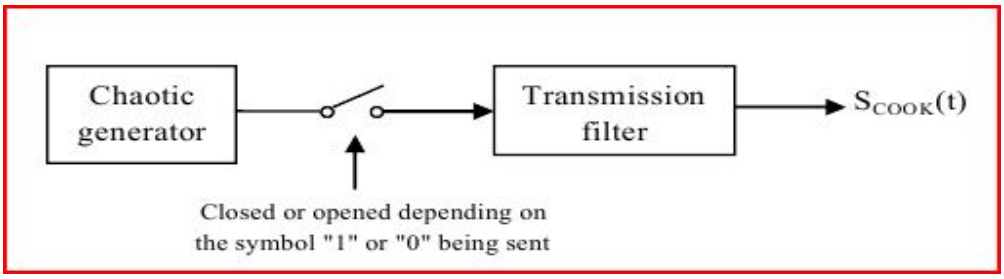


Рис. 2. Схема передатчика системы связи COOK

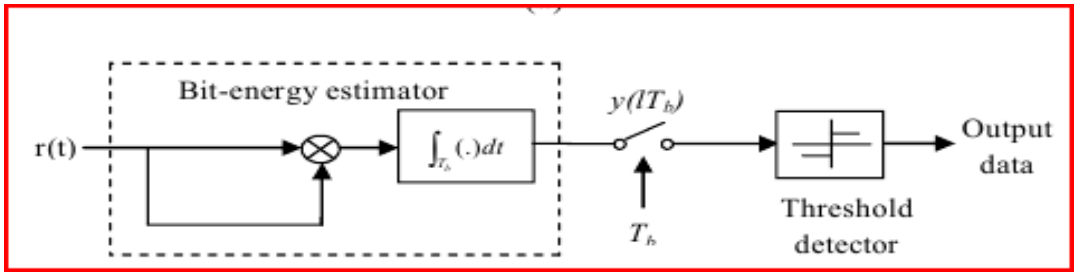


Рис. 3. Схема приемника системы связи COOK

Для качественного анализа системы связи COOK обратимся к известной литературе. Так известно множество имитационных моделей данной системы связи с использование различных генераторов хаотических сигналов. На рис. 4 приведены временная диаграмма исходного информационного сигнала и соответствующая ей временная диаграмма сигнала в канале связи, созданная с помощью кусочно-линейного отображения [5].

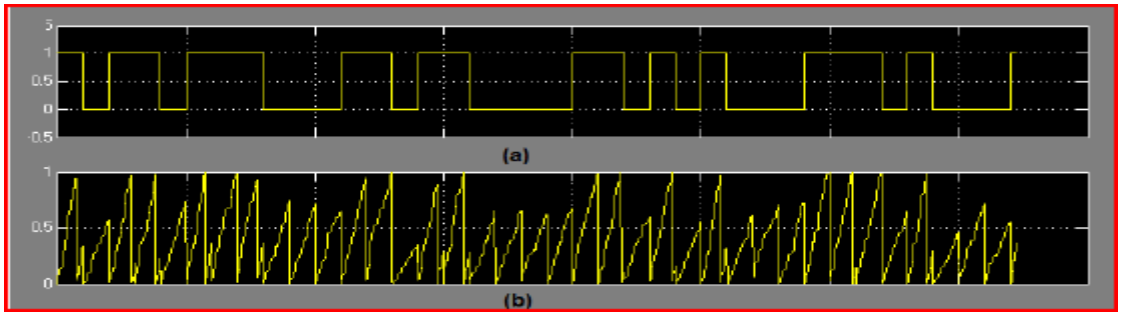


Рис 4. Временная диаграмма исходного информационного сигнала (a) и соответствующая ей временная диаграмма сигнала в канале связи (b), созданная с помощью кусочно-линейного отображения

На рис. 5, 6 приведены временная диаграмма исходного информационного сигнала и соответствующая ей временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Хенона [6].

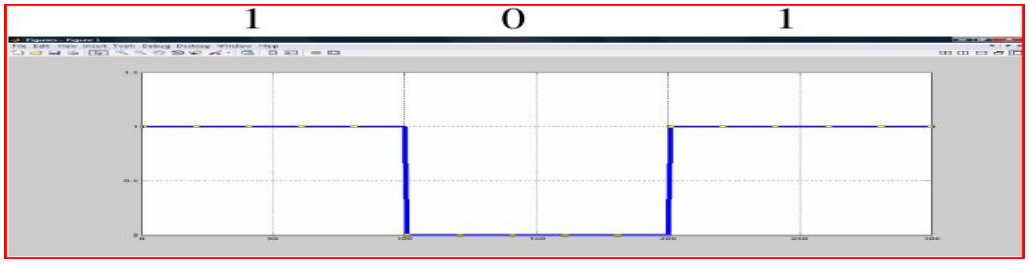


Рис. 5. Временная диаграмма исходного информационного сигнала

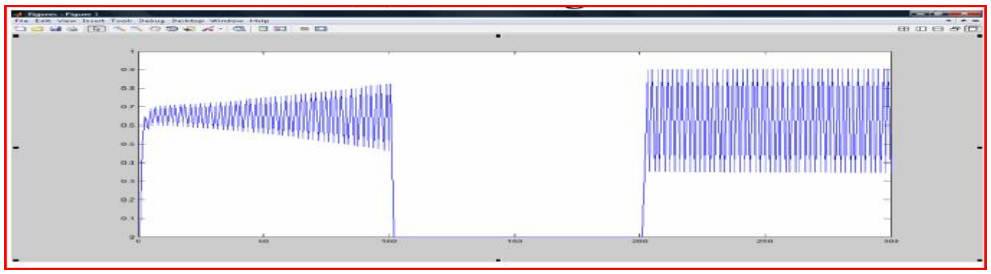


Рис. 6. Соответствующая рис. 5 временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Хенона

На рис. 7, 8 приведены временная диаграмма исходного информационного сигнала и соответствующая ей временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Лоренца [7].

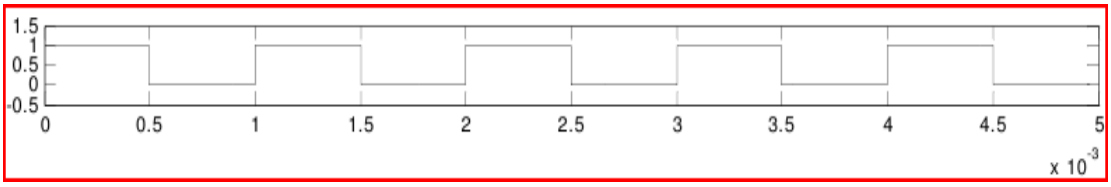


Рис. 7. Временная диаграмма исходного информационного сигнала

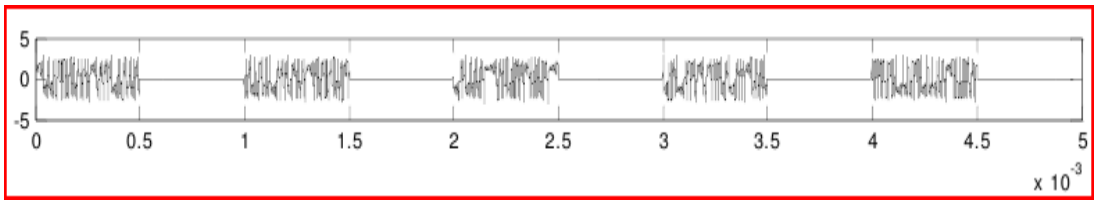


Рис. 8. Соответствующая рис. 7 временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Лоренца

На рис. 9, 10 приведены временная диаграмма исходного информационного сигнала и соответствующая ей временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Чуа [8].

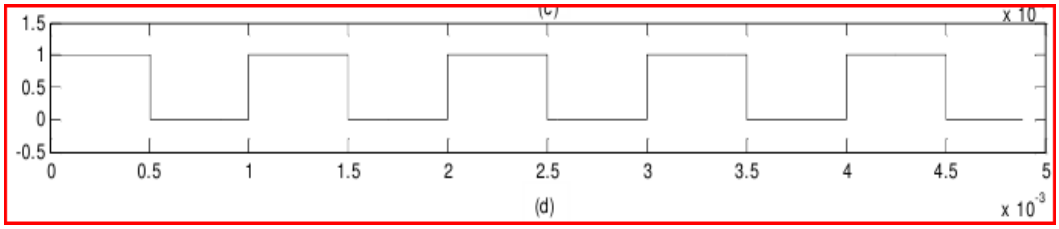


Рис. 9. Временная диаграмма исходного информационного сигнала

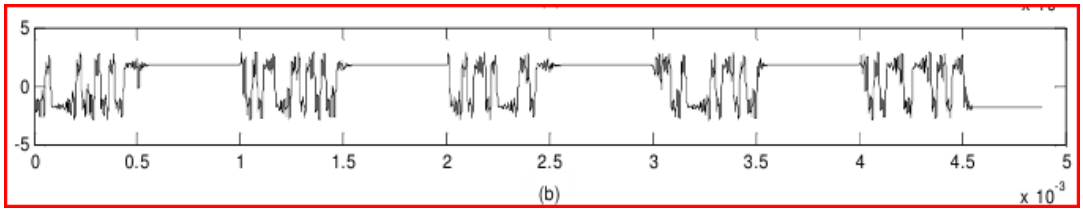


Рис. 10. Соответствующая рис. 9 временная диаграмма сигнала в канале связи, созданная с помощью аттрактора Чуа

На рис. 11, 12 приведены временная диаграмма исходного информационного сигнала и соответствующая ей временная диаграмма сигнала в канале связи, созданная с помощью системы, основанной на гиперхаосе Ци [9].

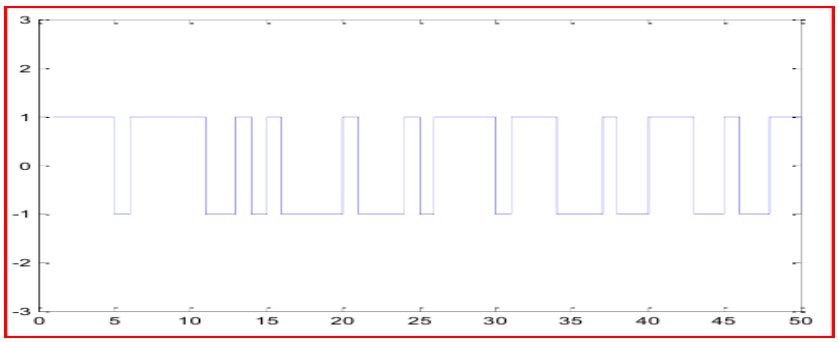


Рис. 11. Временная диаграмма исходного информационного сигнала

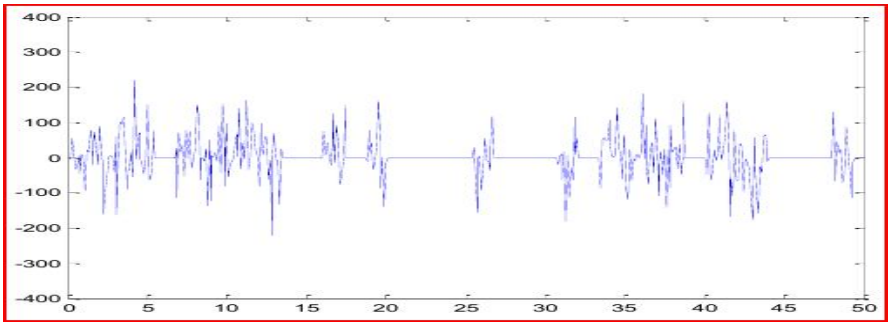


Рис. 12. Соответствующая рис. 11 временная диаграмма сигнала в канале связи, созданная с помощью системы, основанной на гиперхаосе Ци

В работе [10] приведена прямохаотическая система передачи информации, использующая в своем составе систему связи COOK (рис. 13). В ее состав входят [10]: 1 – сверхширополосный генератор хаотических сигналов, 2 – модулятор, 3 и 7 – СВЧ-усилители, 4 – источник цифровых управляющих сигналов, 5 и 6 – передающая и приемная сверхширокополосные антенны, 8 – демодулятор, 9 – осциллограф. Модуляция/демодуляция осуществляется на основе системы связи COOK.

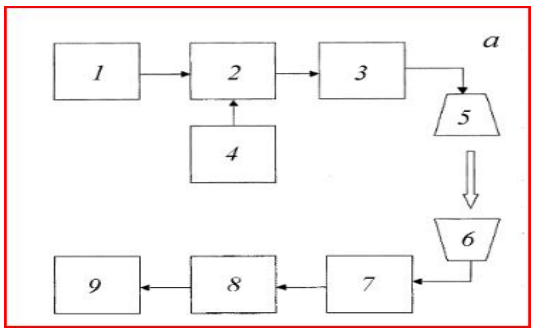


Рис. 13. Схема прямохаотической системы передачи информации

В качестве генератора хаотических сигналов для прямохаотической системы передачи информации был использован специально разработанный генератор, состоящий из трех биполряных СВЧ-транзисторов и двух частотно-избирательных цепей. На рис. 14 показана временная диаграмма, на которой вверху изображено формирование потока хаотических радиоимпульсов при передаче информации, а внизу – исходной информационной последовательности [10].

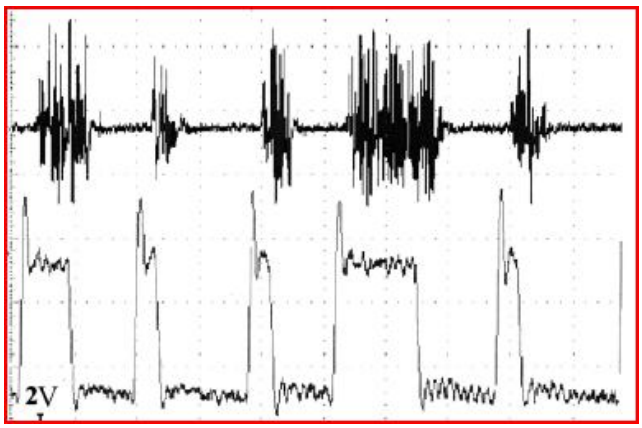


Рис. 14. Временная диаграмма потока хаотических радиоимпульсов в канале связи (сверху) и соответствующей исходной информационной последовательности (внизу)

Как видно из приведенных временных диаграмм сигналов в канале связи (рис. 4b, 6, 8, 10, 12, 14), отличительной чертой системы связи COOK при использовании различных генераторов хаотических сигналов является наличие пауз между передаваемыми в канале связи сигналами. Однако наличие пауз при передаче информации хаотическим сигналом позволяет условному противнику восстанавливать моменты перехода из единицы в минус единицу и обратно, используя энергетический приемник, состоящий из квадратора и интегратора (рис. 15) [9, 11]. Опишем более подробно, как происходит процесс восстановления исходного информационного сигнала системы связи COOK [9, 11].

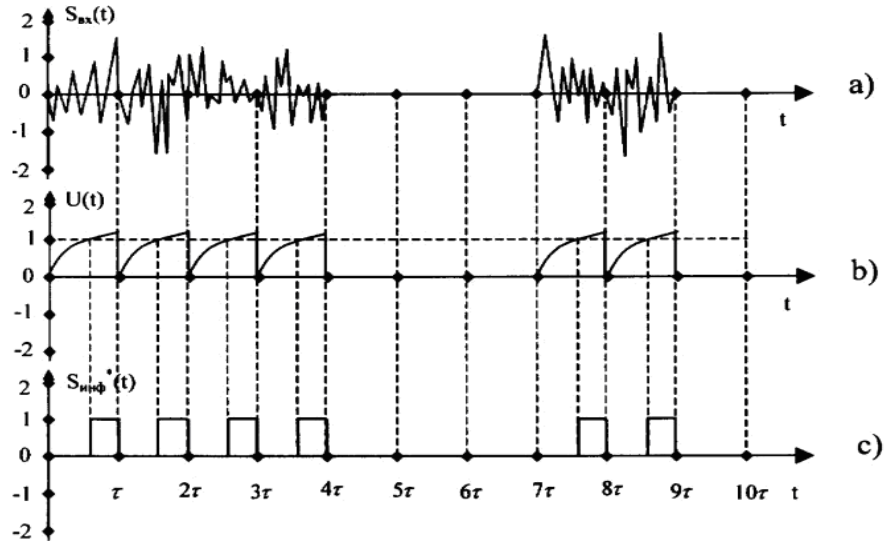


Рис. 15. Временные диаграммы, поясняющие принцип работы энергетического приемника, на вход которого поступает сигнал, сформированный системой связи COOK

В случае если хаотический сигнал, используемый системой связи COOK (рис. 15), поступает на вход энергетического приемника (не показан), состоящего из диода и интегратора, путем интегрирования (накопления) мощности принятых импульсов в пределах их длительности, то на его выходе будет выделяться сигнал (рис. 15b), необходимый для принятия решения пороговым устройством. С выхода порогового устройства на вход декодера поступают импульсы (рис. 15c) длительностью, равной длительности превышения интегрированного сигнала над пороговым уровнем. С поступившего на вход энергетического приемника сигнала (рис. 15a) происходит выделение полезной информации (рис. 15c), при этом наличию импульса на заданной позиции в потоке информации соответствует передаваемая единица, а отсутствию импульса – символ минус единица [11]. Условный противник может восстановить структуру сигнала-переносчика, что свидетельствует о низкой структурной и информационной скрытности системы связи COOK [9, 11]. Таким образом, система связи COOK не обладает достаточным уровнем защищенности от несанкционированного доступа.

Вывод

Таким образом, в данной работе был проведен качественный анализ защищенности распространенной системы связи, основанной на методе переключения хаотических режимов – системы связи COOK. Были показаны обобщенные схемы передатчика и приемника системы связи COOK, показан принцип работы данной системы связи. Были рассмотрены различные литературные источники, в которых описано множество имитационных моделей данной системы связи с использование различных генераторов хаотических сигналов. В результате качественного анализа, представляющего собой исследование временных диаграмм исходного информационного сигнала и сигнала,

передаваемого в канале связи, было установлено, что отличительной чертой системы связи СООК, при использовании различных генераторов хаотических сигналов, является наличие пауз между передаваемыми в канале связи сигналами. Данное обстоятельство позволяет условному противнику восстанавливать моменты перехода из единицы в минус единицу и обратно, используя энергетический приемник, состоящий из квадратора и интегратора (рис. 15). Условный противник может восстановить структуру сигнала-переносчика, что свидетельствует о низкой структурной и информационной скрытности системы связи СООК [9, 11]. Таким образом, система связи СООК не обладает достаточным уровнем защищенности от несанкционированного доступа.

Для повышения структурной и информационной скрытности сигналов-переносчиков защищенных систем связи на основе хаотических сигналов, например, можно воспользоваться принципами, положенными в основу устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков [12]. В основу данных принципов положено использование на передающей и приемной сторонах перезаписываемых накопителей хаотических последовательностей (в которых содержаться одинаковые хаотические последовательности), в которые потенциально возможно записать бесконечное количество различных уникальных хаотических реализаций, что потенциально может повысить, как структурную, так и информационную скрытность передаваемых сигналов [2, 11, 12]. Так же в предлагаемом подходе передаваемые в канале связи сигналы, в отличие от системы связи СООК, имеют на временных диаграммах сплошной (без пауз) непрерывный вид [2, 3]. Таким образом, использование для них энергетического приемника является малоэффективным.

Литература:

1. Леонов К.Н., Потапов А.А., Ушаков П.А. Математическое моделирование системы передачи информации на основе хаотических сигналов с фрактальной размерностью // Физика волновых процессов и радиотехнические системы. 2010. Т. 13. № 3. С. 47–53.

2. Гавришев А.А., Жук А.П. Применение методов нелинейной динамики для исследования хаотичности сигналов- переносчиков защищенных систем связи на основе динамического хаоса // Вестник НГУ. Серия: Информационные технологии. 2018. Т. 16. № 1. С. 50-60.

3. Гавришев А.А., Жук А.П. Применение пакета программ ScicosLab в учебных целях для качественного анализа защищенности беспроводных систем связи // Дистанционное и виртуальное обучение. 2018. № 1. С. 94-104.

4. Xiangjun Wu, Zhengye Fu, Jurgen K. A secure communication scheme based generalized function projective sunchronization of new 5D hyperchaotic system // Physica Scipra. 2015. no. 90. 12 p.

5. Hikmat N. Abdullah, Alejandro A. Valenzuela Efficient chaotic communication system for wireless sensing applications // 9th International Multi-Conference on Systems, Signals and Devices. 2012. 5 p.

6. Anchan Dikshith, Sudha K. L. Secure chaotic modulation schemes using henon map // Elixir Comp. Sci. & Engg. 2011. no. 38. pp. 4496-4499.

7. Kamil I.A., Fakolujo O.A. Lorenz-Based Chaotic Secure Communication Schemes // Ubiquitous Computing and Communication Journal. 2012. vol. 7. no 2. pp. 1248-1254.

8. Kamil I.A., Fakolujo O.A. Chaotic Secure Communication Schemes employing Circuit Chua's // 17th International Conference on Systems, Signals and Image Processing. 2010. 4 p.

9. Denis Luke Owour, Guoyuan Qi Secure communication based on Qi hyper-chaos // International journal of new computer architectures and their application. 2012. no. 2(1). pp. 70-80.

10. Дмитриев А.С., Кяргинский Б.Е., Панас А.И., Пузиков Д.Ю., Старков С.О. Сверхширокополосная прямохаотическая передача информации в СВЧ-диапазоне // Письма в ЖТФ. 2003. Т. 29. В. 2. С. 70-76.

11. Баркетов С.В., Жук А.П., Сазонов В.В., Авдеенко С.И., Жук Е.П., Лохов В.И., Голубь Ю.С. Когерентная система передачи информации хаотическими сигналами // Патент РФ № 2326500. 2008. 6 с.

12. Осипов Д.Л., Жук А.П., Гавришев А.А. Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Патент РФ № 2560824. 2015. 15 с.

Грицинин А.С., Жданов С.А.

Институт компьютерных технологий и информационной безопасности

Инженерно-технологическая академия г. Таганрог

РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА ДЛЯ АНАЛИЗА УГРОЗ И УЯЗВИМОСТЕЙ КОМПЬЮТЕРНОЙ СЕТИ

В настоящее время очевидным фактором обеспечения устойчивости деятельности многих организаций, в частности непрерывности бизнеса, стало состояние информационной безопасности их систем управления. Используемые современные вычислительные сети организаций содержат множество критичных узлов и сервисов, нарушение доступности и целостности которых может привести к нанесению значительного ущерба [1]. Поэтому высокая защищенность сетей от угроз информационной безопасности приобретает все большую актуальность и требует для практической реализации все большее количество ресурсов [2].

Возникает потребность в обучении специально подготовленных кадров, владеющих практическими навыками. Актуальность работы заключается в том, что стенд для проведения практических работ, лабораторных занятий и ознакомления студентов с различными видами атак максимально приближен к реальным информационным системам.

Для решения этой проблемы в рамках нашего университета, была выдвинута и одобрена идея создания лабораторного стенда для анализа угроз и уязвимостей компьютерной сети. В дальнейшем данный стенд планируется использовать в ходе лабораторных работ студентами ИКТИБ ЮФУ.

Начало работы

Целью создания стенда является создание набора образов виртуальных машин со встроенными уязвимостями.

Цель конкретизируется задачами:

1. Сбор информации.

Стенд должен имитировать реальные информационные системы, которые используются в государственных информационных системах. Был проведен анализ различных государственных информационных систем и определено, что для их создания используются решения на основе виртуализации, используется операционная система CentOS и гипервизор KVM [3].

Также популярным решением становится Astra Linux, которая как заверяет разработчик: «предназначена для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию до степени секретности "совершенно секретно" включительно» и сертифицирована основными сертификатами соответствия требованиям безопасности информации, такими как «ФСТЭК России», «ФСБ России», «Министерство Обороны России» и «институтом системного программирования им. В.П. Иванникова» [4] .

Операционные системы windows также были добавлены в наш стенд, хоть они и не сертифицированы, но так же активно используются многими пользователями и предприятиями

2. Разработка лабораторного стенда.

Для разработки был выделен сервер, со следующими характеристиками:

- Процессор Intel Core i7 (Broadwell) (с интегрированным графическим ядром) - 2 шт;
- Количество встроенных ядер – 32;
- Объём оперативной памяти – 64 гб;
- 2 SSD накопителя по 256 гб;
- 2 сетевых интрефейса;
- GNOME версия 3.22.2;
- Тип ОС 64-бит.

В качестве основной системы выбрана “CentOS 7”. Преимущества Centos 7 над другими операционными системами:

- CentOS, которая основана на Red Hat, тщательно тестируется перед тем, как выйти в свет. Большинство ошибок исправлено;
- Относительна стабильна, по сравнению с другими ОС;
- Предустановлено много полезных программ;
- Прост в использовании, особенно для новичков;
- При установке можно выбрать профиль сервера;
- Наличие графического интерфейса.

3. Создание набора образов виртуальных машин со встроенными уязвимостями.

В ходе проведения исследовательской работы для создания набора образов виртуальных машин был выдвинут следующий план действий:

- Подбор актуальных операционных систем используемые на предприятиях;
- Установка на стенде этих образов.

В ходе подбора систем были предложены и одобрены следующие системы:

• семейство Windows NT:
- Windows 7;
- Windows 8;
- Windows 10;
- Windows Server 2008;
- Windows Server 2012.

• Семейство UNIX-подобных операционных систем
- CentOS 7;
- Astra Linux.

4. Настройка, создание сервера виртуализации, настройка маршрутизации, добавление программно-аппаратных средств защиты.

В ходе выполнения курсовой работы была разработана следующая топология сети, представленная на рисунке 1.

Для установки виртуальных машин был выбран гипервизор KVM, так как он дает возможность осуществлять виртуализацию на серверах с операционной системой Linux. Однозначным плюсом является то, что данный гипервизор входит в состав ядра Linux, поэтому он постоянно совершенствуется и обновляется. Процессорный модуль KVM дает ему возможность осуществлять доступ непосредственно к ядру. Благодаря этому можно напрямую управлять файлами виртуальных машин и образами дисков. Для каждой ВМ предназначено индивидуальное пространство.

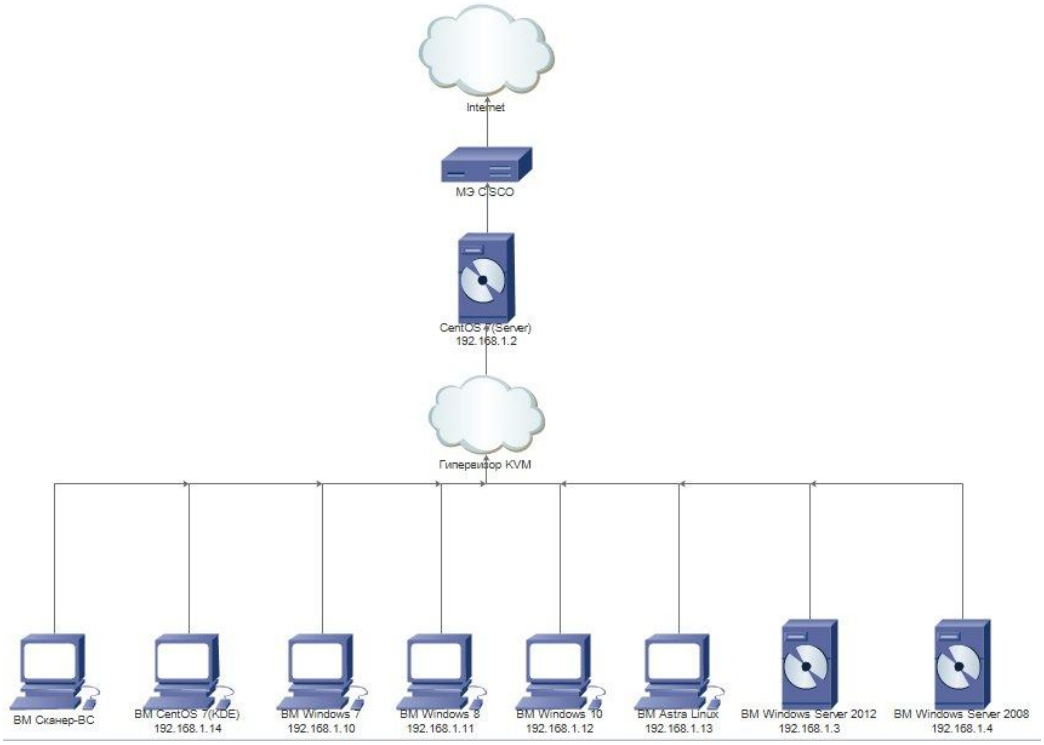


Рис. 1. Схема разработанного стенда

В качестве виртуальных машин были выбраны следующие образы:

• Windows 7;
• Windows 8;
• Windows 10;
• Windows Server 2012;
• Windows Server 2008;
• CentOS 7;
• Astra Linux.

Данные операционные системы выбраны потому, что они наиболее популярны среди пользователей крупных и маленьких предприятий.

На Windows server 2012/2008 были установлены и настроены следующие сервисы:

-DHCP-сервер (для раздачи ip-адресов системам на ядре windows);

Диапазон ip-адресов 192.168.1.10-192.168.1.100.

-DNS-сервер (для связывания доменных имён с цифровыми адресами);

Создали файл «host.local» для проверки доступа к хосту.

-IIS-сервер (для безопасного размещения веб-узлов, служб и приложений);

Отвечает за обработку запросов клиентов к веб-сайту и исполнение скриптов.

На CentOS 7 были установлены и настроены следующие сервисы:

-DHCP-сервер (для раздачи ip-адресов системам на ядре linux);

Диапазон ip-адресов 192.168.1.10-192.168.1.100.

-DNS-сервер (для связывания доменных имён с цифровыми адресами);

Создали файл «local.local» для проверки доступа к хосту.

-FreeRadius (для аутентификации, авторизации и сбора сведений о пользователях);

server = "localhost" # Наименование сервера

port = 3306 # Порт этого сервера

login = "radius"# Логин для подключения(пользователи используют логин, соответствующий названию их машины)

password = "radiuspassword" # Пароль для подключения

Сервер проводит автоматическую авторизацию, путём введения пользователем его логина и пароля. К примеру, пользователю ОС Windows 7 «ARM2» для проведения успешной авторизации нужно ввести свой логин (ARM2) и пароль (Taganrog).

-TFTP-сервер (для передачи файлов между ОС);

На данном сервере нет средств аутентификации пользователей. Используется для передачи файлов. Используется для передачи при загрузке бездисковых рабочих станций, учувствует в процессе резервного копирования и восстановления конфигурации сетевого оборудования.

-Chrony (для синхронизации внутренних часов ОС);

Данный сервер синхронизирует время на рабочих системах, с заданным географическим положением, в данном случае синхронизация происходит по московскому времени.

-SSH-сервер (для удалённой настройки ОС);

Могут использовать только пользователи с правами Администратора. Используется для безопасного удалённого подключения к другим ОС, с целью безопасной работы.

Все системы и сервисы развертывались в KVM виртуализаторе. Так же поднята внутри виртуальной машины виртуальная сеть в режиме «NAT».

Для выхода в интернет используется межсетевой экран Cisco, который осуществляет контроль и фильтрацию проходящего через него трафика в соответствии с заданными правилами.

5. Анализ защищенности информационной системы

В ходе создания, эксплуатации или модернизации информационной системы нередко возникает вопрос об анализе её защищенности от разного рода угроз. Работы по анализу защищенности информационной системы предполагают: обработку большого объема информации об архитектуре, анализ конфигураций сетевого и коммуникационного оборудования, применяемых средств защиты информации, особенностей использования каналов связи и т.д., особенно если информационная система представляет собой сложную многоуровневую и распределенную сетевую структуру [5].

Проведение анализа защищенности информационной системы предоставляет Заказчику объективную информацию, содержащую:

– актуальные и независимые данные о состоянии применяемых технических мер и средств защиты информации;

– рекомендации и варианты технических решений, способных повысить уровень безопасности информационной системы с учетом лучших мировых практик в области защиты информации.

Типовой состав работ, проводимых по анализу защищенности информационных систем включает в себя:

– Проведение инвентаризации применяемых в информационной системе средств вычислительной техники;

– Контроль соответствия конфигураций применяемых средств защиты информации, включая штатные механизмы защиты системного и прикладного программного обеспечения;

– Построение физической и логической схем сетевой инфраструктуры информационной системы;

– Определение взаимосвязей между логической (программное обеспечение) и физической (оборудование) топологией информационной системы;

– Анализ информационных потоков информационной системы;

– Анализ защищенности сетевого периметра;

– Анализ защищенности беспроводной инфраструктуры (при наличии);

– Анализ достаточности/избыточности применяемых средств и механизмов защиты информации;

– Измерения уровня загрузки системных ресурсов программно-аппаратных платформ, определяющих среду функционирования средств защиты информации;

– Измерения уровня загрузки защищенных каналов передачи данных;

– Проведение инструментальных проверок наличия уязвимостей в используемых средствах обработки, хранения и передачи информации.

Для сканирования системы был использован «Сканер ВС» так как он сертифицирован ФСТЭК. Для начала проводится сканирование открытых портов, а затем сканирование на наличие уязвимостей.

Заключение

В ходе проведенной работы был разработан лабораторный стенд, для дальнейшего использования его студентами на практике, а также изучено развёртывание операционных систем, настройка сервисов и настройка виртуальной сети в виртуальной машине.

Работа выполнена при поддержке Гранта РФФИ № 17-07-00106 Разработка метода и эффективной системы защиты беспроводных сенсорных сетей от активных атак злоумышленников.

Литература:

1. Киверина Н.Ш. Анализ уязвимости информационной системы. Международный научно - исследовательский журнал. № 5 (36) 2015. с 73-74.

2. Смычёк М.А. Обеспечение информационной безопасности при проектировании технологических сетей связи нефтегазовой отрасли. T-Comm - Телекоммуникации и Транспорт.2018. С. 9-16.

3. Коновалов А.А. Организация системы информационного обеспечения здравоохранения региона. Журнал ПРОБЛЕМЫ СОЦИАЛЬНОЙ ГИГИЕНЫ, ЗДРАВООХРАНЕНИЯ И ИСТОРИИ МЕДИЦИНЫ. Издательство: Издательство «Медицина» (Москва). 2014. С. 33-37.

4. Ищейнов В.Я., Чудинов С.М. К вопросу структуры изучаемой совокупности угроз безопасности информации; Вопросы радиоэлектроники. 2016. № 7. С. 90-92.

5. Димов Э.М., Маслов О.Н., Раков А.С. Управление информационной безопасностью корпорации с применением критериев риска и ожидаемой полезности; Информационные технологии. 2016. Т. 22. № 8. С. 620-627.

Добровольская Н.Ю.

Кубанский государственный университет

АЛГОРИТМИЗАЦИЯ ОБРАБОТКИ МАССИВОВ В ИССЛЕДОВАНИЯХ БАКАЛАВРОВ ПРИКЛАДНОЙ МАТЕМАТИКИ

Современные требования к обучению в высшей школе предполагают не только приобретение профессиональных навыков и умений, но и формирование научно-исследовательских компетенций. Исследовательская работа студентов позволяет систематизировать полученные знания по ряду смежных дисциплин, выделить межпредметные связи, расширить полученные знания в предметной области, сформировать культуру научного мышления [1,2].

В рамках учебной дисциплины «Основы программирования» для бакалавров прикладной математики первого курса рассматривается раздел «Обработка одномерных массивов». Кроме традиционных заданий этого раздела нами в дистанционный компо-

нент дисциплины добавлены задания-исследования по этому разделу. Дистанционный компонент учебных дисциплин поддерживается Средой модульного дистанционного обучения КубГУ (www.moodle.kubsu.ru) и позволяет увеличивать долю самостоятельных и факультативных заданий для студентов [3].

В дистанционном компоненте раздела «Обработка одномерных массивов» нами предлагается следующий формат заданий. После изучения основного учебного материала раздела на лекционных и лабораторных занятиях студенты выполняют задание-исследование. Им необходимо рассмотреть несколько однотипных задач раздела, выделить общие аспекты алгоритмизации, сконструировать обобщенную схему алгоритмического решения задач данного типа. При выполнении задания следует соблюдать структуру исследования: указать цель исследования, определить этапы и сделать выводы. Рассмотрим некоторые предложенные работы.

Исследование бакалавра А. на тему: «Использование обобщенных схем для проверки делимости числа X».

Цель: сформировать умение применять обобщенные схемы для проверки делимости числа X, удовлетворяющих поставленному условию, переходя от частных случаев к общим при помощи использования обобщенных схем.

Изучение раздела «Обработка одномерных массивов» курса «Основы программирования» предполагает следующие базовые знания учащихся:

- умение описывать переменные регулярного типа (массивы);
- навыки организации ввода/вывода элементов массива;
- умение определять свойство делимости числа;
- умение вычислять количество чисел;
- знание цикла с заранее известным числом итераций и цикла с условием (for, while).

Будем называть обобщенной схемой задачи алгоритм определения свойств числа X.

Этапы исследования.

Этап 1. На основе двух однотипных задач, алгоритмы которых используют цикл с заранее известным числом итераций, построим обобщенную схему задачи.

Пример 1. Найти количество четных элементов массива.

```
k=0;
for (i=0; i<n; i++){ if (a[i]%2==0){    k++;    }}       cout<<k<<endl;
```

Пример 2. Найти сумму не кратных трем элементов массива.

```
K=0;
for (i=0; i<n; i++){  if (a[i]%3!=0){    k+=a[i];}}      cout<<k<<endl;
```

Тогда обобщенная схема будет иметь вид:

```
k=0;
for (i=0; i<n; i++){  if Check(a[i], digit, b){ D(op);}} cout<<k<<endl;
```

Здесь Check – обобщенная функция, описывающая свойство параметра – элемента массива. Первый параметр функции – это элемент массива, второй параметр – делитель, третий параметр равен 1, если элемент делится на digit и равен 0, если не делится.

Функция D(op) – обобщенная функция, определяющая операцию либо подсчет количества (op=1), либо подсчет суммы (op=2).

Тогда для примера 1 значения обобщенных функций равно Check(a[i], 2, 1) и D(1), а для примера 2 Check(a[i], 3, 0) и D(2).

Этап 2. Рассмотрим аналогичные решения с использованием цикла с предусловием.

Пример 1. Найти количество четных элементов массива.

```
k=0; i=0;
while ( i<n) { if (a[i]%2==0) k++; i++;}       cout<<k<<endl;
```

Пример 2. Найти сумму не кратных трем элементов массива.

```
k=0; i=0;
while ( i<n) { if (a[i]%3!=0) k+=a[i]; i++;}       cout<<k<<endl;
```

Тогда обобщенная схема будет иметь вид:

```
k=0; i=0;
while ( i<n) {  if Check(a[i], digit, b) D(op); i++;}     cout<<k<<endl;
```

Функции Check и D аналогичны этапу 1.

Этап 3. Сравнение двух обобщенных схем.

Обобщенные схемы, выделенные на первом и втором этапах, работают по времени одинаково и обе достаточно просты для понимания и применения учащимися.

Выводы:

1. Введение обобщенных схем позволяет преподавателю объяснить ученику наглядно на частных случаях, как конструировать функцию для разных условий однотипных задач, переходя к общему случаю.

2. Сравнение обобщенных схем, решающих одну задачу с помощью двух различных конструкций позволяет выбрать наиболее оптимальный и удобный способ решения.

Исследование бакалавра Б. на тему: «Использование обобщенных схем при определении разрядности элемента массива».

Цель: расширить умение выявлять разрядность элемента массива, переходя от частных случаев к общим при помощи обобщенных схем.

Изучение раздела «Обработка одномерных массивов» курса «Основы программирования» предполагает следующие базовые знания учащихся:

- умение описывать переменные регулярного типа (массивы);
- навыки организации ввода/вывода элементов массива;
- умение определять разряд числа;
- умение вычислять количество чисел;
- знание цикла с заранее известным числом итераций и цикла с условием (for, while).

Будем называть обобщенной схемой задачи алгоритм определения свойства элемента массива.

Этапы исследования.

Этап 1. Рассмотрим решения двух однотипных задач. Решения используют цикл с заранее известным числом итераций. Построим обобщенную схему задачи.

Пример 1.

```
k=0;
For (int i=0; i<N; i++) If (a[i] >= 10 && a[i]<100) { k++;}
```

Пример 2.

```
k=0;
For (int i=0; i<N; i++) If (a[i] >= 100 && a[i]<1000) { k++;}
```

Тогда обобщенная схема будет иметь вид:

```
k=0;
For (int i=0; i<N; i++) If Y(x,p) { k++;}
```

Здесь Y(x, p) – обобщенная функция, описывающая разрядность элемента X (двузначность для первого примера и трехзначность для второго примера). X имеет целочисленный тип и является элементом массива. P – разрядность, является натуральным числом.

Рассмотрим примеры значений обобщенной функции Y(a[i] ,2): a[i] >= 10 && a[i]<100 и Y(a[i] ,3): a[i] >= 100 && a[i]<1000. Таким образом, в общем случае формула функции имеет вид:

$X >= 10^p$ && $X<10^{(p+1)}$, где p требуемый разряд числа.

Этап 2. На основе двух примеров, использующих цикл с заранее известным числом итераций, построим обобщенную схему задачи.

Пример 1.

```
k=0; i=0;
While (i<N) { If (a[i] >= 10 && a[i]<100)  { k++;}   i++;}
```

Пример 2.

```
k=0;i=0;
While (i<N) { If (a[i] >= 100 && a[i]<1000) { k++;}  i++;}
```

Тогда обобщенная схема будет иметь вид:

```
k=0;i=0;
While (i<N){ If Y(a[i],p)  { k++;}  i++;}
```

Обобщенная функция Y(x, p) аналогична описанной выше.

Этап 3. Сравнение двух обобщенных схем.

Обобщенные схемы, приведенные в первом и втором этапах, отличаются только структурой организации цикла.

Выводы:

1. Использование обобщенных схем позволяет понять общий алгоритм решения, выделить основные свойства.

2. Сравнение обобщенных схем, решающих однотипную задачу с помощью двух различных операторов цикла показывает, что сама обобщенная функция не зависит от выбора оператора цикла.

Исследования бакалавров показывают, что студенты не только закрепляют навыки программирования базовых конструкций и типовых задач. Выявляются общие признаки и свойства чисел, принципы алгоритмизации той или иной структуры данных, выполняется сравнение и анализ конструкций языка. Подобные исследования определяют систематический подход к изучению алгоритмизации структур данных, формируют исследовательские компетенции у студентов, раскрывают их творческие способности.

Литература:

1. Добровольская Н.Ю., Харченко А.В. Применение информационных технологий в обучении // Актуальные проблемы информационно-правового пространства. – 2017. – С. 28-31.

2. Добровольская Н.Ю. Формирование умения формального исполнения алгоритма как основы алгоритмических навыков учащихся // Преподавание математики и информатики в школе и вузе. – 2017. – С. 56-58.

3. Харченко А.В. Опыт творческой педагогической деятельности при конструировании учебных задач на основе фасетной технологии // Проблемы современного педагогического образования. – 2017. – № 57-2. – С. 265-272.

Домбровская Л.А., Васютина Т.Л., Сударев В.С.
Санкт-Петербургский университет МВД России

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации в информационных системах в большей мере основывается на человеческих отношениях. В комплексной системе защиты информации организации человек является самым слабым звеном. Находясь в коллективе, человек – пользователь компьютерной системы, неизбежно вступает в межличностные отношения, которые зачастую полны противоречий [1]. На них влияют как собственное здоровье и

общее жизненное состояние, так и сложившаяся психологическая ситуация в трудовом коллективе, отношения с руководством, реальные производственные проблемы. Возникающие конфликты могут послужить мотивом совершения компьютерных преступлений. Обиженные, не удовлетворенные работой и жизнью сотрудники по-разному пытаются избавиться от внутреннего дискомфорта. Тем более, если в результате разрешения каких-либо конфликтов последовали по отношению к пользователю реальные меры со стороны руководства: выговор, предупреждение, увольнение. В таких случаях под влиянием эмоций со стороны пользователя можно ожидать таких действий как месть и вредительство, утаивание, искажение или уничтожение информации и т.д.

Однако в настоящее время исследователи приходят к мнению, что в некоторых случаях конфликты в рабочем коллективе полезны, если они поддерживают здоровый дух соперничества и в малой степени оказывают негативное влияние на состояние и работоспособность его членов в целом. Руководителям надо не только вести работу на предотвращение конфликтов, но поддерживать социально-психологическую обстановку в коллективе.

Рассмотрим некоторые типы конфликтов в организациях.

1. Конфликты, обусловленные требованиями режима

Требования режима, которые всегда носят ограничительный характер при работе с определенной информацией, заставляют пользователей искать возможности компенсации неудовлетворенных потребностей. Негативно влияют на моральное самочувствие человека требования на запрет выезда за границу, на публикацию научных работ и выступления на конференциях. Кроме того, работа в специальных маленьких экранированных комнатах без окон, где используются генераторы помех, экранирование, может оказывать отрицательное воздействие и на психофизиологические качества сотрудников, а в целом и на его профессиональные действия.

Для нивелирования последствий от режимных требований рекомендуется:

– проанализировать объем режимной информации и возможности его сокращения;

– контролировать время работы в специализированных помещениях и не допускать превышения в соответствии с имеющимися инструкциями;

– предусматривать меры поощрения работников, работающих с режимной информацией и другие.

2. Конфликты, обусловленные несоответствием ожиданий и реальности, конфликты «несбывшихся надежд»

На фоне неудовлетворенности своих важных потребностей и целей в части карьеры и успеха, условий труда и уровня зарплаты, достойного места в коллективе у человека возникает стресс, желание не выполнять требования режима, непредсказуемые поступки под воздействием эмоций, чувство мести.

Для нейтрализации подобных конфликтов рекомендуется:

– создание определенного порядка приема на работу, включающего информирование претендента о реальных условиях работы, перспективах и ограничениях, накладываемых на него при получении работы; подписание обязательства о неразглашении конфиденциальной информации, даже в случае увольнения;

– четкое разграничение ответственности и состава работ (например, ознакомление с должностной инструкцией);

– контроль трудовых результатов, учитываемых при продвижении сотрудников по служебной лестнице.

3. Конфликты «человек – система защиты»

Важнейшими причинами из-за которым персонал уклоняется от использования инструкций системы безопасности, являются: большой их объем, противоречивость положений друг другу или реальным условиям работы; сравнительная редкость злого

умысла, в результате которого сотрудники не видят серьезных причин следования инструкциям; отсутствие или ограниченность своего негативного опыта, первое же столкновение сотрудника с атакой на защищаемые данные бывает реальной; отказ руководящего состава учитывать специфику работы отдельных сотрудников и подразделений в виде оплаты, что приводит к восприятию некоторых требований как дополнительной неоплачиваемой работы. Кроме того, часть пользователей противопоставляют себя системе безопасности, показывая свое превосходство умением обойти режимные требования, т.е. действуют как хакеры.

Рекомендации:

– формирование требований и правил в форме, удобной для восприятия; акцент на тех пунктах, нарушение которых связано с особо тяжкими последствиями, а также отдельное выделение пунктов, чаще нарушаемых; ликвидация дублирования, обоснование правил;

– стимулирование: материальное, социальное, при необходимости - отрицательное (порицание, наказание);

– воспитательная работа: печатные издания, плакаты, газеты, доклады, беседы, коллективное обсуждение вопросов безопасности.

Конфликты, обусловленные ограниченностью ресурсов

Конфликты, вызванные ограниченностью ресурсов (вычислительных или информационных) возникают и между отделами организации, и между сотрудниками. Такого рода конфликты приводят к образованию слухов, антагонизму интересов, мешают инициативному сотрудничеству.

В таких случаях рекомендуется:

– организация четкой информационной политики, корректное ведение дел, соблюдение дистанции в общении с сотрудниками, грамотная мотивация;

– формирование общей целевой политики организации, понимания ее престижа;

– формирование понятной системы поощрения в зависимости от результатов работы.

Конфликты, обусловленные несоответствием целей сотрудников системы защиты информации и других работников и отделов.

Конфликты возникают из-за того, что службы защиты информации (СИБ) относятся к вспомогательным, обслуживающим подразделениям. В то же время они определяются руководителем организации, сотрудники этой службы имеют определенные права, в том числе контролирующие[2]. Контроль со стороны службы информационной безопасности вызывает раздражение у специалистов-пользователей. Помогут избежать подобных конфликтов следующие рекомендации:

– формирование общих целей и ценностей, налаживание коммуникаций;

– разъяснение политики безопасности организации и роли службы безопасности в ее реализации;

– включение в критерии материального поощрения взаимозависимые показатели сотрудников СИБ и сотрудников-пользователей;

– учет предложений других отделов по совершенствованию системы защиты информации;

– замена прямого контроля со стороны СИБ сбором и анализом статистической информации (где это возможно);

– проведение совместных тренингов по возможным критическим ситуациям.

Конфликты иерархии

Конфликты иерархии принято различать по следующим видам:

1. Конфликт «равный – равный» проявляется в конкуренции между сотрудниками.

2. Конфликт «высший – низший» характеризуется стремлением усилить власть над подчиненными и – напротив – сохранить и увеличить свою автономию.

3. Конфликт «формальной и неформальной структур» (формальный руководитель и неформальный лидер) реализуется борьбой за власть.

Рекомендации:

– изменение руководящей структуры, по возможности установление более «горизонтальных» связей при сохранении централизованных решений по стратегическим направлениям деятельности организации;

– грамотная кадровая политика в организации и подразделениях;

– делегирование ответственности (по возможности) неформальным лидерам;

– более четкая организация работ, постановки служебных задач, разграничения прав и обязанностей между сотрудниками;

– формирование здорового психологического климата и духа соревнования в коллективах;

Конфликты «человек – машина»

Управление современными техническими устройствами требует от пользователя определенных профессиональных и психофизиологических качеств [3]. Если эргономические характеристики не соответствуют возможностям восприятия человека, возникает конфликт «человек - машина» [4]. Такой конфликт происходит также, если у сотрудника не хватает знаний и умений по обслуживанию, использованию технических средств. Например, неумение работы на компьютере, незнание возможностей программного обеспечения и т.п. приводят к страху совершить ту или иную ошибку, снижению качества труда.

В таких случаях рекомендуется:

– профессиональный отбор, обучение и тренировки;

– установление рационального режима труда и отдыха сотрудников, перерывов для отдыха в работе;

– установление переменной нагрузки (например, темпа подачи и количества перерабатываемой информации и т. п.) в соответствии с динамикой работоспособности человека;

– чередование различных по содержанию или форме деятельности заданий в течение рабочего дня;

– организация наставничества.

Литература:

1. Васютина Т.Л., Стахно Р.Е. Применение современных информационных технологий в обучении // Проблемы современной науки и образования. 2016. № 7. С. 52-54.

2. Парфенов Н.П., Стахно Р.Е. Технология защиты персональных данных // Наука, техника и образование. 2016. № 4. С. 15-16.

3. Стахно Р.Е., Гончар А.А. Защита информации в современном документообороте // Наука, техника и образование. 2016. № 4. С. 19-21.

4. Алексеев С.А. Технология эргономического обеспечения проектирования АРМ интегрированной автоматизированной системы управления / Известия вузов. «Приборостроение» 2009 № 9 С.6 – 11.

Дусева Н.Ю.
Волгоградская академия МВД России

КРИТЕРИИ ОЦЕНКИ КАЧЕСТВА ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Современный образовательный процесс предполагает активное использование компьютерных и сетевых технологий. К общей проблеме всех образовательных организаций, обеспечивающих обучение в электронной форме, можно отнести проблему оценки качества, как программ электронного обучения, так и оценки результатов электронного обучения. При этом в определение понятия качества электронного обучения включены следующие критерии оценивания образования в традиционной форме:

– качество образовательных технологий (качество электронных образовательных ресурсов);

– качество содержания образования;

– качество результатов образования (качество образованности личности) [1].

При оценке качества электронного образовательного ресурса (ЭОР) необходимо выделить специфичность данного вида образовательных ресурсов. При использования электронных образовательных ресурсов необходимым условием является наличие определенного программно-технический комплекса, который реализует использование различных видов представления информации: текстовой, аудио-, фото-, видео-, графической, анимации. Следовательно экспертиза качества ЭОР будет существенно отличаться от экспертизы средств традиционного обучения.

Оценку качества разработанного электронного образовательного продукта производят как по традиционным критериям, так и с точки зрения соответствия основным характеристикам электронного обучения. К традиционным критериям можно отнести:

– соответствие примерной программе учебной дисциплины (соответствие содержания образовательного ресурса требованиям изучения дисциплины согласно ФГОСу);

– преемственность и взаимосогласованность (изложение учебного материала с учетом предшествующих тем);

– практичность (возможность использования разнообразных приемов и методов обучения, адекватных содержанию обучения);

– стилистика изложения (системность, последовательность изложения, однозначное значение употребляемых терминов, нормы современного русского языка);

– содержательность (наглядность образовательного продукта и наличие справочно-сопроводительного аппарата);

– информативность (актуальность, правильность, точность приводимых сведений, ориентация на возрастную группу) [2].

К специфическим критериям, применяемым при оценке качества ЭОР, необходимо отнести следующие:

– «дружественность» интерфейса (восприятие обучающимся цветовых образов на ахроматическом фоне);

– качество компьютерных тестов (формат контента позволяет обмениваться тестовыми заданиями, гарантируя их неизменность и однозначную трактовку);

– качество компьютерных лабораторных работ (обеспечение мультимедийного интерфейса обучающегося);

– качество компьютерных имитационных тренажеров (соответствие имитируемой модели оборудования и выполняемых операций требованиям ФГОСа и адекватная система контроля и оценки действий пользователя);

–качество мультимедиа сопровождения (форматы представления видео- и аудиосопровождения) [3].

К методам комплексной оценки качества средств ЭОР, используемых в обучении относятся апробация и экспертиза [4].

Апробации образовательных электронных изданий и ресурсов происходит путем непосредственного использования в процессе обучения через демонстрацию и обсуждение этих средств информатизации обучения на конференциях, семинарах, выставках, презентациях и других общественных мероприятиях. Процесс апробации и последующего совершенствования образовательных электронных изданий и ресурсов носит итеративный циклический характер и должен продолжаться до полного достижения средством информатизации соответствия требованиям качества.

Апробация образовательных электронных изданий и ресурсов в учебном процессе предполагает наличие экспериментальной группы обучающихся с различной степенью успеваемости. В целях повышения точности оценки в апробации может принимать участие несколько экспериментальных групп.

Использованию образовательного электронного издания при проведении занятий обязательно должен предшествовать подготовительный этап, заключающийся в ознакомлении обучающихся с изучаемой тематикой и объяснением правил работы с предлагаемым ресурсом. Последующее проведение занятия должно соответствовать методическим указаниям и рекомендациям, сопровождающим конкретную разработку.

В течение проведения апробационного занятия выявляется эффективность усвоения материала, возникающие у обучающихся вопросы, а также фиксируются сбои в работе электронной разработки. После проведенного занятия обобщаются и анализируются все возникшие вопросы и трудности.

Результаты апробации в условиях реального учебного процесса направляются специалистам-разработчикам для принятия мер по совершенствованию электронного издания или ресурса.

Центральным звеном оценки качества образовательных электронных изданий и ресурсов является технология экспертизы. Целью проведения независимой компетентной экспертизы является установление соответствия показателей качества средства информатизации образования заранее определенным требованиям международных, государственных и отраслевых стандартов, нормативно-технических документов и др., а также обеспечение качества и эффективности процесса обучения на основе применения данного ОЭИ.

Единая система экспертизы качества образовательных электронных изданий и ресурсов должна удовлетворять следующим требованиям:

- системный подход к организации экспертизы;
- в качестве экспертов должны выступать специалисты различных направлений, что обеспечит всесторонний анализ ОЭИ;
- экспертиза образовательных электронных изданий и ресурсов должна быть разделена на два этапа: подготовительный и основной;
- в случае изменения и совершенствования ОЭИ, уже прошедшего экспертизу, процедура экспертной оценки качества должна периодически повторяться в полном объеме.

Комплексная экспертиза включает в себя разносторонние экспертизы: технико-технологических, психолого-педагогических и дизайн-эргономических аспектов создания и использования образовательных электронных изданий и ресурсов.

Таким образом, оценка качества электронного обучения является сложной и актуальной на сегодняшний день задачей, решение которой видится в многоаспектном анализе электронных образовательных ресурсов, а также в глубокой и разносторонней оценке результатов электронного обучения.

Литература:

1. Бубнов Г.Г., Плужник Е.В, Солдаткин В.И. Критерии оценки качества в системе электронного обучения // [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/kriterii-otsenki-kachestva-v-sisteme-elektronnogo-obucheniya (дата обращения 20.07.2017).
2. Просветов А.В. Экспертиза электронных учебных изданий и критерии ее качества // Научные исследования в образовании, 2011.
3. Гриценко А.Г. Оценка качества программ электронного обучения: дис. … кандидата эконом. наук: Москва, 2006.
4. Лапенок М.В. Теоретические подходы и практическая оценка качества информационной среды дистанционного обучения // Педагогическое образование в России. № 3. 2012.

Жмурко Д.Ю.
Краснодарский университет МВД России

ЦИКЛИЧЕСКИЙ ГЕНОМ САХАРНОГО ПОДКОМПЛЕКСА АПК

Социоэкономическая генетика имеет дело с закономерностями и механизмами развития социальных и экономических отношений, рыночных механизмов, динамики воспроизводственной структуры, взаимодействия факторов, влияющих на изменения жизненного уровня населения, с причинами и последствиями периодических экономических кризисов разной глубины. Этой сфере уделяли основное внимание А. Смит и Д. Рикардо, К. Маркс и В. Ленин, Н. Кондратьев и А. Богданов, многочисленные современные исследователи. Литература по этим проблемам огромна, однако закономерности социоэкономической генетики во многом не изучены, что порождает изобилие противоречивых рекомендаций [с.86, 5].

При реализации целей важно правильно определить закономерности и механизмы, измерить ритм смены технологических способов производства, технологических укладов, раскрыть кумулятивность и изменчивость в динамике технических систем, энергоисточников, основных материалов, информационных систем, оценить причины, механизмы и последствия волн технических инноваций в любом производстве.

Производством сахара в Мире занимаются порядка 110 стран. Большинство из них вырабатывают сахар из сахарного тростника – 75, из сахарной свеклы – 35, также есть страны, в которых культивируются обе культуры – 11 (рисунок 1).

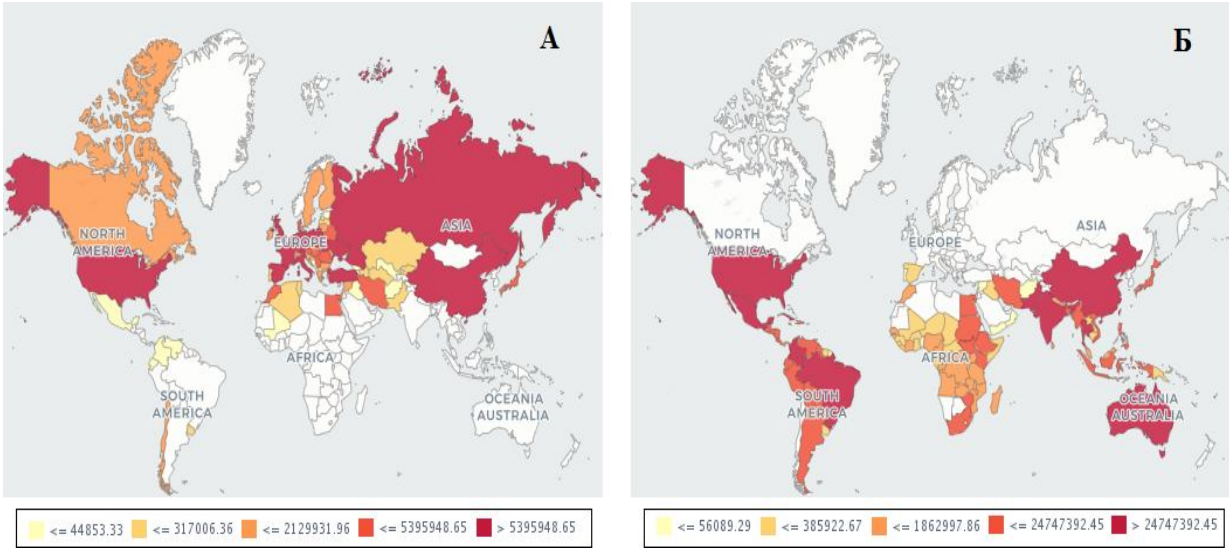


Рис. 1. Ореол производства сахара из:
А – производство сахарной свеклы, Б – производство сахарного тростника

Постановкой задачи исследования является выявление новых закономерностей в виде общих для производелей сахара циклических траекторий, которые позволят более точно прогнозировать деятельность отдельных производственных единиц, региональных участников данного сегмента, так и всего сахарного подкомплекса АПК.

Предметом исследования являются циклы высокой вероятности и периодограммы циклов высокой вероятности (циклические геномы).

В данной статье будет представлена концепция циклов высокой вероятности (*High probability cycles* или ЦВВ). Здесь ключевым моментом является обнаружения циклов высокой вероятности, которые будут получены наряду с постоянными циклами (т.е. с циклами, которые работают одинаково все время). Например, не возможно предположить, что 18-летний цикл всегда будет одинаково работать для всех показателей. Исследования показывают, что циклический профиль постоянно меняется. Например, на сегодня актуален 15-летний цикл, но через сорок лет он исчезнет, и вместо него «наберет» силу возможно новый 13,5-летний цикл. Подобная изменчивость циклов является предметом исследования спектрального преобразования (вейвлет-анализа, форвардного анализа и т. п.).

Любые циклы проявляются как реакция на некоторые фундаментальные события, в нашем случае это экономика сахарного подкомплекса АПК «общается» с «Большим миром».

Поскольку в этом сегменте мировые события отображаются в виде комплекта циклов, необходимо дополнить скорректировать поставленную задачу следующей подзадачей, а именно, выявить циклы сахарного подкомплекса, которые являются реакцией на некие фундаментальные мировые события. Исходя из того, что в различные периоды времени работают разные циклы. Необходимо помнить, что в мире много событий, и сахарный подкомплекс реагирует на его событийность разными циклами (или комплектами циклов).

Поясним концепцию реализации ЦВВ на следующем примере: предположим, что в сахарном подкомплексе периодически наблюдаются циклы в 7, 9, 11.5, 14 лет и т. д. Все эти циклы периодически проявляют себя. Но 7-летний цикл (по какой-то причине, частота проявления этого цикла больше) появляется чаще, чем другие циклы. Это не постоянный цикл (который работает одинаково все время). Этот цикл может появиться несколько раз в истории социально-экономических временных рядов, и не всегда этот цикл в периодограмме можно увидеть. Но, по некоторым причинам, он имеет больше вероятности проявиться в исследуемых ВР по сравнению с циклами 9, 11.5, 14 лет и т. д.

Циклы высокой вероятности будут использоваться как некоторая модель поведения, которая является общей для определенного множества однородных показателей (т. е. одного сегмента экономике АПК, в нашем случае это производство сахарной свеклы, тростника и сахара).

На рисунке 2 показаны периодограммы ЦВВ, выявленные классическим способом, т.е. с помощью спектрального анализа.

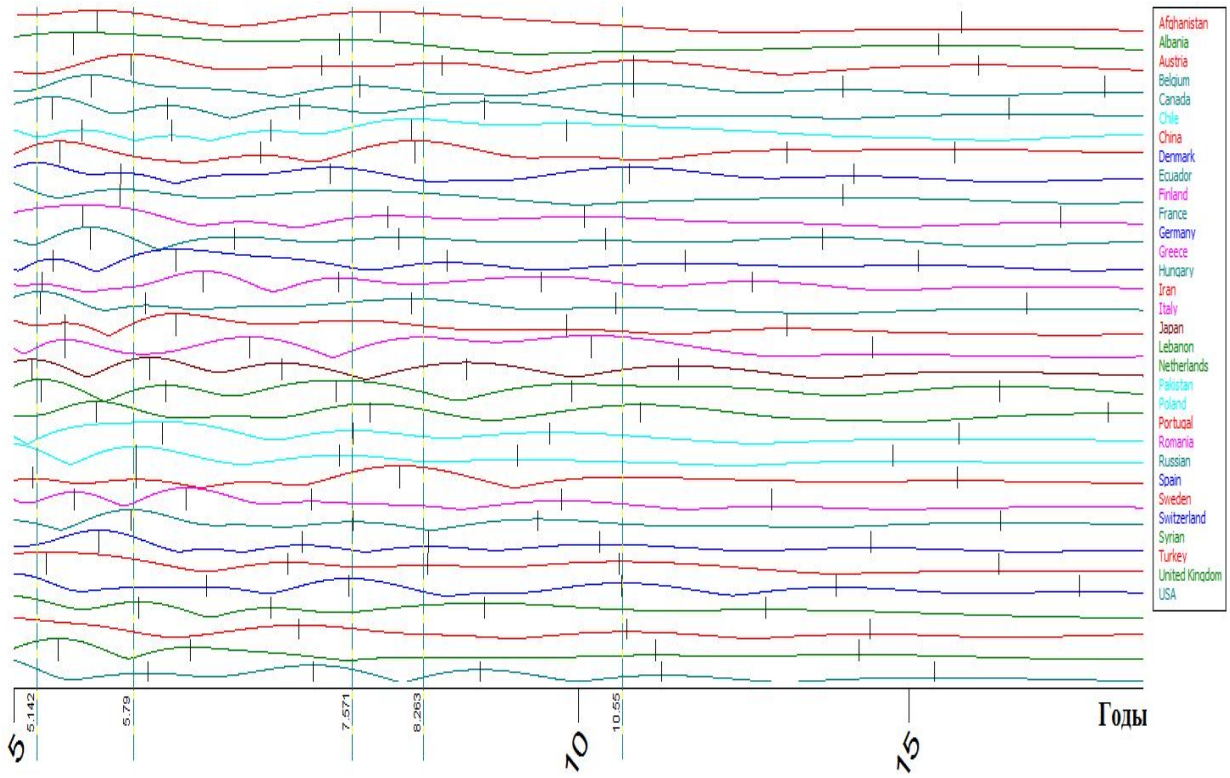


Рис. 2. Спектральная периодограмма циклов высокой вероятности мировой урожайности сахарной свеклы (1961-2017 гг.)

На рисунке 3 показаны периодограммы ЦВВ, выявленные неклассическим способом, т. е. с помощью форвардного анализа.

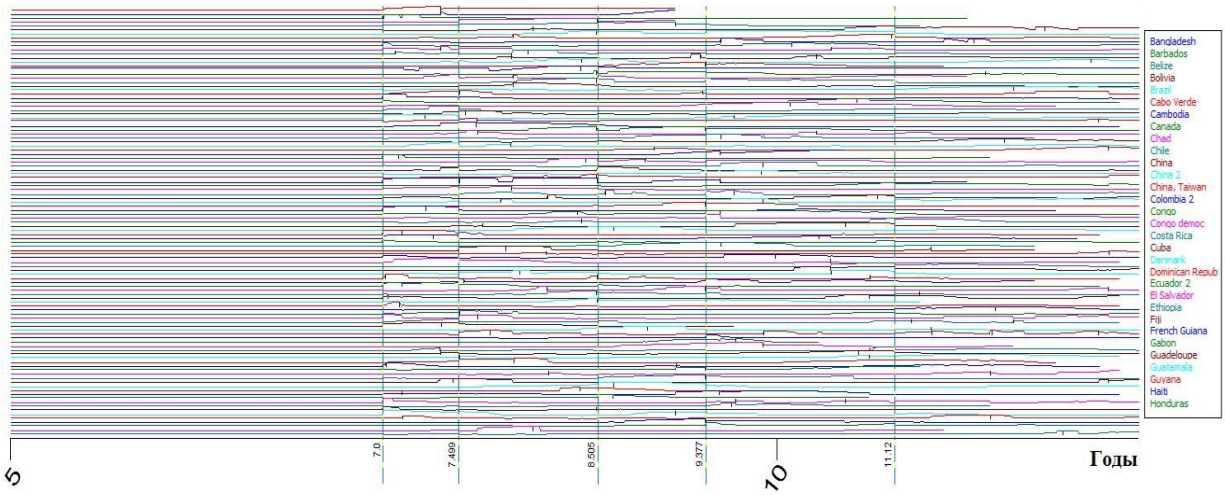


Рис. 3. Форвардная периодограмма циклов высокой вероятности мировой урожайности сахарного тростника (1961-2017 гг.)

На рисунке 4 представлена обобщенная форма в виде единой периодограммы (циклические геномы).

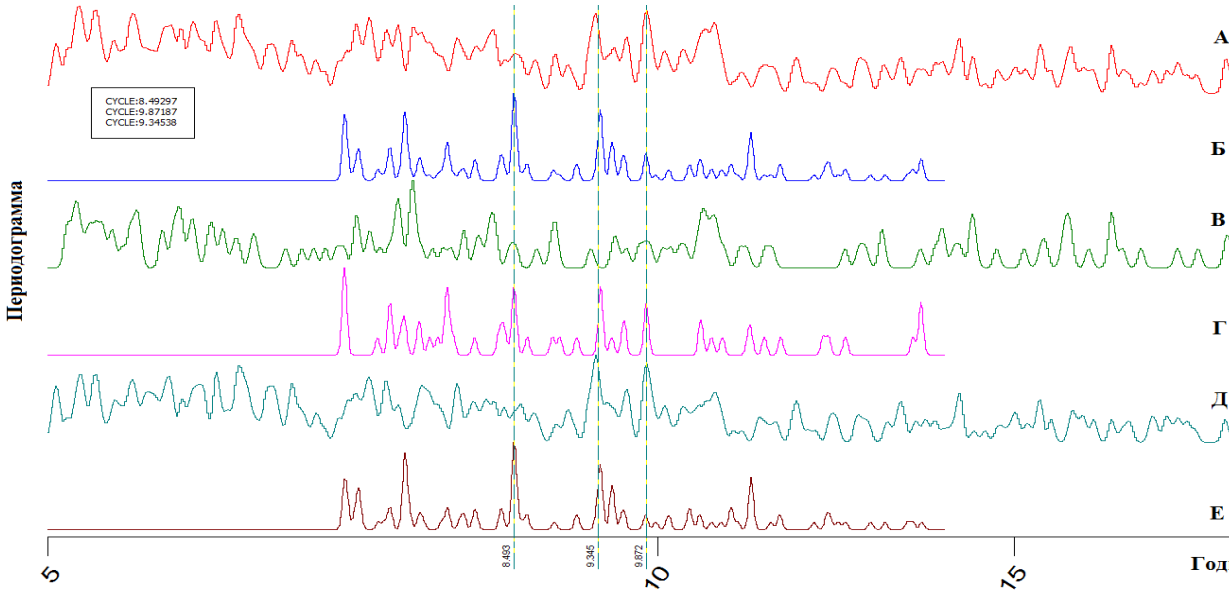


Рис. 4. Циклические геномы урожанойности сахарной свеклы (В и Г) и тростника (Д и Е): А, В и Д – спектральный профиль, Б, Г и Е – форвардный

Примечание. А – это сумма В и Д, Б – сумма Г и Е.

Форвардный и спектральный анализ показывают, как правило, одни и те же циклы, единственное отличие – классический подход выделяет другие циклы (менее значимые).

Спектральный анализ, лет	*Форвардный анализ, лет*
5,1424	7
5,7897	7,489
7,5715	8,505
8,2627	9,377
10,55	11,12

Результаты периодограмм и сводной таблицы указывают на предпочтительность больше к использованию форвардного анализа (т. к. он основан на критериях форвардного анализа) – это ближе к реальной картине исследования. В то время как классический спектр больше связан с подгонкой кривой (стандартная математическая процедура определения активных циклов). Таким образом полученные результаты дают возможность перейти к работе с циклическим геномом.

Циклический геном

Данное исследование показывает, что в настоящее время в сахарном подкомплексе существует порядка 5–6 подобных циклов высокой вероятности. Называется данное множество – периодограммами циклов высокой вероятности (*high probability periodogram*) или циклическим геномом (Cyclic genome, CG). Таким образом, определение циклического генома, если рассматривать с позиции математики – это минимальный набор циклов, который максимально приближенно описывает движения всех исследуемых показателей к эталону. Или минимальный набор циклов, который дает максимальную информацию о движении изучаемого объекта.

В работе для вычисления циклического генома применены специфические математические алгоритмы: был проведен циклический анализ по показателям (398 временным рядам) относящимся к сахарному подкомплексу, извлечены наиболее важные циклы и проведена их кластеризация. Чтобы выявить эти кластеры, данные по ним сведены в общую гистограмму, которая позволяет выявить зоны циклов высокой вероятности.

Такая спектрограмма называется высокочастотной периодограммой. Периодограмма циклов высокой вероятности может использоваться так же, как и в классическом циклическом анализе, т. е. она позволяет выявлять наиболее существенные циклы. Отличие только в одном, высокочастотная периодограмма позволяет одновременно проводить циклический анализ сразу для многих ВР (рисунок 5).

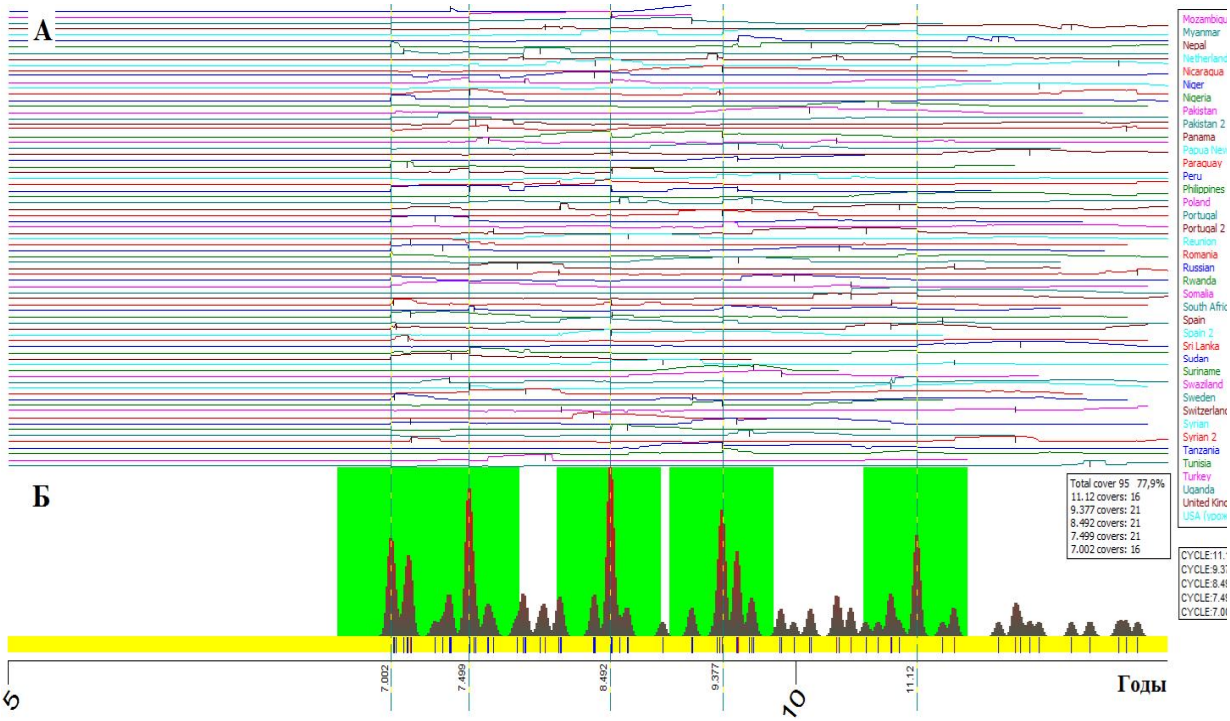


Рис. 5. Форвардная периодограмма циклов высокой вероятности мировой урожайность сахарной свеклы и тростника (1961-2017 гг.) – А; циклический геном и циклокластеры – Б

На рисунке 5 показаны высокочастотные периодограммы и циклический геном, рассчитанные по исследуемым временным рядам. Вертикальные линии показывают пять самых важных циклов (цикло-кластеров), найденных для этих кривых, т. е. это текущий циклический геном для большинства ВР сахарного подкомплекса.

Отмеченные пики внизу графика очень резкие – это означает, что данные циклы весьма убедительно проявили (и проявляют) себя в сахарном подкомплексе. Зеленые зона – это целые кластеры из циклов, на которые разбиты наиболее статистически значимые из них. Видно, что на пяти этих цикло-кластерах сосредоточено порядка 80 % из всех выявленных циклов.

Кластеры, соответственно, указывают нам на наиболее часто проявляющиеся циклы.

Красная гистограмма (полоса снизу) показывает разницу в активности этих кластеров по другому – чем выше гистограмма, тем чаще этот цикл появляется в диаграмме показателей в исследуемых ВР.

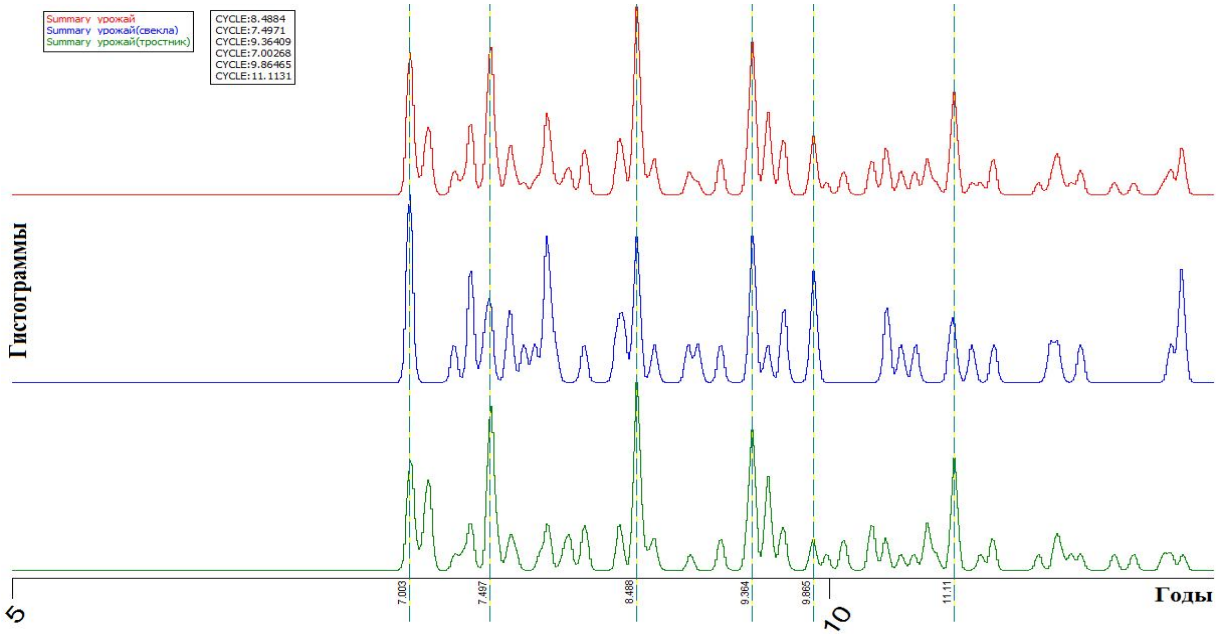


Рис. 6. Циклический геном урожайности, все страны Мира (1961–2017 гг.)

На рисунке 6 показана обобщенная картина циклического генома по урожайности сахарной свеклы и тростника в Мире.

Всего было выявлено 180 (из ВР по 110 странам производителям) наиболее значимых циклов. Высокочастотная периодограмма показывает, как распределяются эти циклы и какие из них более/менее однородны. Например, видно, что самые высокие пики (циклы) соответствуют величинам в 7.003, 7.497, 8.488, 9,364, 9.865 и 11.113 лет. Это указывает на то, что данные циклы проявляется в сегменте производства сахарной свеклы и тростника чаще, чем другие.

Мутации в циклическом геноме

Исходя из того, что при исследовании всего мирового сахарного подкомплекса (МСП) нами было выявлены 646 различных циклов сталкиваемся с проблемой оценки выявленных циклов, все это делает визуальный кластерный анализ просто невозможным. На этом этапе необходимо использовать гистограмму, чтобы увидеть, как распределяются эти циклы. Под мутацией в ЦГ понимается сдвиг по генеральной совокупности по заранее определенной выборки. Называется такая гистограмма высокопараметрической периодикой.

Поскольку циклический геном во всем мире меняется со временем, некоторые циклы исчезают и появляются новые циклы. Очень важный факт состоит в следующем: данный циклический геном очень стабилен (на определенном промежутке времени), он существует практически без изменений, так если рассмотреть три временных диапазона мирового производства сахара с 1864 по 2016 гг. (т. е. усредненную картину за последние 150 лет), то увидим следующие «мутации»: 1) 1864–1915 гг. – 9,4934 лет, 2) 1916–1966 гг. – 9,3712 лет и 3) 1967-2016 гг. – 7,12 лет, т. е. все это время МСП реагировал на внешние события, используя один и тот же набор циклов (проявлял себя через данный циклический геном). Видно, что этот циклический геном стабилен на протяжении последних 50 лет.

На рисунке 6 показан циклический геном, который изменяется с течением времени. Данная диаграмма (гистограмма) построена в качестве пояснения, как исторически изменялся циклический геном.

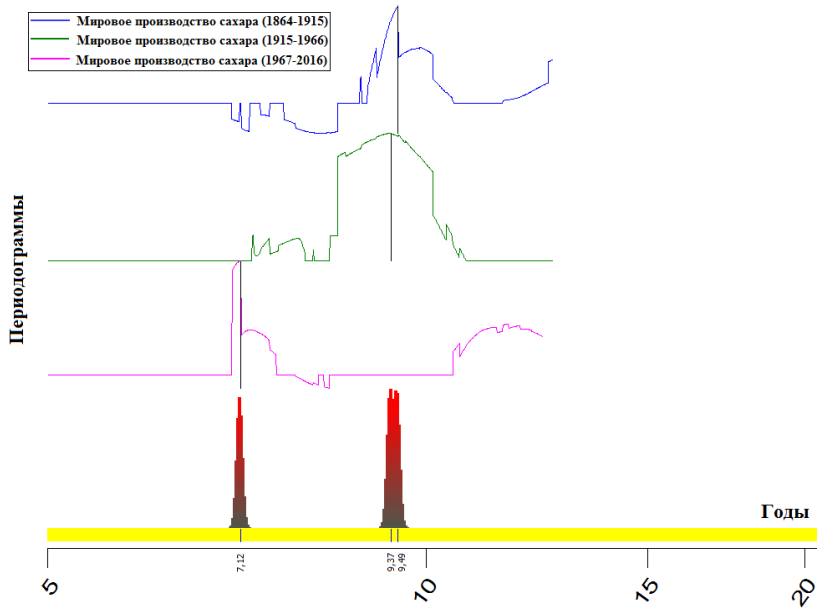


Рис. 7. Циклические «сдвиги» в мировом производстве сахара (1864–2016 гг.)

Нами извлечены три самых мощных цикла (пика) из гистограммы представленной выше. Это и есть циклический геном мирового производства сахара (рисунок 6). Полученный результат – 7,12-летний цикл определенно более активен («моложе»), чем другие циклы. Этот факт указывает на существенное улучшение в понимании общей циклической картины, когда рассматривается не один ВР, а сразу множество.

Это означает, что среди многих других циклов данный цикл в 7,12 лет появляется чаще, чем другие циклы. Соответственно, этому циклу необходимо уделять больше внимания. И вероятность того, что этот цикл будет работать в исследуемых ВР выше, чем подобная вероятность для других.

Таким образом, с помощью вычислений можно увидеть вместе на одном графике наиболее важные циклы для изучаемого производственного показателя и циклический геном, который указывает нам на наиболее вероятные циклы.

Генетические смещенения в циклах в больших или меньших масштабах меняют сложившуюся картину мира и становятся наследственным ядром, исходной базой для появления нового (или радикально обновленного) кластера все более дифференцированной системы в структуре сахарного подкомплекса [с. 88, 5].

Необходимо четко понимать, что в данной работе говорится о возможности, а не о силе или значимости анализируемых циклов.

Выводы

В заключении можно с полной уверенностью сказать, что только с помощью социогенетики (циклического генома) можно выяснить внутренний механизм, закономерности развития, выделить инвариантное ядро, выражающее суть изучаемой области, оценить содержание и перспективы периодически возникающих кластеров мутаций, отбирая те из них, которые войдут в состав обогащаемого генотипа общественной системы (в нашем случае МСП), что в конечном итоге делает его удобным инструментом для выработки достоверных прогнозов [с. 84, 5].

1. В данном исследование и в первые на практике были вычислены циклы с помощью форвардного анализа.

2. На практике такие циклы можно отображать (представить) как высокостабильные циклы при работе со спектральным или форвардным анализом.

3. Глубинные закономерности наследственности и изменчивости в динамике агропромышленного комплекса во многом остаются неизученными из-за отсутсвия в других его сегментах исследований в области социогенетики (циклического генома).

Литература:

1. Мартишин Е. М. Генетические механизмы экономической эволюции / дисс...на соис. док. экон. наук. – Р-н/Д: ЮФУ. 2016. – 433 с. [Электронный ресурс]. Режим доступа: http://hub.sfedu.ru/media/diss/126a5412-fe79-405e-8822-18e8d8dd8931.

2. Кондратьев Н. Д. Основные проблемы экономической статики и динамики: Предварительный эскиз / Авт. статей о Кондратьеве и его творчестве: Ю. Н. Давыдов, Ю. В. Кочеврин, В. В. Симонов. – М.: Наука, 1991. – 567 с.

3. Тарасов С. Циклический геном (CG). [Электронный ресурс]. Режим доступа: https://timing-solution.livejournal.com/35862.html.

4. Тарасов С. Циклический геном (CG). Часть II. [Электронный ресурс]. Режим доступа: https://timing-solution.livejournal.com/?skip=48.

5. Яковец Ю. В. Социогенетика: становление интегрированной отрасли знаний // М.: Общественные науки и современность. 1993. № 4. – С. 82-88. [Электронный ресурс]. Режим доступа: http://ecsocman.hse.ru/data/315/209/1218/008_Yurij_ YaKOVETs.pdf.

Жукова П.Н., Насонова В.А.

Белгородский юридический институт МВД России

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ МЕССЕНДЖЕРОВ В ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

Коммуникации между людьми сегодня достигли высочайшего уровня технологичности. Прогресс в области компьютерных и мобильных разработок сделал возможным обмен сообщениями за считанные секунды. Это позволяет людям общаться в режиме реального времени, находясь при этом за сотни тысяч километров друг от друга. С помощью системы мгновенных сообщений обмениваться можно не только текстовыми посланиями, но также изображениями, звуковыми сигналами и видеозаписями. Для коммуникаций такого рода используется специальная клиентская программа, называемая Instant Messenger. Английское слово messenger является производным от message – сообщение. Мессенджер – это программа, веб-сервис по обмену мгновенными сообщениями. Практически каждая крупная интернет-компания и социальная сеть сегодня имеет на своём сайте маленький мессенджер, позволяющий быть «на связи» в режиме реального времени.

В данной работе рассмотрены понятие «мессенджер», возможности использования в деятельности экстремистской и террористической направленности.

Первым широко известным онлайн-мессенджером был **ICQ**, затем доминировать на рынке мессенджеров стал **Skype**, во многом благодаря внедрению поддержки голосовых и видеозвонков.

На настоящий момент, среди наиболее популярных мессенджеров можно выделить - WhatsApp, Viber, Facebook Messenger, Skype, ICQ, Google Hangouts, Telegram.

Классифицировать мессенджеры можно по-разному, например, существуют мессенджеры, интегрированные в какое-либо приложение или социальную сеть (Skype, Facebook Messenger, обмен сообщениями в Одноклассниках или ВКонтакте) и самостоятельные программы (ICQ, Pidgin, Viber, WhatsApp, MyChat). Также мессенджеры можно разделить на предназначенные для общего пользования и для закрытого общения (корпоративные мессенджеры, мессенджеры для локальной сети). Существуют ис-

ключительно мобильные мессенджеры и мультиплатформенные. Рассмотрим более подробно функциональную часть каждой из указанных групп мессенджеров.

• **Интегрированные.** Это не самостоятельные программы, которые встроены в какое-либо приложение, либо в социальную сеть. Примерами таких мессенджеров являются средства обмена сообщениями в социальных сетях (Facebook Messenger, Одноклассники, ВКонтакте). Имеют достаточную функциональную часть, поддерживают все стандартные возможности, включая отправку файлов, собственный набор смайлов. Не требуют предварительного скачивания и установки.

• **Самостоятельные мессенджеры** (Bleep, MyChat). Отдельные приложения, которые требуется скачать и инсталлировать на устройство. Основаны как клиент-серверный коммуникационный комплекс для корпоративной сети. Работает под Windows через протокол TCP/IP. Функциональность включает передачу/приём текстовых сообщений, файлов, отправку SMS на мобильные телефоны, публичные и секретные каналы, «приваты», рассылки широковещательных сообщений, планировщик, записную книжку, адресную книгу и многое другое. Все административные действия выполняются на сервере с помощью графического интерфейса, встроенной консоли или Telnet сессии. Все передающиеся сообщения могут быть сохранены в протоколах сервера.

• **Мобильные**. Предназначенные для общения между мобильными устройствами по закрытым протоколам. Количество таких мессенджеров стремительно сокращается, поскольку тенденция развития идет в сторону мультиплатформенности. Примерами могут служить: WhatsApp, Line, Snapchat и ряд других. Особенности функционала таких мессенджеров заключается в следующем:

- использование IP-телефонии, возможность совершения «голосовых» или «видео» звонков;

- возможность «исчезающих сообщений» (пользователи могут отправлять друг другу сообщения или изображения, которые исчезают через несколько секунд после просмотра);

- «перехват» контакт-листов из уже имеющегося списка «друзей» в других сервисах, либо телефонной книги;

- функция «отзыв сообщения», возможность отмены передачи сообщения либо его удаления из переписки, уже после отправки;

- шифрование сообщений пользователей, на всем пути, от пользователя до пользователя, то есть не оставляют метаданные на центральном сервере.

• **Мультиплатформенные**. Их можно установить как на мобильные устройства, работающие под управлением разных операционных систем, так и на персональные компьютеры. Все интегрированные мессенджеры являются мультиплатформенными. К ним относятся Viber, Telegram и многие другие. Функционал еще более расширенный, по сравнению с мобильными мессенджарами.

Основным требованием пользователей к мессенджерам является - сохранность тайны переписки. Многие популярные мессенджеры имеют такую функцию и способны обеспечить своим абонентам высокий уровень безопасности.

Рассмотрим мессенджеры с шифрованием.

Telegram. Бесплатный кроссплатформенный мессенджер для смартфонов и других устройств, позволяющий обмениваться текстовыми сообщениями и медиафайлами различных форматов. Используется специальный протокол шифрования, а также таймер на самоуничтожение сообщений. Серверная часть с закрытым кодом, работающая на мощностях нескольких компаний США и Германии. Безопасность от перехвата пересылаемых сообщений со стороны сервера Telegram обеспечивается лишь в режиме «секретных» чатов (Secret Chats). Этот режим реализует шифрование, при котором

лишь отправитель и получатель обладают общим ключом (end-to-end шифрование), с применением алгоритма AES-256 в режиме IGE (Infinite Garble Extension) для пересылаемых сообщений. В отличие от обычного режима, сообщения в секретных чатах не расшифровываются сервером, история переписки сохраняется лишь на тех двух устройствах, на которых был создан чат. Для мессенджера был создан протокол MTProto, предполагающий использование нескольких протоколов шифрования. При авторизации и аутентификации используются алгоритмы RSA-2048, DH-2048 для шифрования, при передаче сообщений протокола в сеть они шифруются AES с ключом, известным клиенту и серверу. Также применяются криптографические хеш-алгоритмы SHA-1 и MD5.

При обмене файлами можно как отправить файлы с устройства, так и искать медиаконтент в интернете, в том случае, если используется мобильная версия для IOS или Android. Программа использует систему «докачки» файлов после обрыва связи. Имеется возможность организовывать мультичаты до 200 участников, супергруппы до 1000 участников.

▪ **Wickr**. Сервис с шифрованием и самоуничтожением документов.

▪ **ChatSecure**. Не является отдельным мессенджером, а отдельным приложением для зашифровки сообщений. Приложение должно быть установлено у всех участников переписки.

▪ **Pidgin**. Популярное приложение, особенно у пользователей Linux. Позволяет шифровать сообщение по выбору.

Рассмотрев основные возможности современных мессенджеров, становится понятна обеспокоенность спецслужб их массовым распространением и возможностью бесконтрольного общения, в частности, криминальной среды.

Нарастание угроз террористического и криминогенного характера как в европейских государствах, так и на территории Российской Федерации порождает необходимость создания комплексных систем защиты (КСЗ) на значимых для государства объектах. Террористические атаки приобретают все более широкий и изощренный характер. Практика показала, что современная террористическая деятельность проводится организованно, имеет свои центры и сеть подготовки террористов, носит системный характер. Уже понятно, что облик террориста-смертника как простого исполнителя акции все более тускнеет перед террористом-организатором и террористом-инженером.

Очевидно, что при планировании любой акции специалистами террористического центра в той или иной степени проводится разработка плана действий для достижения поставленных стратегических целей. В соответствии с этим разрабатывается локальный сценарий и определяются задачи террористическим подразделениям. Области действий могут быть выбраны любыми. Чем значимее объект, тем выше вероятность атаки на него.

Для решения задачи проводится предварительное обследование объекта (разведка), анализ и оценка его уязвимости. По этим данным разрабатываются варианты сценариев и инструкции действий террористических групп по захвату цели или разрушению объекта.

Во исполнение этих целей проводится ряд локальных операций, которые далее проговариваются между участниками, используя новые коммуникационные каналы – мессенджеры с шифрованием. Однако спецслужбы и команда Telegram активно занимаются поиском и дальнейшей блокировкой подобных каналов.

Правительство России занялось регулированием деятельности мессенджеров, и его намерения настолько серьезны, что в обществе о возможных блокировках подобных сервисов говорят с 2016 года.

Еще в 2014 году Роскомнадзор создал реестр организаторов распространения информации. Порядок работы Роскомнадзора с организаторов распространения информации подразумевает, что по требованию правоохранительных органов Роскомнадзор должен направить организаторам распространения информации запрос, в ответ на который последние обязаны предоставить в Службу необходимую контактную информацию. Если же в течение 5 рабочих дней ответ от компании отсутствует, Роскомнадзор направляет уведомление о неисполнении обязанностей организатора распространения информации и предоставляет 15 дополнительных рабочих дней для выполнения требования. В случае отказа от выполнения обязанностей организатора распространения информации власти будут вынуждены ограничить доступ к информационным системам организации на территории РФ.

Регистрация в указанном реестре до лета 2016 года была не обязательна, но с 20 июля для дальнейшей работы на территории России мессенджерам необходимо пройти регистрацию. Помимо этого, мессенджеры должны персонифицировать своих пользователей и предоставлять информацию о методах, применяемых для кодировки сообщений в федеральные органы исполнительной власти.

Власти и компании, владеющие мессенджерами, не могут договориться из-за пакета антитеррористических поправок, получивших название «законов Яровой» в честь их разработчика - депутата Ирины Яровой.

С 1 июля 2018 года начинает действовать одно из положений «пакета Яровой». Данное положение касается регулирования работы мессенджеров на территории России и обязует хранить в течение года информацию о фактах приема, передачи, доставки, обработки сообщений, а также о данных пользователях, участвующих в переписке на территории РФ.

Директор ФСБ России Александр Бортников считает необходимым контроль за мессенджерами в России. По его словам, выявленные в РФ террористические ячейки пользовались мессенджерами с высокой степенью шифрования. В качестве примера Бортников привел случай террористической атаки в метро Санкт-Петербурга 3 апреля 2017 года. При подготовке атаки террористы запрещенной в России организации ИГИЛ общались при помощи WhatsApp и Telegram. Этими же мессенджерами пользовались и другие боевики, нейтрализованные на территории РФ.

Несмотря на это, по мнению эксперта, добавление в реестр организаторов распространения информации – это еще одна из форм контроля над террористической деятельностью в стране.

Эксперт по спецслужбам консультативного агентства по вопросам безопасности TD International Елисей Богуславский пояснил, что в теории закон о мессенджерах должен сделать передачу сообщений более прозрачной, но при этом он сам по себе является угрозой безопасности. Поскольку, массовое дешифрование потоков информации, приведет к ее уязвимости для третьих лиц, делая поток информации незащищённым, государство развязывает руки мошенникам.

Таким образом, вмешательство государства в повседневную жизнь миллионов граждан, неудобство и ограничение свободы могут лишь укрепить идеологическую почву для террористов.

Конечно, маловероятно, что абсолютно все мессенджеры заблокируют, и пользователям придется как 10 лет назад общаться только с помощью SMS-сообщений и электронных писем, но на текущий момент существуют аналоги приложений для обмена сообщениями, которые не требуют подключения к сети.

Одним из самых популярных подобных приложений является Firechat. В отличие от всех популярных мессенджеров Firechat не нужно подключение к интернету для об-

щения с другими пользователями - приложение создает mesh-сеть, используя Bluetooth и прямое подключение через Wi-Fi.

Firechat обеспечивает обмен сообщениями и фотографиями в режиме оффлайн между устройствами. Приложение использует многоскачковую передачу данных от пользователя к пользователю, образуя таким способом сеть, с помощью которой и происходит передача сообщений. Чем больше людей используют данную программу, тем быстрее сообщение дойдет до адресата.

Разработчики также продумали вопросы безопасности - никто кроме собеседника не сможет прочитать отправленное ему сообщение, так как переписка шифруется. Зарегистрировано активное использование Firechat во время массовых беспорядков, при которых озабоченность спецслужб обосновывается невозможностью отследить перемещения протестующих.

Литература:

1. Обзор мобильных мессенджеров // электронный ресурс http://www.voipoffice.ru/tags/ mobil%27nye_messendzhery/

2. Мессенджеры в России: цифры и тренды, весна 2017 // электронный ресурс http://blog.br-analytics.ru/messendzhery-vesna-2017/

3. Лапин В.В., Слесарева Е.А., Старостенко И.Н. Информационные системы в деятельности органов внутренних дел. Учебное пособие. – М.: Московский университет МВД России, 2014.

4. Михайленко, Е.В. Математика и информатика: курс лекций / Е.В. Михайленко, И.Н. Старостенко. – Краснодар: Краснодарский университет МВД России, 2009. – 420 с.

5. Михайленко, Е.В. Информатика: учеб. пособие / Е.В. Михайленко, И.Н. Старостенко, Ю.Н. Сопильняк; под общ. ред. Е.В. Михайленко. –- Краснодар: Краснодарский университет МВД России, 2010. – 336 с.

Журавленко Н.И.
Крымский филиал
Краснодарского университета МВД России

ИСПОЛЬЗОВАНИЕ ПРИНЦИПА ЭКВИФИНАЛЬНОСТИ ДЛЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ КРИМИНОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ ЭКОНОМИЧЕСКОЙ НАПРАВЛЕННОСТИ

В настоящее время в связи с ослаблением контроля экономической деятельности правоохранительными структурами в случае возникновения кризисных явлений в экономике в отдельных странах или даже в целых регионах может произойти резкое увеличение теневого сектора экономики. Возможность возникновения угроз подобного рода существует постоянно, и от них не может быть застрахована ни одна экономическая система. Для предотвращения таких угроз необходимо обеспечить укрепление сил и средств правоохранительных органов в сфере экономической безопасности. Одним из основных направлений этой деятельности является развитие информационно-аналитического обеспечения оперативно-розыскной деятельности. Математические методы и модели способны дать хорошие результаты при прогнозировании противоправного поведения лиц, совершающих экономические преступления. Одним из наиболее эффективных методов прогнозирования преступного поведения является использование принципа эквифинальности (его еще называют «принцип черного ящика», F-подход,

функциональный подход), сущность которого заключается в том, что в одинаковых условиях люди обычно совершают очень схожие поступки.

Впрочем, существуют и исключения из общих правил. Если говорить об экономических преступлениях, то следует отметить, что история криминалистики знает множество случаев отклонения от указанного принципа, когда преступники достигали своих криминальных целей поступая, казалось бы, совершенно нелогично. Поведение таких «нетипичных» злоумышленников всегда являлось одним из самых изощренных. Вспомним, например, знаменитый случай продажи Эйфелевой башни Виктором Люстигом, финансовую пирамиду Сергея Мавроди, всемирно известные махинации Фрэнка Абигнейла (человека по прозвищу «поймай меня, если сможешь») и многие другие. Эти преступные схемы поражают своей хитростью, изощренностью и грандиозностью размаха.

Однако следует признать, что подобные «нетипичные» преступления совершаются достаточно редко, выбиваясь из общей криминальной практики. Если же обратиться ко всей совокупности совершаемых в мире преступлений, то станет очевидным, что большинство преступлений совершается вполне тривиальными и предсказуемыми методами. При этом ежедневные обороты такой «предсказуемой преступности» наносят самый значительный ущерб экономическим структурам. Поэтому для правоохранительных органов и служб безопасности, обеспечивающих экономическую защиту различных субъектов, важным методологическим средством прогнозирования преступного поведения может стать математический аппарат, разработанный для осуществления информационно-аналитического обеспечения оперативно-тактического прогнозирования. Основная цель такого прогнозирования заключается в разработке оперативно-розыскных версий, способствующих принятию обоснованных решений при осуществлении оперативно-розыскной деятельности и планировании профилактических мероприятий. Можно выделить следующие основные направления такого прогнозирования, осуществляемого с целью определения наиболее целесообразных способов предотвращения и расследования преступлений экономической направленности:

- прогнозирование вероятного поведения преступных групп и неформальных объединений с антиобщественной направленностью;
- прогнозирование индивидуального преступного поведения;
- прогнозирование вероятной криминальной ситуации, которая может сложиться в период оперативной проверки и разработки подозреваемых лиц [1].

Одной из первоочередных задач, которые стоят перед оперативными работниками на стадии изучения криминальных событий и лиц, их подготавливающих и совершающих, является распознание криминологических особенностей преступников. Возможность идентификации преступника и прогнозирования его будущих криминальных действий (с проведением последующего анализа с помощью математических методов и моделей) может быть подкреплена созданной для решения этих задач базой данных, построенной на основе методов реферирования, сопоставления и синтеза, позволяющих обрабатывать неструктурированную информацию.

Реферирование информации используется в тех случаях, когда необходимо обрабатывать очень большие объемы сведений, поступающих из различных источников. В подобных ситуациях возникает потребность «отсечь» лишнюю малозначимую информацию, чтобы сформировать выборки материалов, имеющих реальную ценность для исследования. Другими словами, в ходе реферирования из всего информационного массива выбираются и изучаются наиболее значимые сведения, имеющие прямое или опосредованное отношение к изучаемой проблеме (первоначальному объекту исследований).

Сопоставление информации осуществляется путем ее систематизации и классификации. Систематизация предусматривает дальнейшее расчленение сведений, содер-

жащихся в выборках, на менее объемные массивы, и установление конкретных фигурирующих в них объектов, с учетом их характерных признаков. Последующая классификация (она может рассматриваться и как установление групповой принадлежности) предполагает поиск в этих массивах объектов, обладающих классификационным тождеством с первоначальными объектами исследования.

Синтез представляет собой наиболее важную для нашего случая стадию – логическую интеграцию выделенных массивов данных, в которых представлены объекты, на первый взгляд, не располагающие общими признаками, в единую последовательность взаимосвязанных элементов.

Сформированная с помощью трех перечисленных методов база данных должна отвечать критериям, ориентированным на такие параметры криминологических особенностей преступников, как психологические особенности, свойства характера и индивидуальные предрасположенности злоумышленников, непосредственно влияющие на ход их преступных действий. При этом также следует учитывать физиологические особенности преступника, тяжесть совершаемых им деяний, рецидивизм, участие преступника в деятельности организованных преступных группировок и пр.

При построении программно-аппаратного комплекса для работы с массивами неструктурированной информации различного характера (тексты, изображения, видеоизображения, аудиозаписи) могут быть использованы нейронные сети, с помощью которых становится возможным оперирование с поисковыми приложениями для любой информации, представленной в электронном виде. В отличие от заложенного в обычных поисковых системах традиционного подхода, который предусматривает работу с формализованными документами, данная система способна обеспечить автоматическое индексирование символов, содержащихся в полнотекстовых документах, и их последующее распознание за счет морфологического анализа и построения семантических сетей. Она предполагает эффективный поиск необходимых объектов за счет того, что «знает», какие слова связаны по смыслу с устанавливаемым объектом. На этой основе обеспечиваются «нечеткий поиск», семантический поиск, последующее экспертное уточнение запроса, атрибутивный поиск, поиск по образцу и ряд других операций.

Следует уточнить, что не все перечисленные выше параметры криминологических особенностей преступников поддаются математическому описанию, так как для математического моделирования и прогнозирования преступных действий требуется обширная криминологическая база данных, включающая в себя многолетние статистические данные о действиях многих людей. Например, индивидуальные предрасположенности и качества характера человека изначально должны быть разделены на типажи, которые предполагают большое количество возможных вариантов градации типов личности. К примеру, преступники могут быть классифицированы по следующим признакам: по степени общественной опасности, по социально-демографическим признакам, по уголовно-правовым признакам, по нравственно-психологическим признакам.

В качестве математического метода моделирования и прогнозирования преступного поведения могут быть использованы «нечеткие множества», описанные в трудах американского ученого Латфи Заде. Одним из ограничений в применении этого метода является то, что данные об индивидуальных особенностях преступников могут быть достаточно сложными и не поддающимися точному количественному описанию.

Для описания индивидуальных особенностей преступников могут быть использованы лингвистические переменные, оперирующие с естественными или искусственными языками [2]. Лингвистическая переменная представляет собой величину, заданную на некоторой количественной шкале. Она принимает определенные значения в виде слов и словосочетаний естественного языка. Значения лингвистической переменной описываются нечеткими значениями, а всякая лингвистическая переменная и её значе-

ния связаны с конкретной количественной шкалой, которая, в свою очередь, отображает ранее сформированное мнение эксперта (в нашем случае – в области криминальной психологии или криминологии) [3].

В целом же, нечеткое множество строго определяется с помощью функции принадлежности. А четкое множество (возьмем стандартные значения – 1 или 0) является частным случаем нечеткого множества (те же значения, но в интервале от 0 до 1). При этом понятие нечеткого множества является расширенным понятием, охватывающим также и понятие четкого множества [4]. Таким образом, подобные базы данных с идентификационными критериями могут быть полностью представлены посредством четких и нечетких множеств.

Следующим логичным шагом должен быть предположен перевод данных в систему квалификации значений или же в систему измерений результатов. Таких систем может быть огромное количество. Но в каждом конкретном случае первоначальная цель – это оценка прогнозируемого поведения лица на основании одного из самых простых, но одновременно и самых важных принципов – принципа эквифинальности его криминологических особенностей, или, иными словами, предсказуемости его мышления.

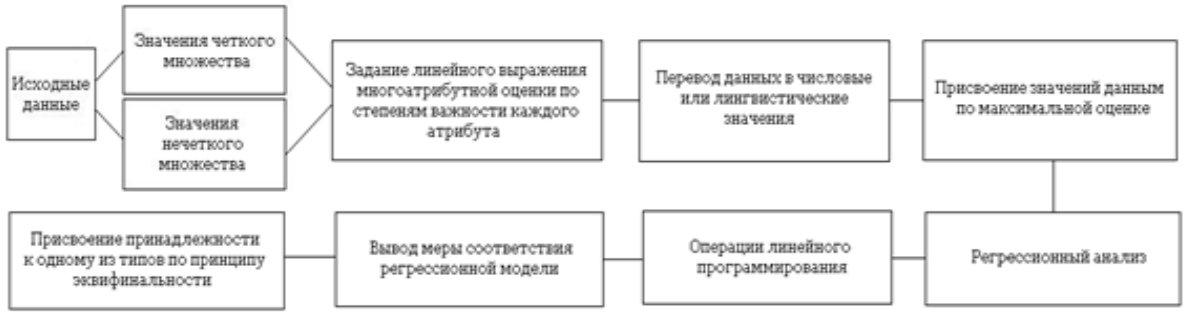
Исходя из принципа эквифинальности можно выделить три вида мышления человека: системное, α-системное и несистемное. Системное мышление подразумевает порядок действий, ранее неоднократно использовавшийся другими людьми в прошлом. α-системное мышление характерно для лиц, использующих порядок действий, крайне редко встречающийся в прошлом (при этом он может сочетаться с элементами системного мышления). И, наконец, несистемное мышление приводит к такому порядку действий, который ранее не встречался в практике.

С целью анализа данных по принципу эквифинальности необходимо предварительно произвести ряд математических действий оценочного характера. Для описания четких и нечетких множеств наиболее удобно использовать многоатрибутную оценку, приведенную в трудах японских ученых Т. Тэрано, К. Асаи, М. Сугэно, продолживших изучение нечетких множеств и нашедших им применение в различных областях, - в бизнесе, медицине, промышленности. В криминологии существует огромный пласт данных, математическое описание которых наиболее точным образом возможно именно с помощью теории нечетких множеств. Возвращаясь к проблеме прогнозирования криминального поведения лиц, совершающих преступления в экономической сфере, следует отметить, что с помощью указанной методики может осуществляться оценка вероятности предполагаемого преступного поведения подозреваемых лиц.

Диагностика личности преступника и прогноз его дальнейших действий осуществляется следующим образом. Изначально многоатрибутная оценка задается с помощью линейного выражения, в котором определяется степень важности каждого атрибута. После этого в соответствии с поставленной задачей производится перевод данных в числовые или лингвистические значения. Далее в линейном выражении многоатрибутной оценки осуществляется присвоение значений данным, которые впоследствии дадут самую максимальную из возможных оценку для изучаемой личности, исходя из ее характеристик. В последующем, с целью достижения однозначных результатов проводимых исследований, посредством регрессионного анализа производится ряд вычислений.

Этот метод позволяет использовать выведенную ранее линейную формулу для последующего определения возможного диапазона её значений. После этого посредством линейного программирования становится возможным нахождение в полуинтервале [0;1) искомого значения, указывающего меру его соответствия регрессионной модели [5]. При этом предполагаемая оценка, рассчитанная исходя из ранее обозначенной цели определения по одному из параметров исследования личности, приобретает свойство

принадлежности одному из трех типов системного мышления по принципу эквифинальности. Для этого, как и в случае лингвистической переменной, всему диапазону оценочных параметров экспертом предварительно присваиваются характеристики по типам мышления. В свою очередь можно предположить, что наиболее точная оценка будет достигаться при задании общего диапазона значений для каждого из типов. Полная диагностика личности по предлагаемому принципу может считаться состоявшейся в случае получения всего множества параметров исследования и их последующего сопряжения. Для придания наглядности всей описанной совокупности производимых операций над данными, схематически их можно представить следующим образом.



Следует отметить, что главная роль в определении криминологических особенностей лиц, совершающих преступления экономической направленности, принадлежит эксперту, а обозначенные математические и программные инструменты являются лишь продолжением его функций, которые усиливают и совершенствуют их [6]. В заключение следует отметить, что рассмотренный в этой статье способ моделирования преступного поведения, основанный на принципе эквифинальности и построенный на основе теории нечетких множеств, позволит приблизить аналитические возможности компьютера к оперативной логике эксперта, но, наверно, никогда не сможет заменить ее.

Литература:

1. Правовое, техническое и аналитическое обеспечение оперативно-розыскной деятельности по борьбе с коррупционными преступлениями: монография. В четырех томах. Т.4. Аналитическое обеспечение оперативно-розыскной деятельности / И.М. Даукаев, Н.И. Журавленко, А.Н. Халиков, Е.Н. Яковец. – Уфа: РИЦ БашГУ, 2013. С. 324.

2. Понятие лингвистической переменной и его применение к принятию приближенных решений. / Л. Заде – М.: Издательство «Мир», 1976. С. 7.

3. Количественные методы в экономических исследованиях: Учебник для вузов / под ред. М.В. Грачева, Л.Н. Фадеева, Ю.Н. Черемных – М.: ЮНИТИ-ДАНА, 2004. С. 769.

4. Прикладные нечеткие системы: Пер. с япон. / К. Асаи, Д. Ватада, С. Иваи и др.; под ред. Т. Тэрано, К. Асаи, М. Сугэно – М.: Мир, 1993. С. 31.

5. Прикладные нечеткие системы: Пер. с япон. / К. Асаи, Д. Ватада, С. Иваи и др.; под ред. Т. Тэрано, К. Асаи, М. Сугэно – М.: Мир, 1993. С. 318.

6. Оперативно-розыскная информация / С.С. Овчинский; под ред. А.С. Овчинского и В.С. Овчинского – М.: ИНФРА-М, 2000. С. 173.

Заводцев И.В., Железняк А.О., Родионов П.О., Стабровский О.А.
Краснодарское высшее военное училище им. генерала армии С.М. Штеменко

ПЕРЕВОД ИНФРАСТРУКТУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА НОВЫЕ ПРОГРАММНЫЕ РЕШЕНИЯ

Естественным ходом развития информационных технологий является принципиальный переход от открытости к защищенности при построении информационных систем (ИС). На сегодняшний день большая часть программно-аппаратных средств, используемых в ИС, уже обладает встроенными функциями по защите информации или имеет отдельные элементы с такими функциями.

Однако, в общем случае, защита ИС должна строится в предположении о потенциальной уязвимости средств вычислительной техники, и наряду с проблемами производительности, надежности и устойчивости функционирования самой ИС, остро встает проблема защиты от несанкционированного доступа (НСД) циркулирующих в ИС данных.

Публикуемая периодически статистика об ошибках и уязвимостях базового и прикладного программного обеспечения, а также многочисленные сведения о недостаточности штатных средств защиты заставляет специалистов сомневаться в гарантированности защиты от НСД при их использовании, определяя неизбежный переход к широкому внедрению специализированных СЗИ [2,3]. На которые тратятся дополнительные ресурсные затраты по развертыванию и администрированию.

Кроме того, предъявляемые к уровню информационной безопасности ИС организаций сегодня требования предопределяют также необходимость проведения процесса администрирования всех видов СЗИ в сжатые сроки, с высоким качеством и обязательной технической поддержкой. Обуславливая необходимость соответствующей подготовки штатных специалистов по развертыванию как IT-инфраструктуры организации, так и по построению системы обеспечения информационной безопасности.

Цель статьи – рассмотреть возникающие сложности при переводе инфраструктуры обеспечения и контроля целостности информационных систем на новую платформу криптографических средств и возможные способы их решения.

При проникновении в защищаемую информационную систему злоумышленник, как правило, попытается установить программные закладки, изменить системные файлы или отключить систему защиты, а также подменить циркулирующие в ИС данные. В абсолютном большинстве случаев, все эти действия реализуются путем доступа и изменения каких-либо файлов (исполняемых, конфигурационных и динамических библиотек и т.п.).

Поэтому для защиты данных в ИС используется целевой контроль целостности защищаемых ресурсов, основанный на пассивных (не оказывающих заметного влияния на работу ИС) способах проверки меток целостности как самой системы и файлов с данными, а также и отдельных объектов системы, и их атрибутов. Такие решения реализуются с помощью криптографических алгоритмов – систем контроля целостности, в т.ч. систем электронной подписи (ЭП).

Схемотехнически такое решение представляет собой введение относительно небольшого количества избыточной информации, передаваемой вместе с защищаемым массивом данных [1].

Широкое использование в этом направлении получила программа КриптоАРМ, предназначенная для защиты и гарантии авторства документов и файлов, передаваемых по электронной почте и на машинных носителях информации [4, 5].

В тоже время для обеспечения надежного функционирования систем криптографической защиты необходимо обеспечить надежную и устойчивую работоспособность систем распределения ключевой информации и доверия.

Эту задачу призван решить программно-аппаратный комплекс «КриптоПро Удостоверяющий центр». Он предназначен для обеспечения участников информационных систем средствами и спецификациями для использования сертификатов открытых ключей в целях обеспечения:

применение электронной подписи;

контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников ИС;

аутентификации участников информационных систем в процессе взаимодействия;

конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

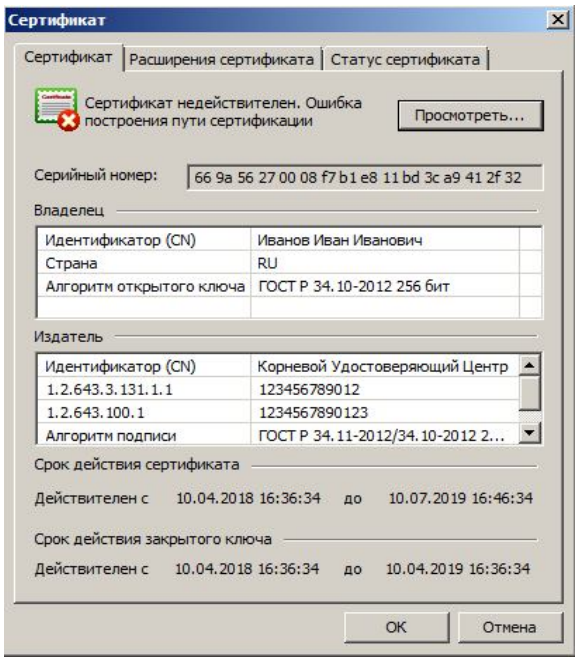


Рис. 1. Ошибка использования переданного сертификата

Сегодня очень актуален переход на версию «КриптоПро Удостоверяющий центр 2.0». Это связано с требованиями ФСБ России, сопряженными с запретом использования ГОСТ Р 34.10-2001 для формирования подписи после 1 января 2019 года.

В тоже время его установка и настройка являются нетривиальной задачей и требует особого рассмотрения. Так, зачастую, при попытке передачи сертификата пользователя, сформированного СЗИ КриптоАРМ на другую автоматизированную рабочую станцию, возникает ошибка построения пути сертификации (рис. 1).

Решить данную проблему удалось путем построения защищенного пути выдачи/передачи сертификата с использованием «КриптоПро УЦ».

Рассмотрим особенности реализации предложенного подхода:

1. Регистрация личного кабинета пользователя с использованием web-интерфейса «КриптоПро УЦ»;

2. Создание заявки на получение сертификата (рис. 2);

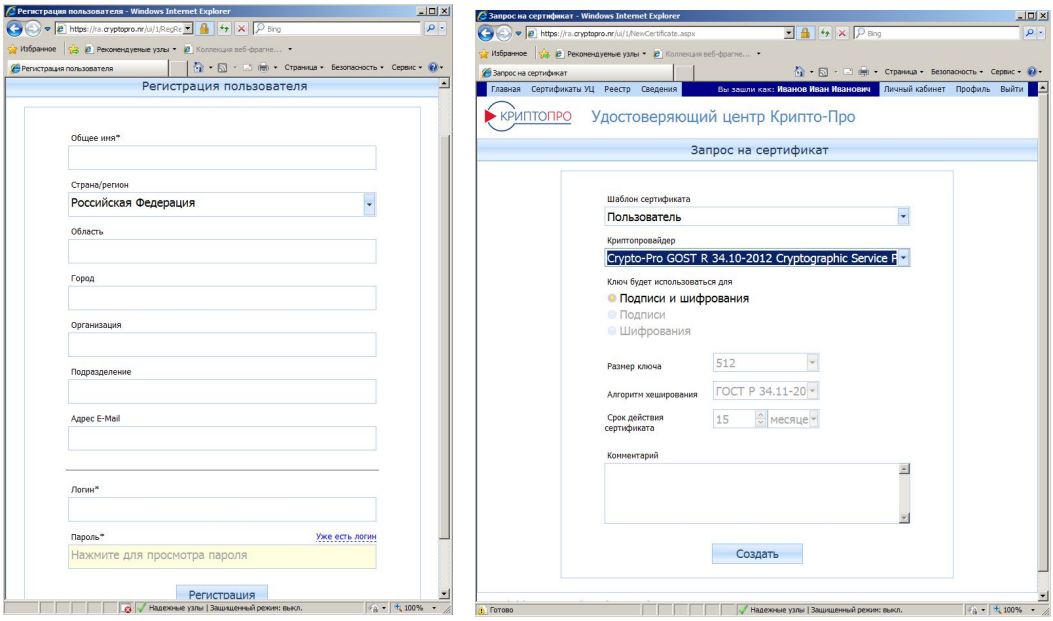


Рис. 2. Регистрация личного кабинета пользователя

3. Получение заверенного сертификата (рис. 3).

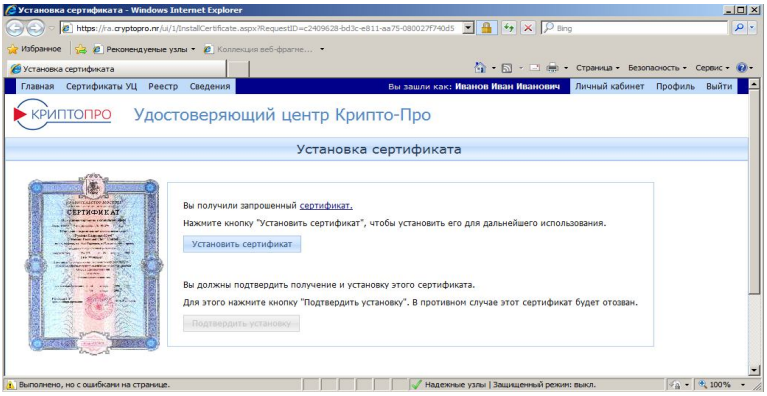


Рис. 3. Получение и выдача заверенного сертификата

Для реализации заявленного подхода осуществлялось полунатурное развертывание объекта информатизации с выделенным сервером, на котором устанавливалось инфраструктура ПАК «КриптоПро УЦ v.2.0». При этом в ходе практического исследования были установлены следующие особенности работы с ПАК «КриптоПро УЦ v.2.0»:

передача сертификатов вне защищенного соединения невозможна;

соединение осуществляется при помощи сервера ISS, куда вносятся корректировки в соответствии с законодательством РФ, реализуя технологии защищенной передачи данных TLS с поддержкой ГОСТ 28147-89;

взаимодействие пользователя и администратора ПАК «КриптоПро УЦ» осуществляется по средствам «Консоли управления УЦ», позволяющей обрабатывать запросы пользователей на регистрацию, получение, отзыв, перевыпуск, приостановления действия сертификатов;

взаимодействие центров регистрации и сертификации осуществляется путем встречной аутентификации за счет сертификатов, содержащих собственные открытые ключи

центр сертификации не может быть привязан к какому-либо домену, а так же не может быть контроллером, он является изолированным сервером;

после установки компонентов изменять их идентификацию нельзя, так как имена и принадлежность к домену записана в сертификаты, и их изменение влечет отказ от

работы web – интерфейса центров регистрации и сертификации как принадлежащего другим субъектам.

Литература:

1. Федеральный Закон Российской Федерации от 25 марта 2011 года № 63-ФЗ «Об электронной подписи»: принят Гос. Думой Российской Федерации 25 марта 2011 г., одобр. Советом Российской Федерации 30 марта 2011 г. // Парламент. газ. - 2011; Рос. газ. - 2011.

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: принят Гос. Думой Российской Федерации 8 июля 2006 г., одобр. Советом Российской Федерации 14 июля 2006 г. // парламент. газ. - 2005; Рос. газ. – 2006.

3. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования.

4. Постановление правительства Российской Федерации «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» от 9 февраля 2012 г. № 111.

5. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСБ Российской Федерации 21 февраля 2008 г. № 149/6/6-622.

Зарубин С.В., Зарубин В.С.
Воронежский институт МВД России

К ВОПРОСУ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ БЕЗОПАСНОСТИ

Для повышения эффективности комплексов средств автоматизации пунктов централизованной охраны (ПЦО) необходимо совершенствовать информационную поддержку и процедуры автоматизации управления при централизованном сборе информации о состоянии технических средств безопасности на охраняемых объектах.

Особенно это важно для таких сложных объектов, как критически важные, потенциально опасные, территориально-распределенные, где интегрированные системы безопасности (ИСБ) представляют собой автоматизированные системы, построенные с применением сетевых технологий. В соответствии с положениями нормативных документов методами обеспечения безопасности информации при взаимодействии подсистем ИСБ с сетью являются:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры охранного оборудования ИСБ;
- мониторинг вторжений в локальные вычислительные сети (ЛВС), нарушающих или создающих предпосылки к нарушению установленных в организации требований по защите информации;
- анализ защищенности охранного оборудования ИСБ, предполагающий применение специализированных программных средств (сканеров безопасности), позволяющих осуществлять анализ защищенности данного оборудования;

- шифрование информации при ее передаче по сети, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации;

- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

- использование средств антивирусной защиты;

- централизованное управление информационной безопасностью.

Безопасность информации как состояние ее защищенности является характеристикой самой информации. Среди свойств этой характеристики выделяется свойство варьируемости, которое, в свою очередь, обусловливает возможность влияния на ее управляемые параметры, к которым относятся параметры механизмов защиты информации, с целью максимизации ее величины.

Задача реализации процесса управления защитой информации в ИСБ при отсутствии формальных моделей объекта и среды является специфичной задачей управления [1] и характерна для такого класса систем как ИСБ. Целевая функция управления определяется исходя из нахождения максимально эффективного состояния механизма защиты информации, а функция ограничений определяется исходя из минимально допустимой величины объема отвлекаемого функционального ресурса, необходимого для реализации этих механизмов. Таким образом, управление механизмом защиты информации в ИСБ определяется через задание цели и способа ее достижения.

В отличие от задач однокритериальной оптимизации, для организационно-технических систем, таких как механизмы защиты информации в ИСБ, характерен набор критериев, которые могут быть, как качественными, так и количественными, при этом один и тот же показатель в разных критериях может выполнять роль целевой функции и функции ограничений. Это обуславливает возможность варьирования набором таких критериев в зависимости от потребностей в обеспечении защищенности информации в ИСБ и отвлекаемых для этого ресурсов. Вместе с тем уникальность и динамичность ИСБ, а так же специфичность потребностей в защите не столько информации, столько информационных процессов и как следствие этого специфичность структуры и параметров механизмов защиты информации как объектов управления не позволяет сформировать регулярную формальную систему критериев оценки состояния защищенности информационных процессов в ИСБ, основанной на объективно измеряемых показателях. Отсюда и само определение набора критериев управления является оптимизационным процессом и является отдельной задачей управления.

С учетом особенностей ИСБ, управление защищенностью его информационных процессов можно определить как целенаправленное изменение структуры и параметров механизмов защиты информации, содержание которого состоит в определении критериев их функционирования и условий выполнения этих критериев. В итоге, в процессе управления необходимо первоначально варьировать критериями функционирования механизмов защиты информации в ИСБ, по которым впоследствии можно оценивать защищенность информационных процессов.

Для механизмов защиты информации в ИСБ М как объектов управления характерны следующие варианты реализации его алгоритмов:

1) реализация алгоритма управления механизмами защиты при фиксированном критерии;

2) варьирование критериями при фиксированном алгоритме управления;

3) изменение целей управления, предполагающее алгоритм управления, реагирующий на изменение условий использования механизмов защиты, которые, в свою

очередь, является следствием постоянного изменения условий функционирования ИСБ.

Несмотря на то, что последний вариант лежит за пределами инженерных подходов в случае повышения защищенности информационных процессов в ИСБ, вследствие специфичности такой системы, он является одним из основных способов совершенствования механизмов защиты информации в ИСБ.

В связи с этим рассмотрим модель управления механизмами защиты информации в ИСБ путем их совершенствования. При этом предполагается, что цель управления и его алгоритм, во-первых, известны и, во-вторых, формулируются субъектом управления, в качестве которого следует рассматривать лицо, принимающее решения о совершенствовании механизмов защиты информации в ИСБ М. Кроме этого, существует ряд упрощающих допущений:

– известность набора и значений оценочных критериев функционирования такого рода механизмов;

– тезаурусная и понятийная адекватность субъекта и устройства управления (проектировщика).

Вместе с тем, при реализации управлении механизмами защиты информации в ИСБ, перечисленные допущения не являются справедливыми. Это порождает трудности практической реализации управления в части оценки состояния защищенности информационных процессов.

Преодоление указанных трудностей осуществляется следующим образом. Априори субъектом определяется множество целей управления, под которыми подразумеваются модели требуемого субъектом качества Q обеспечения защищенности информационных процессов в ИСБ или некоторого перспективного состояния s_i, $i = 1, 2, \ldots, I$, механизма защиты информации, которое не может быть реализовано без управления.

Это приводит к необходимости, во время обеспечения защищенности информационных процессов в ИСБ, фиксирования субъектом внимания на тех параметрах механизма защиты информации $S_{(c)}$, которые определяют качество его функционирования и могут им изменяться в нужную сторону. В этом случае крайне важным является требование измеряемости параметров $S_{(c)}$. Такое восприятие механизма защиты информации можно представить конечным набором значимых и управляемых параметров

$$S_{(c)}(U)=(s_{(c)1}(U), \ldots, s_{(c)I}(U)),$$

где U – множество управляющих воздействий, осуществляемых субъектом.

Определим пространство управляемых ситуаций (ситуационное пространство) набором параметров s_i. Каждая точка такого пространства определяет конкретное качество обеспечения защищенности информационных процессов в ИСБ. Через ситуационное пространство $\{S_{(c)}\}$ субъект воспринимает механизм защиты информации. Любое изменение ситуации, вызванное изменением состояния механизма защиты, приводит к смещению точки $S_{(c)}$ вдоль определенной траектории данного пространства.

Вместе с тем, как правило, субъект не может воспринимать сложившуюся ситуацию $\{S_{(c)}\}$ и таким образом формулировать свои цели в терминах объекта $S_{(c)}$, оперируя лишь свойственными ему понятиями защищенности информации. В общем случае эти понятия и составляют понятие качества обеспечения защищенности информационных процессов в ИСБ. Тогда вектор качества:

$$Q_{(c)}=(q_{(c)1}, \ldots, q_{(c)I}), \quad (1)$$

представляет собой набор параметров качества q_i однозначно определяющихся текущей ситуацией $S_{(c)}$ (состоянием механизма защиты информации) т.е. $q_{(c)i}=$

$\psi_i(S_{(c)})$. При этом функция ψ_i определяет связь состояния механизма защиты информации $S_{(c)}$ и параметра качества $q_{(c)i}$. В векторной форме эта связь выражается в виде:

$$Q_{(c)}=\Psi(S_{(c)}), \quad (2)$$

где $\Psi(S_{(c)}) = (\psi_1(S_{(c)}),..., \psi_l(S_{(c)}))$ – определенная в пространстве состояний вектор-функция.

Таким образом, представление Ψ состояния механизма защиты информации $S_{(c)}$ через состояние качества обеспечения защищенности информационных процессов в ИСБ $Q_{(c)}$ позволяет субъекту формулировать свои цели в терминах и понятиях, связанных с измеряемыми, но не тождественных им. Учитывая, что требуемое качество обеспечения защищенности информационных процессов в ИСБ $Q_{(m)}$ может быть достигнуто при различных комбинациях значений показателей качества, имеет место следующая формальная система целей:

$$S_{(m)}:\begin{cases}\psi_i(S)=a_i,\\ \psi_i(S)\geq b_i,\\ \psi_i(S)\to \min(\max).\end{cases} \quad (3)$$

При этом точка, характеризующая состояние механизма защиты информации $s_{(m)i}$ из пространства ситуаций $S_{(m)}$, удовлетворяющая этим целям будет являться требуемым состоянием механизма защиты информации.

Формальный процесс формулирования вектора целей совершенствования обеспечения защищенности информационных процессов в ИСБ $Q_{(m)}$ включает:

– определение составляющих его показателей качества $q_{(m)i}$;

– определение вектор-функции $\Psi(S)$ (2);

– выработку требований, накладываемых на каждую составляющую этого вектора (3).

Из изложенного следует, что цель управления механизмами защиты информации в общем случае сводится к решению задачи:

$$Q(S)\to\max\Rightarrow S_{(m)}, \quad (4)$$
$$s_{(m)i}\in S_{(m)}$$

максимизации функционала $Q(S)$, путем варьирования оператором $s_{(m)i}$ в некотором определенном классе операторов $S_{(m)}$.

Таким образом вышеизложенное позволяет определить управление механизмами защиты информации в ИСБ как сложный процесс, протекающий на двух уровнях:

– прикладном: формулирование целевых решений $Q_{(m)}$ субъектом управления по совершенствованию обеспечения защищенности информационных процессов в ИСБ;

– проектном: выработка решений субъектом управления (собственно управление механизмами защиты информации).

Взаимосвязь уровней определяется правилом Ψ(2).

Такой подход позволит не только повысить уровень защиты информации с охраняемых объектов, но и улучшить информационную поддержку принятия решений дежурным персоналом ПЦО.

Литература:

1. Сошнева Д.А. Управленческие аспекты обеспечения защищенности информационных процессов в автоматизированных комплексах физической защиты / С.Ю. Рослов, А.А. Никитин, Д.А. Сошнева // Обеспечение безопасности информационных процессов и систем: сборник научных трудов. – Воронеж: ВГТУ, 2013. – С. 21–27.

Иващук О.А., Щербинина Н.В., Федоров В.И., Штана А.И.
Белгородский государственный национальный исследовательский университет

МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ БИОТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ НА ОСНОВЕ НЕЙРОСЕТЕВОГО МОДЕЛИРОВАНИЯ

Настоящее время характеризуется стремительным сокращением ареалов и исчезновением многих видов растений в связи с активной хозяйственной деятельностью человека [2,3]. Проблема сохранения и воспроизводства редких и исчезающих видов растений сегодня становится крайне актуальной [1,5]. Ее эффективное решение возможно при использовании технологии клонального микроразмножения, основанной на методе культуры клеток и тканей. В условиях *in vitro* не только удается укоренить те растения, которые трудно размножаются традиционным способом, но и получить достаточный объем материала для размножения редких и исчезающих растений [4,9].

Однако следует отметить, что процесс управления клональным микроразмножением растений и оптимизации его параметров для получения качественного посадочного материала, является длительным, трудоемким и затратным; требует постановки и повторения значительного числа лабораторных экспериментов. Кроме того, при анализе результатов подобных экспериментов необходимо работать с большими объёмами разнородной, иногда слабоструктурированной, информации.

Вышесказанное определяет перспективность использования при решении задач управления и оптимизации клонального микроразмножения растений современных средств информационных технологий, методов интеллектуального анализа данных, которые успешно применяются при прогнозировании и управлении процессами и объектами в различных сферах, в том числе при решении различных задач в биотехнологии (например, [6-8,10]).

В качестве растительных эксплантов рассматривались семена редких, исчезающих и лекарственных растений, относящиеся к семейству Labiatae Juss. (Lamiaceae) Губоцветные: *Bellevalia sarmatica* (Georgi) Woronow, *Nigella damascena* (L.), *Echinacea purpurea* (L), *Hyssopus cretaceus* Dubjan, *Prunella grandiflora* (L.) Sholl. и *Salvia sclarea* L., произрастающих на территории Белгородской области [3,4].

Осуществлялась разработка моделей оценки и прогнозирования результатов важнейшего этапа клонального микроразмножения растений – этапа стерилизации – с использованием аппарата искусственных нейронных сетей (ИНС). Конкретная топология и параметры ИНС определялись путем построения и последующей проверки на адекватность двух видов ИНС: многослойный персептрон и ИНС с радиальными базисными функциями – RBF-сеть. Варьировалось число скрытых слоев, число нейронов в скрытых слоях, а также вид функции активации.

Для оценки адекватности построенных моделей использовались следующие критерии: средняя квадратичная ошибка, минимизируемся в процессе обучения ИНС (*mse*); коэффициент детерминации (R^2); средние ошибки аппроксимации на обучающей и тестовой выборках ($\overline{A}_{об.}$ и $\overline{A}_{прог.}$ соответственно).

Для разработки и оценки адекватности моделей были сформированы обучающие и тестовые выборки по результатам лабораторных опытов по стерилизации семян трех видов растений семейства губоцветные: *B. Sarmatica, N. Damascena, E. Purpurea*. Данные лабораторные опыты проводились специалистами научной исследовательской лаборатории «Инновационные методы исследования растительных объектов» кафедры биотехнологии и микробиологии НИУ «БелГУ».

На основе разработанной модели проводились имитационные эксперименты для определения оптимальных параметров этапа стерилизации семян трех других видов растений (*H. Cretaceus, P. Grandiflora, S. Sclarea)*.

Для построения ИНС и осуществления имитационных экспериментов использовался пакет прикладных программ и функций Neural Network Toolbox системы MATLAB, позволяющий реализовывать ИНС различных парадигм.

Для получения модели, обеспечивающей возможность оценки и прогнозирования результатов этапов стерилизации растительных эксплантов с выбором оптимальных параметров, были реализованы ИНС двух парадигм: многослойный персептрон и RBF-сеть.

В результате исследования и оценки адекватности моделей с различными структурами получено, что лучшими прогностическими способностями обладает ИНС с 143 нейронами в скрытом слое и радиально-базисными функциями активации. Для данной модели: $mse = 10^{-6}$; $R^2 = 99{,}89$; $\overline{A}_{об.} = 0{,}86$ %, $\overline{A}_{прог.} = 0{,}98$ %. Ее общий вид в системе компьютерной математики MATLAB представлен на рисунке 1. В таблице 2 показаны результаты оценки адекватности ИНС с другими структурами, также показавшими хорошие результаты аппроксимации

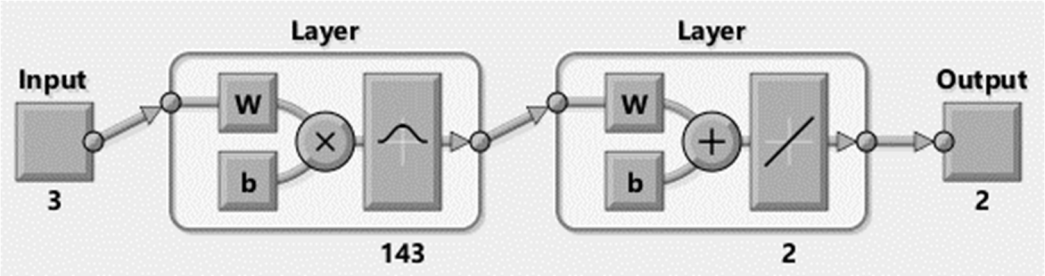


Рис. 1. Структура RBF-сети, реализованная в системе MATLAB.

Таблица 2

Результаты экспериментов для подбора характеристик ИНС

Топология сети	Количество нейронов в скрытом слое	Функция активация нейронов скрытого слоя	*mse*, 10^{-5}	R^2, %	$\overline{A}_{об.}$ %	$\overline{A}_{пр.}$ %
RBF	143	Радиально - базисная	0,1	99,89	0,86	0,98
Персептрон	9	Линейная	0,18	99,72	0,92	2,36
Персептрон	11	Линейная	0,14	99,87	0,77	4,64
Персептрон	15	Линейная	0,15	99,82	0,82	3,12
Персептрон	17	Линейная	0,19	99,75	0,88	4,18
Персептрон	19	Линейная	0,2	99,58	0,97	3,48
Персептрон	8	Сигмоидная	0,16	99,88	0,33	1,35
Персептрон	12	Сигмоидная	0,12	99,86	0,61	2,44
Персептрон	13	Сигмоидная	0,14	99,88	0,42	1,39
Персептрон	15	Сигмоидная	0,17	99,85	0,55	1,6

Входы ИНС: вид стерилизующего агента (X_1), его концентрация (X_2,%), время обработки растительных эксплантов (X_3,мин.); выходы: количество стерильных эксплантов (Y_1,%) и асептических жизнеспособных проростков (Y_2,%). Промежуточные слои отражают биохимические процессы.

Разработанная модель была использована для проведения имитационных экспериментов по выбору оптимальных параметров этапа стерилизации семян при введении в культуру *in vitro* других растений, относящихся к семейству губоцветных, произрастающих на территории Белгородской области, с которыми не проводились лабораторные эксперименты. На вход модели подавались различные комбинации параметров X_1, X_2, X_3 в более широком диапазоне пределов изменения и с меньшим шагом варьирования, чем это возможно реализовать в лабораторном эксперименте. Так, концентрация стерилизу-

ющего агента варьировалась в пределах от 1 до 100%, шаг 0,01, время стерилизации – 1÷30 мин., шаг 1. Результаты имитационных экспериментов по выбору оптимальных параметров представлены в таблице 1.

Таблица 1

Оптимальные параметры этапа стерилизации

Вид растения	Стерилизующий агент X_1	Время стерилизации X_3, мин	Концентрация стерилизующего агента X_2, %	Колличество стерильных эксплантов Y_1, %	Количество жизнеспособных эксплантов Y_2, %
H. cretaceus	Лизоформин 3000	9	7,12	74,2	15,9
P. grandiflora	Белизна (5-15%)	16	77,1	79,3	32,1
S. sclarea	Нитрат серебра	18	0,12	94,3	55,3

Построены и исследованы структуры ИНС двух парадигм: многослойный персептрон и RBF-сеть. Выбрана адекватная нейросетевая модель для проведения имитационных экспериментов по оценке и прогнозированию результатов процесса стерилизации с выбором оптимальных параметров: RBF-сеть с 143 нейронами в скрытом слое.

С помощью разработанной модели были проведены имитационные эксперименты и выбраны оптимальные параметры стерилизации для трех видов растений, относящихся к семейству губоцветных, для которых не проводился лабораторный эксперимент.

Литература:

1. Бутенко Р.Г., 1999. Биология клеток высших растений in vitro и биотехнологии на их основе. Москва: ФБК-ПРЕСС, 160 с.

2. Красная книга Российской Федерации (Растения, грибы) / Отв. редактор Л.В. Бардунов, В.С. Новиков. – Москва, 2008. – 847 с.

3. Красная книга Белгородской области. Редкие и исчезающие растения, грибы, лишайники и животные. Официальное издание / Общ. науч. ред. А.В. Присный. – Белгород, 2004. – 532 с.

4. Маслова Е.В., Гуля Н.И. Определение наиболее эффективного режима стерилизации растительных эксплантов редкого вида Astragalus albicaulis DS (Fabaceae) во флоре Белгородской области для получения его в культуре in vitro / Материалы сборника научных работ II-го Международного молодежного конкурса «Молодежь в науке: Новые аргументы». Отв. ред. А.В. Горбенко. – 2015. – С. 48-50.

5. Флинт, В.Е. Сохранение и восстановление биоразнообразия: серия учебных пособий / В.Е. Флинт. – М.: Издательство Научного и учебно-методического центра, 2002. – 286 с.

6. Gago, J.; Landín, M. & Gallego, P.P. Artificial neural networks modeling the in vitro rhizogenesis and acclimatization of Vitis vinifera L/ Journal of Plant Physiology, 167, 2010, 1226-1231.

7. Ivashchuk O.A., Lazarev S.A., Ivashchuk O.D., Fedorov V.I. Situational modeling for the control of technospheric safety/Journal of current research in science: 4 (1), 2016: 84-90

8. Ivashchuk Olga Alexandrovna, Igor Sergeevich Konstantinov, Sergej Aleksandrovich Lazarev, Vjacheslav Igorevich Fedorov. Research in the Field of Automated Environmental Safety Control for Industrial and Regional Clusters/ International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 22 (2014) pp. 16813-16820

9. Kikowska M., Thiem B., Sliwinska E., Rewers M., Kowalczyk M., Stochmal A., Długaszewska J. Micropropagation of eryngium campestre l. via shoot culture provides valuable uniform plant material with enhanced content of phenolic acids and antimicrobial activity/Acta Biologica Cracoviensia Series Botanica. 2016. Т. 58. № 1. С. 43-56.

10. Pedro P. Gallego, Jorge Gago and Mariana Landín. Artificial neural networks technology to model and predict plant biology process/ World's largest Science, Technology & Medicine Open Access book publisher, 2011.

Ивличев П.С., Трофимов М.Н.
Рязанский филиал
Московского университета МВД России имени В.Я. Кикотя

О ПРОБЛЕМЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Растущее количество информационных ресурсов и информационных технологий в мире приводит к естественному росту числа пользователей и к переходу многих традиционных форм взаимодействия людей в социуме в цифровую форму. Кроме того, цифровые технологии подразумевают создание принципиально иных форм взаимодействия людей в информационном обществе. В качестве примера можно привести, в частности, сервисы социальных сетей, технологии общения в реальном времени (мессенджеры).

Преступный мир достаточно оперативно отреагировал на появление новых технологий, создав новые методы совершения преступлений. Основным мотивом совершения таких преступлений является получение финансовой выгоды [5, 7]. Цифровые технологии породили совершенно новые принципы совершения краж, мошенничеств, вымогательств. В случае организованных преступных групп наиболее предпочтительными объектами для атак являются непосредственно собственники информационных ресурсов – банковские организации, государственные структуры, торговые организации и т.п.

Согласно мониторингу The Open Web Application Security Project для организованных атак на информационные ресурсы злоумышленники используют 10 групп методов [8]:

1. Инъекции.
2. Некорректная аутентификация и управление сессией.
3. Ошибки в шифровании.
4. Использование внешних сущностей XML.
5. Ошибки контроля доступа (использование ошибок системы контроля доступа и логических ошибок в приложениях).
6. Ошибки конфигурации системы безопасности.
7. Межсайтовый скриптинг.
8. Некорректная десериализация (deserialization).
9. Использование уязвимостей компонентов приложений.
10. Недостаточный уровень мониторинга.

Приведенный перечень составлен по убыванию частоты использования злоумышленниками.

Анализ механизма использования перечисленных методов показывает, что для их применения требуются специальные технические навыки и познания, а в ряде случаев успешность атаки зависит от наличия сообщника среди администраторов или разработчиков атакуемых ресурсов [5]. Разумеется, рядовой пользователь информационного ресурса в данном случае никак не может повлиять на безопасность своей личной информации.

Таким образом, к примеру, защита от инъекций баз данных – это прямая обязанность собственника этой базы данных. Даже корректное поведение пользователя не

поможет защитить свою информацию в базе данных, если злоумышленник выполнит к базе некорректный SQL-запрос на выборку.

Также пользователь никак не может повлиять на степень своей защищенности, если злоумышленниками используется уязвимость внешних сущностей XML. В этом случае совершается попытка внедрить в код страницы на сервере вредоносный скрипт, нацеленный на выдачу информации из базы. XML-страница и компьютер пользователя при этом никак не взаимодействуют.

Механизмы получения несанкционированного доступа с использованием ошибок системы контроля также опираются на некачественную работу собственников информационных ресурсов и разработчиков приложений по обеспечению информационной безопасности. Даже положительное поведение пользователя никак не поможет в случае, когда злоумышленник напрямую меняет содержимое адресной строки или применяет некорректные данные (эксплойт).

Защита со стороны пользователей от использования злоумышленниками ошибок в конфигурации системы безопасности невозможна в принципе, поэтому при использовании этих ошибок степень защищенности информации пользователя зависит от собственника информационного ресурса.

В период времени с 2013 года актуальной стала угроза несанкционированного доступа с использованием некорректной десериализации. Под этим термином The Open Web Application Security Project подразумевает перевод данных из файла в формат сетевого пакета. Злоумышленники анализируют хранящиеся на своем компьютере данные, полученные с ресурса (например, файлы cookie), и с помощью их изменения пытаются получить неавторизованный доступ к другим данным ресурса (например, записав себе в cookie права администратора ресурса) [8]. Появление уязвимости такого рода происходит из-за небрежности собственников ресурсов, не предпринимающих мер по шифрованию данных, записываемых на компьютер пользователя, или записывающих избыточную для взаимодействия с ресурсом информацию. Поведение пользователя никак не может повлиять в данном случае на его защищенность.

Использование остальных методов несанкционированного доступа к информации в той или иной мере зависит от действий пользователей.

К примеру, использование уязвимости, связанной с некорректной аутентификацией и управлением сессией, зависит не только от настроек сайта, но и от действий пользователя. К числу отрицательных действий в данном случае можно отнести сохранение пароля в браузере [4], [7] или распространение ссылок на ресурсы с данными о сессии авторизованного пользователя [7], [8].

Технологии межсайтового скриптинга подразумевают не только использование ошибок конфигурации системы безопасности сайта, позволяющие выполнять скрипты, расположенные на сторонних ресурсах, но и действия пользователя, активирующие выполнение скрипта. Зачастую злоумышленники, побуждая пользователя выполнить активацию требуемого объекта, используют методы социальной инженерии либо рассчитывают на недостаточные знания пользователя в области информационной безопасности [4], [7].

Согласно исследованиям [8], межсайтовый скриптинг в последние пять лет становится менее распространенным, а угроза межсайтовой подделки запроса в настоящее время не является актуальной. Во многом это связано с повышением безопасности при разработке сайтов и сетевых приложений [5]. Однако, технологии, аналогичные межсайтовому скриптингу, используются как составная часть иных методов несанкционированного доступа к информации [1].

За последние пять лет резко возросла доля случаев несанкционированного доступа к информации, осуществляемых с помощью ошибок шифрования [8]. Поскольку ис-

пользование защищенных протоколов передачи данных в настоящее время стало фактическим стандартом для обмена информации в сети интернет [5], можно обоснованно утверждать, что рост числа таких случаев обусловлен развитием атак, относящихся к классу man-in-the-middle (MITM-атаки). Традиционной проблемой MITM-атак в сети интернет является скрытие факта подключения постороннего устройства и перехвата ключей шифрования. Современные браузеры обладают развитыми средствами проверки сертификатов ключей, некоторые (Google Chrome, Yandex browser) не позволяют пользователю проигнорировать факт обнаруженного несоответствия сертификата. Очевидно, что успешность таких атак напрямую связана с использованием невнимательности пользователя, пренебрежения со стороны пользователя предупреждениями системы безопасности браузера, а также недооценкой пользователями возможностей злоумышленников по внедрению своих устройств в процедуру обмена информацией.

До сих пор в новостях проскальзывают сообщения об успешности атак с помощью организации бесплатных беспроводных сетей, либо с помощью контроля над маршрутизатором такой сети, хотя об опасности использования бесплатных сетей для передачи конфиденциальной информации было известно уже достаточно давно [4], [1].

Стабильно держится в статистике распространенных способов несанкционированного получения доступа к цифровой информации метод использования уязвимостей компонентов приложений. Полностью ликвидировать такую угрозу может только разработчик приложения, однако методы существенного снижения риска реализации такой угрозы известны и приведены во многих источниках, в частности, [4], [5]. Пренебрежение обновлением приложений, использование контрафактного программного обеспечения и программного обеспечения из недоверенных источников – таковы типичные действия пользователей, способствующие успешности таких атак.

В последние пять лет специалисты классифицировали новый тип атак на информационные ресурсы [8], основанный на недостаточном контроле над доступом к информационному ресурсу. Выделение такого класса может быть спорным, поскольку опирается не на действия злоумышленников, а на действия собственника информационного ресурса. Пользуясь отсутствием должного контроля над попытками доступа к ресурсу, злоумышленники могут совершать различные по своему механизму действия, направленные на доступ к информации пользователя, в частности, подбор пароля, инъекции, попытки обхода системы авторизации, использование данных авторизации, полученных из различных источников [6], [1].

Таким образом, в настоящее время существенная доля случаев несанкционированного доступа к информации в цифровой форме осуществляется с помощью некорректных с точки зрения безопасности действий пользователей.

Перечисленные выше методы получения несанкционированного доступа являются достаточно технологичными и используются специалистами в области информационных технологий, как правило, в составе преступных групп.

Другую сторону так называемой киберпреступности составляют «бытовые» преступления, осуществляемые, как правило, по мотивам мести. В данном случае получение финансовой выгоды и использование в качестве цели финансовых инструментов отходят на второй план. Основной целью преступлений в области охраняемой законом компьютерной информации, совершаемых по мотивам мести, являются персональные информационные ресурсы, такие, как электронная почта и страницы социальных сетей [3], [7].

В проводимых ранее исследованиях [2] были проанализированы типичные алгоритмы действий злоумышленников, направленные на получение доступа к ресурсам своей жертвы. Исследование проводилось на основе открытой информации, публикуемой при вынесении приговоров. Таким образом, в статистику не вошли незарегистри-

рованные случаи совершения преступлений и невыявленные преступления. В силу этого обстоятельства оценить достоверность полученных количественных характеристики невозможно.

Более информативна в плане исследований и выявления тенденций качественная картина. Анализируя типовые методы получения несанкционированного доступа к страницам социальных сетей и электронной почты, выделены следующие основные группы методов:

1. Вредоносные программы. Использование программ класса Password Steal Ware для получения доступа к электронной почте и страницам социальных сетей теряет популярность, поскольку в настоящее время эти ресурсы довольно хорошо защищены от атак методом грубой силы, а хранение паролей в браузерах стало более безопасным. Программы класса PSW (по классификации Лаборатории Касперского) чаще используются для получения доступа к аккаунтам иных ресурсов: онлайн-магазинов, онлайн-игр. Поскольку преступления по мотивам мести, как правило, совершаются знакомыми или родственниками жертвы, часто используются утилиты удаленного администрирования, установка которых на компьютер часто не представляет сложностей.

2. Фишинг. Под этим термином понимается группа методов, направленных на получение данных аутентификации непосредственно от пользователя информационного ресурса [6], [1]. Современные технологии фишинга многообразны и далеко не всегда связаны с классическим созданием дубликатов информационных ресурсов. В случае наличия контактов с жертвой вне сети интернет возможна организация мистификаций по телефону или посылкой адресного электронного письма. Такой персонифицированный фишинг более опасен в сравнении с массовыми рассылками, поскольку жертва лишается возможности проверки письма в интернет-сообществе и использования для принятия решений мнения более опытных пользователей.

3. Заказ «взлома». Такие случаи стали регистрироваться на территории Российской Федерации. В конце нулевых годов использование баз паролей для доступа в сеть интернет носило довольно массовый характер. С повышением доступности сети интернет доступ как цель совершения преступлений ушел в прошлое, а с распространением хэширования паролей само понятия «база паролей» стало неактуальным. Однако, с развитием «теневого» интернета появились торговые площадки, торгующие паролями, полученными, к примеру, с помощью массового фишинга. В настоящее время на таких площадках можно заказать пароли от аккаунтов социальных сетей, интернет-магазинов.

4. Использование сохраненного пароля. В случае, когда преступник и жертва состояли в близких отношениях, общее использование информационных ресурсов не рассматривается большинством людей как нарушение правил информационной безопасности, хотя, по сути, сохранение паролей от личных ресурсов на чужих компьютерных устройствах делает возможным использование некорректной аутентификации и управления сессией и сводит на нет всю работу разработчиков браузеров по безопасному хранению паролей. Как показывает анализ судебной практики [2], сохраненный на устройстве злоумышленника пароль занимает одно из лидирующих мест среди способов несанкционированного доступа в информационным ресурсам жертвы. Другой категорией лиц, использующих сохраненный пароль для несанкционированного доступа, являются лица, проводящие техническое обслуживание компьютерных устройств. Также известны случаи, когда сохраненный в программном обеспечении пароль использовали лица, купившие технику, бывшую в употреблении.

5. Подбор пароля. Использование злоумышленниками этого метода наглядно показывает, что многочисленные статьи, посвященные формированию устойчивого к перебору пароля, далеко не всегда принимаются к сведению пользователями информаци-

онных ресурсов. В случае, когда жертва и злоумышленник были тесно знакомы друг с другом, использование в качестве пароля любой личной информации является абсолютно ненадежным методом защиты, поскольку все личные данные, как правило, уже известны злоумышленнику.

6. Получение пароля из источника. В качестве источника для данный идентификации и аутентификации могут использоваться различные ресурсы – записи в мобильном телефоне, сим-карта, электронная почта и «классические» стикеры на компьютерном устройстве. Анализ уголовной практики показывает, что многие потерпевшие достаточно халатно относятся к факту утери телефона, привязанного к банковской карте или к привязке к банковской карте сим-карты, оформленной на другое лицо.

7. Пароль доверен собственником. К сожалению, доверяя данные идентификации близкому человеку, пользователи не в состоянии оценить развитие отношений с этим человеком и, зачастую, в случае разрыва отношений становятся жертвами мести. Скопированные интимные фотографии, удаленные аккаунты, публикация личной переписки – это наиболее часто встречающиеся действия злоумышленников, которые стали возможны из-за того, что когда-то собственником информационных ресурсов им был доверен пароль.

В целом, анализ компьютерной преступности на бытовом уровне и в сфере действия организованной преступности показывает, что несмотря на наличие опыта в использовании информационных технологий, активную просветительскую работу в средствах массовой информации, многие преступления совершаются из-за уязвимостей, использование которых обусловлено некорректными действиями пользователей. В связи с этим, перспективным выглядит разработка мер защиты, позволяющих снизить риск неправомерного доступа к информации вне зависимости от действий пользователя.

Такие действия, в частности, предпринимались операторами сотовой связи, отключавшими СМС-сообщения при замене сим-карты. К таким же действиям можно отнести изменение процедур онлайн-банкинга, связанных с отказом от СМС-команд и идентификации посредством одноразовых паролей и постоянных кодов доступа.

Литература:

1. Белова А.А., Немытова Е.В., Шилов А.К. Фишинг: характеристики и технологии. // Теория и практика современной науки. 2016. № 4 (10). С. 126-129.

2. Ивличев П.С., Ивличева Н.А. Современные средства идентификации и аутентификации пользователей популярных информационных ресурсов и методы их обхода злоумышленниками // Математические методы и информационные технологии управления в науке, образовании и правоохранительной сфере: сборник материалов Всероссийской научно-технической конференции. Московский государственный технический университет имени Н.Э. Баумана, Академия ФСИН России, Рязанский государственный университет имени С.А. Есенина. 2017. С. 65-68.

3. Ивличев П.С., Ивличева Н.А. Структура преступлений в сфере компьютерной информации в Российской Федерации в 2010-2014 гг. // Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. (Минск, 31 марта 2016 г.) / ред. кол. А. В. Яскевич (отв. ред.). Минск, 2016. С. 74-77.

4. Информационная безопасность населения как средство противодействия преступности в финансово-кредитной сфере: учебно-методическое (учебно-практическое) пособие / Корнилович Р.А., Ивличев П.С., Ивличева Н.А., Коноваленко С.А., Ребров А.А., Пинчук Л.В. Рязань, 2017. – 61 с.

5. Савин Г.Е., Страхов А.А., Дубинина Н.М., Александров Ю.Н. Обеспечение информационной безопасности государственных, коммерческих и банковских структур при использовании глобальных сетей // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: материалы Всероссий-

ской научно-практической конференции / под общей редакцией: В.И. Третьякова, Н.В. Ходяковой. 2012. С. 10-22.

6. Хачатурова С.С., Жихарева Ю.П. Осторожно, фишинг! // Международный журнал прикладных и фундаментальных исследований. 2016. № 4-4. С. 793-795.

7. Чеботарева Е.А., Борисов Б.В. Особенности преступлений в сфере информационных технологий // Технологии информационной безопасности в деятельности органов внутренних дел Сборник научных трудов XIII научно-практической конференции. 2016. С. 127-130.

8. OWASP Top 10 – 2017. [Электронный ресурс] Режим доступа: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Ивличева Н.А.
Рязанский филиал
Московского университета МВД России имени В.Я. Кикотя

К ВОПРОСУ О ДОВЕРИИ К СПОСОБАМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В современном обществе использование информационных ресурсов различного плана давно стало обыденностью. Развитие программы «Информационное общество» привело к тому, что значительная доля населения страны использует информационно-телекоммуникационные ресурсы для общения, получения государственных услуг, совершения финансовых операций, осуществления трудовой деятельности, развлечений и т.п.

Информационные технологии вывели многие перечисленные сферы на принципиально иной уровень оказания услуг, удобства, времени ожидания. Однако оборотной стороной комфортности сервисов является проблема безопасности использования ресурсов [6].

Использование информационных ресурсов тесно связано с проблемой идентификации и аутентификации пользователей. Без обхода систем идентификации и аутентификации ни одна атака злоумышленника не может быть успешной и привести к негативным последствиям для собственника информации. Организаторами обмена информации и собственниками информационных ресурсов разрабатываются и поддерживаются различные механизмы, ограничивающие доступ к информации вопреки желанию владельца [4], [1].

Создавая системы идентификации и аутентификации, помимо вопросов надежности собственник информационного ресурса учитывает и стоимость такой системы, и удобство ее эксплуатации. Поскольку в большинстве случаев в качестве собственников ресурсов выступают коммерческие структуры, заинтересованные в первую очередь в большом количестве пользователей, вопросы снижения издержек на создание и эксплуатацию системы защиты, а также вопросы ускорения обработки информации выходят на первый план, негативно влияя на безопасность использования ресурса [2].

В краткосрочной перспективе пренебрежение вопросами обеспечения безопасности со стороны организатора обмена информацией или собственника информационного ресурса приносит ему выгоду, поскольку все риски по использованию ресурса традиционно ложатся на пользователя, однако, в долгосрочной перспективе такая политика наносит ущерб репутации владельца ресурса и заставляет его принимать меры по усилению информационной безопасности своих пользователей [2].

Как показывает уголовно-правовая статистика [3], преступный мир довольно быстро адаптируется к новым методам защиты, разрабатывая методы обхода новых алгоритмов и средств авторизации пользователей [6]. При этом далеко не все методы яв-

ляются высокотехнологичными и требуют специальных технических навыков. Во многих случаях злоумышленниками используются ошибки в методике применения средств защиты или недостаточный уровень информационной культуры пользователей [5].

В рамках повышения информационной культуры пользователей организаторами обмена информацией и собственниками информационных ресурсов проводится активная работа. Разрабатываются памятки пользователю, выходят тематические статьи и передачи в средствах массовой информации. В Рязанском филиале Московского университета МВД России имени В.Я. Кикотя в 2016 году проводилось научное исследование, посвященное проблемам информационной безопасности при использовании платежных инструментов [4], по итогам которого был разработан ряд методических и научных материалов.

Одной из проблем, связанных с повышением уровня информационной культуры населения и доверия к безопасности информационных ресурсов, является появление в средствах массовой информации материалов, которые не вполне корректно освещают проблемы информационной безопасности при использовании различных информационных технологий. Уровень угроз в таких материалах может быть как преувеличен, так и преуменьшен. Аналогичные сведения можно встретить в социальных сетях. Опасность такого рода информации заключается в формировании необоснованного мнения о степени защищенности информационных продуктов различного вида.

Для обозначения проблемы формирования адекватного представления о реальном уровне информационной безопасности ресурсов было проведено исследование на определение уровня доверия пользователей к различным механизмам идентификации на информационных ресурсах.

Перечень механизмов составлялся на основе изучения современных информационных продуктов, представленных в различных сферах общественной жизни. В перечень вошли следующие механизмы идентификации пользователей:

1. Идентификация путем подтверждения личности пользователя посредством видеосвязи. Такая идентификация используется, в частности, при организации дистанционного обучения, при осуществлении трудовой деятельности удаленным способом.

2. Идентификация путем ответа на заранее определенный контрольный вопрос. Такая идентификация используется на некоторых почтовых сервисах и в электронных образовательных средах.

3. Идентификация с помощью биометрических данных (отпечатки пальцев, форма лица, сетчатка глаза и т.п.). Такая идентификация используется для доступа к рабочему месту пользователя и к облачным хранилищам информации.

4. Идентификация с помощью квалифицированной (имеющей сертификат) электронной подписи. Такая идентификация используется в системах электронного документооборота.

5. Идентификация с помощью установленного в смартфоне (планшете) приложения (путем простого запуска приложения). Используется для удаленного доступа к различным информационным ресурсам (интернет-магазинам, страницам социальных сетей, и т.п.).

6. Идентификация с использованием токена (устройства, подключаемого к компьютеру) с вводом пин-кода. Такая идентификация используется в системах электронного документооборота и для доступа к автоматизированному рабочему месту. В ряде случаев используется для онлайн-банкинга.

7. Идентификация с использованием смарт-карты. Используется для доступа к автоматизированному рабочему месту.

8. Идентификация путем ввода данных документа (паспорта, пропуска, удостоверения и т.п.). Используется в ряде организаций для доступа к автоматизированному рабочему месту, а также в некоторых организациях страховой сферы.

9. Идентификация с помощью поочередного ввода одноразовых паролей из выданного заранее списка. Используется в финансово-кредитной сфере для подтверждения операций через интернет-банк.

10. Идентификация с помощью кода, присылаемого на адрес электронной почты. Используется в ряде онлайн-магазинов, а также для восстановления паролей к другим интернет-ресурсам.

11. Идентификация с помощью кода, присылаемого по СМС на номер телефона. Используется в качестве системы вторичной идентификации на многих интернет-ресурсах.

12. Идентификация вводом пары логин/пароль. Классический способ идентификации пользователя, используемый либо в качестве первичной идентификации, либо в качестве единственного этапа идентификации пользователя.

Указанные методы идентификации пользователя были оценены экспертом в области информационных технологий, входящим в рабочую группу научного исследования. Оценка проводилась методом ранжирования по уровню безопасности с обоснованием выставления ранга, основываясь на судебной практике и оценке вероятности обхода средства идентификации с учетом квалификации злоумышленника. Мнение эксперта было согласовано с другим экспертом методом ранговой корреляции. Коэффициент Спирмена равный 0,864 подтвердил высокую степень согласованности мнений по оценке уровня безопасности методов идентификации пользователей.

Учитывая, что значительная часть преступлений осуществляется в финансово-кредитной сфере [3], к оценке был привлечен эксперт из этой области, согласованность мнения которого оказалась довольно низкой – с оценками других экспертов совпали только две первые позиции, в остальных разница в рангах достигала 7. Эксперт в финансово-кредитной сфере пояснил, что делал оценки с учетом соблюдения рекомендованных правил использования механизмов идентификации без учета халатности или злого умысла со стороны участников обмена информацией.

Таким образом, для дальнейшего исследования были сформированы две шкалы, с которыми проверялось на согласованность мнение исследуемой группы.

В качестве опрашиваемых лиц были выбраны лица из возрастной группы 20-25 лет, поскольку эта группа активно использует информационные ресурсы различных видов. Опрос проводился анонимно. Результаты опроса были проверены на согласованность с мнениями двух экспертов. Средняя согласованность с мнением эксперта по информационной безопасности составила 0,545 (коэффициент Спирмена), с экспертом в финансово-кредитной сфере – 0,699.

Единственной совпавшей оценкой анкетируемых с экспертами оказалась низкая оценка защищенности информационных ресурсов с помощью мобильных приложений. Такая оценка обусловлена со стороны экспертов уязвимостью API мобильных платформ и пренебрежением информационной безопасностью со стороны заказчиков мобильных приложений. Многочисленные инциденты со стороны мобильных банковских приложений [6], [1] привели к тому, что пользователи не доверяют этому механизму идентификации, хотя в последнее время в мобильных приложениях используется и вторичная идентификация, и ограничение времени сессии. Пользователи готовы использовать мобильные приложения, но в сферах, где риск потери денежных средств невысок.

Более высокий уровень согласованности мнений пользователей с мнением эксперта в финансово-кредитной сфере может означать успешность работы по формиро-

ванию доверия к использованию информационных технологий. В тройку методов идентификации и аутентификации, заслуживающих наибольшего доверия, вошли следующие:

1. Идентификация путем подтверждения личности пользователя посредством видеосвязи.

2. Идентификация с помощью биометрических данных (отпечатки пальцев, форма лица, сетчатка глаза и т.п.).

3. Идентификация с помощью квалифицированной (имеющей сертификат) электронной подписи.

Следует отметить, что только третий из перечисленных методов в настоящее время сравнительно часто применяется в банковском секторе. Высокая степень доверия к биометрическим системам сформирована у пользователей на основе бытового опыта использования таких систем и устройств и, в целом, соответствует экспертной оценке уровня надежности этой технологии.

В связи с этим планируемое многими банковскими структурами массовое внедрение таких систем, скорее всего, найдет поддержку среди клиентов.

В то же время определенную настороженность вызывает высокая степень доверия пользователей к использованию электронной подписи. Опрос респондентов и беседа с экспертом в финансово-кредитной сфере показали, что многие респонденты не имеют надлежащего преставления об угрозах, связанных с несанкционированным использованием квалифицированной электронной подписи, и о мерах безопасности при ее использовании. В то же время, в судах общей юрисдикции рассматриваются дела, связанные с неправомерным проведением финансовых операций с использованием электронной подписи. В большинстве случаев ключ и сертификат подписи злоумышленники получают путем злоупотребления доверием потерпевших, либо используя халатное отношение потерпевших к безопасности применения ключа. Значительная часть пользователей не представляют, каким образом электронную подпись необходимо защищать от несанкционированного использования.

Среди методов идентификации, вызывающих наибольшее недоверие среди пользователей, лучшую согласованность показала идентификация путем использования мобильного приложения. Респонденты и эксперт в финансово-кредитной сфере поставили этот метод идентификации пользователей информационных ресурсов на последнее место. Невысокую оценку этот метод получил и у эксперта в области информационной безопасности. Незащищенный интерфейс разработчика, возможность неавторизованного доступа при доступе к устройству, возможность наличия методических ошибок в шифровании и управлении сессией пользователя адекватно указывают на ненадежность этого метода.

В последнее время собственники информационных ресурсов, разрабатывающие мобильные приложения, стали подходить к вопросам информационной безопасности более ответственно. Многие современные приложения имеют механизмы вторичной идентификации, ограничения по времени для сессии и для своей работы не требуют доступа к неиспользуемым фактически ресурсам системы. Также шагом, направленным на повышение информационной безопасности, является решение ряда разработчиков ограничить функционал приложений при использовании беспроводных сетей. Таким образом, в случае блокирования SIM-карты доступ к данным приложения становится, как минимум, затрудненным, либо невозможным вообще.

Серьезные опасения вызывает доверие пользователей и эксперта в финансово-кредитной сфере к такому методу идентификации, как ввод данных документа. Мнение опрашиваемых и эксперта опирается на то, что данные документов, в соответствии с законодательством, относятся к персональным данным и не могут быть известны тре-

тьим лицам. Однако, реальное положение дел в этой области далеко от идеального. Персональные данные граждан регулярно запрашиваются организациями и государственными структурами, однако контроль за действиями операторов персональных данных в России находится на уровне, не обеспечивающем их адекватную защиту. Случаи утечки данных паспортов и других документов носят далеко не единичный характер [5], [1], однако многие пользователи считают вполне надежной авторизацию, в которой в качестве пароля выступает номер паспорта. Все опрашиваемые имеют адекватное представление о вопросах предоставления своих паспортных данных, но многие не имеют реального представления о случаях неправомерного использования их персональных данных операторами [6].

Существенное расхождение по результатам опроса наблюдается среди оценок эксперта и пользователей, касающихся методов вторичной идентификации:

1. Идентификация с помощью поочередного ввода одноразовых паролей из выданного заранее списка.

2. Идентификация с помощью кода, присылаемого на адрес электронной почты.

3. Идентификация с помощью кода, присылаемого по СМС на номер телефона.

Эксперт в области информационной безопасности отнес эти методы к вполне надежным, но пользователи и эксперт в финансово-кредитной сфере считают, что эти методы не вызывают доверия.

Беседа с пользователями, принимавшими участие в опросе, показала, что причиной такого отношения во многих случаях является халатность пользователей, связанная с использованием средств коммуникации.

Так, многие пользователи доверяют работу со своим почтовым ящиком третьим лицам. Многие используют SIM-карты, оформленные на других людей. Многие пренебрегают средствами защиты мобильных устройств от несанкционированного использования.

Следует признать, что в таких условиях перечисленные методы идентификации не могут обеспечить адекватный уровень защиты информационных ресурсов пользователей, однако это мнение не связано с объективными возможностями защиты, предоставляемыми такими методами.

Таким образом, результаты предварительного исследования в области доверия к безопасности использования средств идентификации и аутентификации пользователей выявили следующие проблемы:

1. Пользователи не готовы соблюдать требования информационной безопасности использования средств идентификации, поскольку при соблюдении они лишаются определенной степени комфортности использования ресурса.

2. Пользователи не имеют представления о реальном количестве злоупотреблений со стороны операторов персональных данных и сотрудников собственников информационных ресурсов.

3. Даже в случае устранения недостатков способа идентификации не происходит быстрого восстановления доверия к этому способу.

Проведенное исследование и анализ результатов позволяют обратить внимание на важность формирования информационной культуры граждан в целом. Несоблюдение рекомендуемых специалистам мер безопасности приводит к неверному представлению об особенностях, достоинствах и недостатках конкретных методов идентификации и аутентификации пользователей.

Также потенциально серьезную проблему представляет отсутствие единой точки зрения экспертов из разных областей к вопросам информационной безопасности при эксплуатации информационных ресурсов.

Литература:

1. Бондарчук О.П., Ляшенко К.В. Новые виды мошенничества с платёжными картами в России // Аллея науки. 2017. № 15. Т.2. С. 275-278.

2. Ивличев П.С., Ивличева Н.А. Информационные технологии обеспечения безопасности платежных средств в свете современных тенденций в киберпреступности // Экономика и предпринимательство. 2017. № 2-1. С. 135-139.

3. Ивличев П.С., Ивличева Н.А. Структура преступлений в сфере компьютерной информации в Российской Федерации в 2010-2014 гг. // Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. (Минск, 31 марта 2016 г.) / ред. кол. А. В. Яскевич (отв. ред.). Минск, 2016. С. 74-77.

4. Информационная безопасность населения как средство противодействия преступности в финансово-кредитной сфере: учебно-методическое (учебно-практическое) пособие / Корнилович Р.А., Ивличев П.С., Ивличева Н.А., Коноваленко С.А., Ребров А.А., Пинчук Л.В. Рязань, 2017. – 61 с.

5. Каширина Е.А., Курганов А.Н. Анализ основных угроз безопасности банковских сервисов в потребительском секторе // Современные научные исследования и инновации. 2018. № 1 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2018/01/85489 (дата обращения: 22.01.2018).

6. Савин Г.Е., Страхов А.А., Дубинина Н.М., Александров Ю.Н. Обеспечение информационной безопасности государственных, коммерческих и банковских структур при использовании глобальных сетей // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: материалы Всероссийской научно-практической конференции / под общей редакцией: В.И. Третьякова, Н.В. Ходяковой. 2012. С. 10-22.

Каменецкая Н.В., Медведева О.М.
Санкт-Петербургский университет ГПС МЧС России

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МЕТОДОВ ДЛЯ ЭФФЕКТИВНОГО РЕШЕНИЯ УПРАВЛЕНЧЕСКИХ ЗАДАЧ В ДЕЯТЕЛЬНОСТИ МЧС РОССИИ

Рассмотрена возможность комплексного применения методов теории графов, динамического и линейного программирования, исследования операций при обосновании решений в системе управления МЧС России. Приведены практические примеры оптимизации оперативной деятельности подразделений МЧС России методами математического моделирования.

Математическая модель, исследование операций, система массового обслуживания, оптимизация оперативной деятельности, подразделения МЧС

Эффективное применение сил и средств МЧС России для выполнения широкого спектра задач по предназначению в существенной степени зависит от деятельности системы управления, связанной с разработкой оптимальных управленческих решений.

При планировании мероприятий по поставленной задаче руководитель управления МЧС России соответствующего уровня сталкивается с необходимостью разработки наиболее рациональных в ожидаемых условиях обстановки структуры и способов действий подчиненных сил и средств. Для научного обоснования таких изысканий могут быть применены принципы теории принятия решений и исследования операций, включающих как методы математического моделирования, так и методы оптимизации. Более того, в ряде случаев возможно комплексное использование указанных методов [1].

Приведем примеры применения методов математического моделирования для оптимизации оперативной деятельности подразделений МЧС России в повседневной работе и при ликвидации чрезвычайных ситуаций (ЧС).

1. Формирование оптимальных маршрутов передвижения сил и средств отрядов спасателей МЧС в зону ЧС с применением методов теории графов.

Первоочередная задача при возникновении ЧС – спасение людей. Чтобы предотвратить гибель пострадавших, спасатели должны прибыть на место происшествия максимально быстро.

Очевидно, что проблема поиска оптимальных маршрутов передвижения сил и средств подразделений спасателей в условиях ограничения времени является одной из наиболее актуальных в деятельности МЧС России.

Ввиду того, что на рассматриваемой территории в зоне ЧС может находиться большое число (несколько десятков) населенных пунктов, а также возможных маршрутов передвижения, то для формализации поставленной задачи применим математический аппарат теории графов и методы решения экстремальных задач на графах.

Наиболее эффективным следует считать такой алгоритм, который позволит доставлять силы и средства не только в кратчайшие сроки, но и во все без исключения населенные пункты в зоне ЧС. Для достижения этой цели можно рассмотреть в теории графов различные методы поиска так называемых гамильтоновых циклов, или, в крайнем случае, гамильтоновых путей.

Для отыскания всех кратчайших маршрутов передвижения сил и средств подразделений МЧС в условиях ограничения времени в заданном районе (следования пожарно-спасательных отрядов на место возникновения пожара с целью его ликвидации в кратчайшие сроки) применяется алгоритм Дейкстры нахождения кратчайшего дерева графов [2].

2. Оптимизация структуры Центра управления в кризисных ситуациях (ЦУКС) МЧС России с применением теории графов.

ЦУКС МЧС России является головным органом повседневного управления Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС). Он создан в целях осуществления специальных и управленческих функций, координации деятельности подразделений федеральной противопожарной службы Главного управления МЧС России.

Основная цель оптимизации структуры ЦУКС МЧС России – это обеспечение возможности максимально эффективного достижения целей системы в рамках принятых стратегий. Все задачи, возлагаемые на ЦУКС, должны выполняться оперативно и точно.

С точки зрения математического моделирования удобно рассматривать структуру ЦУКС МЧС России в виде ориентированного графа.

Для решения задачи оптимизации организационно-штатной структуры ЦУКС соответствующий ориентированный граф может быть представлен в виде уровневого графа, в котором четко просматривается иерархия, что позволяет удалить возможно лишние (дублирующие функции) связи [3].

Далее, выделяя сильные компоненты ориентированного графа и построив граф конденсации, можно определить сильно связанные компоненты. В организационно-штатной структуре ЦУКС сильные компоненты соответствуют отдельным службам. Существует также возможность проверить избыточность данной структуры.

Целесообразность моделируемой оптимизации структуры можно оценить с помощью математических методов. Проводится выбор соответствующих показателей, выполняются необходимые расчеты, формируется вывод об эффективности планируемой операции.

3. Применение методов динамического программирования для планирования мероприятий на проведение взрывных работ на реках в паводковый период.

Ежегодно в ряде регионов Российской Федерации ввиду их природно-климатических и хозяйственно-экономических особенностей наблюдаются весенние паводки, возникающие в результате опасного гидрологического природного явления – повышения уровня воды в реках в период весеннего таяния снежных покровов и вскрытия рек ото льда, и являющегося во многих случаях источником возникновения чрезвычайных ситуаций.

Силы и средства функциональной и территориальной подсистем РСЧС *проводят превентивные мероприятия по предотвращению наводнений и смягчению их возможных последствий в период весеннего половодья, в том числе, подготовку и проведение взрывных работ по предупреждению и ликвидации заторов льда на реках. И*спользование методов математического моделирования позволяет провести наиболее эффективное планирование таких мероприятий.

Решение задачи рационального *распределения взрывчатых веществ при проведении превентивных инженерно-саперных работ на трех реках с целью предотвращения паводков найдено с применением принципа оптимальности и функционального уравнения Беллмана [4].*

4. Оптимизация оперативной деятельности подразделений МЧС России с применением теории массового обслуживания.

4.1. Математическое моделирование при решении задач обоснования структуры и организации функционирования мобильного госпиталя МЧС России.

Одним из важнейших направлений деятельности МЧС России является оказание экстренной медицинской помощи пострадавшим в местах ликвидации чрезвычайной ситуации. В этих целях аварийно-спасательные формирования МЧС России оснащаются мобильными госпиталями, обладающими способностью к быстрой доставке и развертыванию в зоне ЧС.

При возникновении ЧС со значительным количеством пострадавших, нуждающихся в медицинской помощи, весьма актуальной становится проблема оптимизации структуры и организации функционирования как отдельных элементов, так и всего разворачиваемого в зоне бедствия мобильного госпиталя. Решение задачи может быть осуществлено с использованием методов теории массового обслуживания [5]. В этом случае работу мобильных госпиталей можно представить как функционирование системы массового обслуживания (СМО).

4.2. Применение методов математического моделирования для решения задачи выявления и оценки радиационно-химической и биологической (РХБ) обстановки в зоне ЧС.

Наибольшую опасность для человечества в настоящее время представляют крупные техногенные аварии и катастрофы, акции технологического терроризма, а также масштабные загрязнения природной среды долгоживущими радиоактивными, химическими и биологическими веществами.

Для предотвращения поражений среди населения и личного состава формирований МЧС России, оказавшихся в зонах радиационного, химического и биологического заражения, проводится комплекс мероприятий, получивших название «РХБ защита» и направленных, в первую очередь, на выявление и оценку радиационной, химической и биологической обстановки.

Математические методы позволяют решить задачу выбора оптимального распределения времени обслуживания между средствами радиационной разведки и средствами обработки информации в комплексе. Такая оптимизация выполняется в два этапа.

На первом этапе методами теории массового обслуживания определяются исходные показатели, характеризующие функционирование каждой СМО в оптимальном режиме, в том числе определяется оптимальное среднее время обслуживания. На втором этапе методами линейного программирования производится перераспределение времени обслуживания между всеми СМО в рамках единого комплекса при минимизации целевой функции – математического ожидания времени обработки информации. Улучшение плана распределения времени обслуживания осуществляется классическим симплекс-методом [6].

4.3. Оценка риска отказа в работе специальной техники в ходе ликвидации ЧС.

Методы теории массового обслуживания могут быть применены для предварительной оценки, учета и предупреждения рисков, связанных с применением «ненадежной», то есть временно находящейся в нерабочем состоянии или в состоянии ремонта, специальной техники пожарно-спасательных подразделений в ходе выполнения аварийно-спасательных работ [7].

Рассматривается СМО с отказами, в которой допускается применение «ненадежных» условных средств обслуживания. В такой системе каждый вновь поступивший объект может получить отказ не только в случае занятости всех средств обслуживания, но и тогда, когда часть средств занята обслуживанием других объектов, а оставшаяся часть находится в нерабочем состоянии. При этом предполагается, что выход из строя средства одинаково возможен как на этапе применения, так и в период подготовки его к использованию.

Расчеты позволяют выработать практические рекомендации для повышения надежности работы специальной техники, устранять или корректировать риски, связанные с временно не работающей и восстанавливаемой специальной техникой, и управлять этими рисками для поддержания постоянной высокой готовности сил и средств пожарно-спасательных подразделений Федеральной противопожарной службы МЧС России.

Литература:

1. Каменецкая Н.В., Медведева О.М., Хитов С.Б. Комплексное использование методов исследования операций при обосновании управленческих решений в системе управления МЧС России // Приоритетные научные направления: от теории к практике. 2016. № 30. С. 92-99.

2. Каменецкая Н.В., Кусайло Ф.А. Нахождение оптимальных маршрутов передвижения отрядов спасателей МЧС в зоне ЧС на основе применения теории графов // Современное образование: содержание, технологии, качество. 2016. Т. 2. С. 175-176.

3. Сорока А.В., Каменецкая Н.В. Применение теории графов для оптимизации структуры Центра управления в кризисных ситуациях (ЦУКС) МЧС России // Современное образование: содержание, технологии, качество. 2016. Т. 2. С. 172-174.

4. Каменецкая Н.В., Медведева О.М., Хитов С.Б. Математическое моделирование при планировании мероприятий на проведение взрывных работ на реках в паводковый период // Современные тенденции развития науки и технологий. 2016. № 6-1. С. 22-27.

5. Каменецкая Н.В., Медведева О.М., Хитов С.Б. Математическое моделирование при решении задач обоснования структуры и организации функционирования мобильного госпиталя МЧС России // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2016. № 1. С. 62-67.

6. Каменецкая Н.В., Медведева О.М., Хитов С.Б. Применение методов математического моделирования при решении задачи выявления и оценки радиационной, химической и биологической обстановки в зоне чрезвычайной ситуации // Проблемы управления рисками в техносфере. 2016. № 2 (38). С. 64-69.

7. Каменецкая Н.В., Медведева О.М., Хитов С.Б., Маслаков М.Д. Методика оценки риска отказа в работе специальной техники в ходе ликвидации чрезвычайной ситуации. России // Пожаровзрывобезопасность / Fire and Explosion Safety. – 2018. – Т. 26. № 2-3. – С. 5-13.

Карпика А.Г., Лемайкина С.В.
Ростовский юридический институт МВД России

ЗАКОНОДАТЕЛЬНЫЙ И ТЕХНОЛОГИЧЕСКИЙ АСПЕКТЫ ФОРМИРОВАНИЯ ЕДИНОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА МВД РОССИИ

В настоящее время в Российской Федерации решается комплекс стратегических задач, направленных на развитие всех видов образования. Приоритетные направления государственной политики в этой области определяются нормами Федерального закона от 29 декабря 2012 г. N 273-ФЗ (ред. от 07.03.2018) "Об образовании в Российской Федерации" [1], Указа Президента Российской Федерации от 7 мая 2012 г. №599 «О мерах по реализации государственной политики в области образования и науки» [2], Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденной распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р [3].

В Прогнозе долгосрочного социально-экономического развития Российской Федерации на период до 2030 года [4], разработанном Министерством экономического развития Российской Федерации, предусмотрена необходимость формирования гибкой и диверсифицированной системы профессионального образования, отвечающей требованиям рынка труда и потребностям инновационной экономики, как в части образовательных программ, так и в части условий и материально-технического оснащения процесса обучения.

Созданная к этому моменту перспективная система профессионального образования предполагает наличие типовой устойчивой инновационной модели деятельности вуза, предполагающей эффективное решение стоящих перед ним учебных, методических, научных и воспитательных задач. Степени свободы указанной модели должны допускать варьирование ее параметров в зависимости от содержания образовательных программ, целевой аудитории и условий, в которых реализуются эти программы.

Мировыми образовательными трендами в современном обществе являются: внедрение вариативных образовательных программ на основе индивидуализации образовательных траекторий с учетом личностных свойств, интересов и потребностей обучающегося, внедрение в профессиональную образовательную среду технологий проектного обучения, дистанционных образовательных технологий.

Основоположником одного из современных трендов – дистанционного обучения считается Исаак Питман. В 1840 году для обучения стенографии на расстоянии он впервые использовал почту, при этом задания студентам и результаты их выполнения отправлялись и получались в письмах и посылках. Считается, что именно в этом году им был создан первый дистанционный образовательный курс.

Первый этап массового использования дистанционных образовательных технологий начался в 1850 – е годы. Первым образовательным учреждением, внедрившим элементы дистанционных образовательных технологий, стал Лондонский Университет в Великобритании. В нем впервые была предоставлена возможность студентам из других городов сдать квалификационные экзамены и получить диплом, при условии, что они учились в аккредитованных Лондонским Университетом высших учебных заведениях. Таким образом, студенты получили возможность получить высшее образование, обуча-

ясь на расстоянии. В 1858 году образовательные услуги, предоставляемые указанным Университетом, охватили студентов из других стран. Считалось не принципиальным, какое образовательное заведение они посещали.

Подобный опыт получил распространение на всей территории Великобритании. Стало нормой открывать колледжи, осуществляющие обучение посредством почтовых сообщений, при этом программа обучения совпадала с программами университетов. Всего в течение 19 века новая технология охватила большинство развитых на тот момент государств: Великобританию, Германию, Францию, Соединенные Штаты Америки.

В начале XX века в 1910-1914 годах появились курсы дистанционного обучения в Австралии. Они были организованы Квинслендским университетом, при этом впервые дистанционные технологии были применены для обучения детей, которые проживали в районах, в которых школы отсутствовали. Дальнейшее развитие и внедрение в педагогическую практику рассматриваемых технологий можно условно разделить на ряд этапов.

Характерной чертой первого этапа было использование рукописных и машинописных учебных материалов. Это было связано в первую очередь с тем, что, не смотря на то, что учебники уже издавались достаточно давно, их качество и количество не позволяли организовать полноценное обучение с их использованием.

На втором этапе (50-80-е годы прошлого века) качество полиграфии значительно улучшилось, книги получили цветные иллюстрации. В этот же период широкую популярность приобрели аудио, фото и кино материалы. Так же материалы дополнялись аудио и видеозаписями. Параллельно проводились эксперименты по использованию в образовательных целях кино и телевидения.

Третий этап, начавшийся в конце 1980-х, начале 1990-х годов, характеризовался активным применением сервисов электронной почты, электронных рассылок, электронных конференций. Для подготовки образовательных материалов использовались текстовые редакторы, средства разработки иллюстративных материалов. [5].

В Российской Федерации активное использование технологий дистанционного обучения началось в конце 1990-х, начале 2000-х годов. Отставание в общей сложности на 10 лет было обусловлено технологическим отставанием в области внедрения информационных технологий в образовательный процесс и сложной экономической ситуацией, связанной с изменением политического строя и экономической модели страны.

Старт применению дистанционных образовательных технологий в России был дан в 1995 году постановлением Государственного Комитета Российской Федерации по высшему образованию от 31 мая 1995 г. №6. Этим документом была утверждена «Концепция единой системы дистанционного образования России». В 2002 г. в Закон Российской Федерации от 10 июля 1992 г. № 3266-1 «Об образовании» были внесены соответствующие изменения.

Однако вопрос о законодательном закреплении необходимых положений все еще находился в повестке дня вследствие неоднозначного толкования понятия «дистанционное обучение».

В следующем 2003 г. Федеральным законом от 10 января 2003 г. № 11-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации "Об образовании”» и Федеральным законом «"О высшем и послевузовском профессиональном образовании» было закреплено следующее определение: дистанционные образовательные технологии – это образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Способы организации обучения посредством дистанционных образовательных технологий были зафиксированы в приказе Министерства образования России от

18 декабря 2002 г. № 4452 «Об утверждении Методики применения дистанционных образовательных технологий (дистанционного обучения) в образовательных учреждениях высшего, среднего и дополнительного профессионального образования Российской Федерации».

Развитию дистанционных электронных образовательных технологий способствовал взрывной рост интереса к ним как со стороны государственных структур, заинтересованных в подготовке новых кадров, переподготовке и повышении квалификации сотрудников, так и со стороны бизнеса, заинтересованного в обучении персонала с целью быстрого внедрения в передовых технологий в производство и управление.

На сегодняшний день в мире электронное образование используется повсеместно, при этом, развитие аналогичного рынка в России, по некоторым оценкам [6] отстает на 5–7 лет, что несколько лучше той ситуации, которая имела место в начале 2000-х годов. Неформальная периодизация становления электронного обучения в Российской Федерации может быть представлена на сегодняшний день следующими периодами:

Первый (1990 – 1999) характеризуется развитием электронных образовательных технологий, как элемента заочного обучения. В этот период в качестве средства организации участников образовательного процесса активно используется электронная почта. Учитывая неразвитость системы широкополосного доступа к сети Интернет, для распространения образовательных материалов, содержащих файлы значительного по меркам того времени объема, применяется технология, базирующаяся на протоколе FTP.

Второй (2000 – 2009) – отмечен активизацией рынка корпоративного обучения на основе развития услуг бизнес-образования. Период не случайно совпал с повышением качества и значительным снижением стоимости аренды высокоскоростных каналов доступа в Интернет, развитием мобильных технологий и технологии Веб2.0. Обучающиеся, работодатели и педагогические работники получили возможность равного, интерактивного взаимодействия.

В этот период появились первые электронные системы управления обучением, позволяющие образовательным организациям разрабатывать и поддерживать собственные электронные образовательные ресурсы, что так же существенно снизило их стоимость и способствовало их более широкому внедрению в педагогическую практику.

Третий (с 2010 года) – характеризуется окончанием формирования рынка электронного образования, как самостоятельной области, повсеместным проникновением образовательных технологий во все сферы человеческой деятельности.

В настоящее время поддержка развития дистанционного обучения в Российской Федерации является одним из приоритетных направлений государственной политики. С 2014 года в Российской Федерации реализуется государственная программа «Развитие образования» (2013 – 2020 г.), утвержденная постановлением Правительства РФ от 15 апреля 2014 г. № 295 «Об утверждении государственной программы Российской Федерации "Развитие образования на 2013-2020 годы"».

Заявленная основная цель реализации программы – повышение образовательных результатов обучающихся за счет эффективного встраивания электронных ресурсов в образовательный процесс с целью его качественного изменения. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 7 марта 2018 г.) содержит ст. 16, посвященную общим требованиям к организации образовательного процесса, где определены общие для РФ правовые нормы в области реализации образовательных программ с применением дистанционных образовательных технологий.

Для органов внутренних дел вопрос создания единой электронной информационно-образовательной среды, несомненно, является актуальным, поскольку его решение позволяет создать в образовательных организациях системы МВД России единое обра-

зовательное пространство. Платформой, на базе которой оно в принципе может быть развернуто, может стать интегрированная мультисервисная телекоммуникационная сеть МВД России.

Как отмечается в [7], задача объединения разнородных информационных ресурсов в единую систему безусловно относится к сложным организационно-техническим задачам и требует затрат времени, интеллектуального труда и материальных ресурсов.

Коллекции учебно-методических материалов, базы данных и программное обеспечение поддержки образовательного процесса, накопленные образовательными и научными организациями системы МВД России, для их интеграции в перспективное образовательное пространство требуют реструктуризации и унификации с точки зрения программно-аппаратной совместимости [8].

Стандартизация и унификация информационных ресурсов образовательных организаций системы МВД России является первоочередным и, безусловно, необходимым этапом их интеграции [9].

Решение этой перспективной задачи, безусловно, требует ее периодизации и декомпозиции на отдельные этапы. С учетом существующей структуры образовательных организаций может быть предложен следующий вариант периодизации.

На первом этапе устанавливается стандарт электронной информационно-образовательной среды образовательной организации в рамках единого образовательного пространства МВД России, ранее созданные среды приводятся в соответствие с ним.

На втором этапе разворачиваются стандартизированные электронные информационно-образовательные среды всех образовательных организаций системы МВД России, участвующие в функционировании образовательного пространства.

На третьем этапе проводится опытная эксплуатация каждого компонента, корректируются решения, осуществляются необходимые доработки. Цель данного этапа – обеспечение полной совместимости электронных информационно-образовательных сред в рамках образовательного пространства.

На четвертом этапе происходит выход на опытную эксплуатацию в масштабе региона. На этом этапе координирующими центрами могут стать университеты и академии МВД России.

Пятый этап – подготовка к штатной эксплуатации и внедрение единого образовательного пространства в педагогическую практику.

Ожидаемый эффект от подобной системы – повышение эффективности системы образования МВД России за счет интеграции электронных информационно-образовательных сред в единое образовательное пространство, что позволит реализовать единый подход к подготовке, переподготовке и повышению квалификации сотрудников МВД России.

Литература:

1.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=24068781005355192779604101&cacheid=A45109620EF68A6835778753C180E36E&mode=splus&base=LAW&n=292679&rnd=80AE5B4822069E84F9138DFB2C544637#08746970371470024

2.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=82406878100535519 2779604101&cacheid=3BF954FEEBF336CAA969EFE6A7F5225C&mode=splus&base=LAW&n=129346&rnd=80AE5B4822069E84F9138DFB2C544637#07841344293328985.

3.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=82406878100535519 2779604101&cacheid=6E256F82745C3BDEB2B6BCA3B2FDF257&mode=splus&base=LAW&n=212832&dst=100007&rnd=80AE5B4822069E84F9138DFB2C544637#05525570373241211

4.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=82406878100535519 2779604101&cacheid=6FFC890D22585A761B60AA078D437F74&mode=splus&base=LA

W&n=144190&rnd=80AE5B4822069E84F9138DFB2C544637#035211763511114214

5. Маслакова Е. С. История развития дистанционного обучения в России // Теория и практика образования в современном мире: материалы VIII Международной научной конференции (г. Санкт-Петербург, декабрь 2015 г.).

6. URL:http://www.logrusit.com/ru/glavnaya/articles/razvitie-elearning-v-rossii/.

7. Лемайкина С.В., Арбузов П.В., Карпика А.Г. Электронная информационно-образовательная среда как форма реализации дистанционных технологий образовательных организаций системы МВД России // Сборник материалов двадцать второй всерос. науч.-метод. конф.: в 2-х статьях. Иркутск 2017.

8. Михайленко, Е.В. О создании Автоматизированной системы «Мониторинг» / Е.В. Михайленко // Математические методы и информационно-технические средства: Труды V всерос. науч.-практ. конф., 19 июня 2009 г. / редкол.: Ф.Г. Хисамов, Е.В. Михайленко, И.Н. Старостенко. – Краснодар: Краснодар. ун-т МВД России, 2009. – С. 99 – 101.

9. Михайленко, Е.В. Об автоматизации проведения контрольно-проверочных и итоговых занятий по определению уровня профессиональной подготовленности сотрудников органов внутренних дел к выполнению служебных задач / Е.В. Михайленко // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 3-й междун. науч.-практ. конф. (14 октября 2016 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017. – С. 185 – 193.

Копыткова Л.Б.

Северо-Кавказский федеральный университет

НЕМОДУЛЬНЫЕ ОПЕРАЦИИ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ ДЛЯ ЧИСЕЛ РАЗНЫХ ЗНАКОВ

Система остаточных классов (СОК) первоначально была введена для представления целых неотрицательных чисел, в которой число указанной природы представляется в виде набора остатков от деления этого числа на основания системы счисления. В качестве оснований для однозначности представления выбирают взаимно простые числа. В дальнейшем в работах [1, 4, 6] рассматриваются способы построения модулярной арифметики для чисел другой природы, а именно, для целых чисел, включая отрицательную часть диапазона, для рациональных чисел, целых комплексных и даже для гиперкомплексных чисел.

Для представления отрицательных целых чисел в СОК возможны два подхода. Во-первых, знак числа может быть введён в явном виде и зашифрован как отдельный разряд числа. При этом подходе можно воспользоваться, например, основанием 2. Но в отличие от других оснований, по которым цифры есть остатки от деления на модуль, если значение цифры по основанию 2 рано 1, то будем считать число положительным, а если цифра равна 0, то число отрицательное (или, наоборот). При этом подходе можно визуально определить знак числа. Однако, минус этого подхода заключается в том, что для этого модуля надо по другому организовывать алгоритм работы по сравнению с остальными основаниями. Второй подход введения знака числа является более естественным с точки зрения организации вычислений, так как работа по всем модулям будет вестись по одним алгоритмам, но в этом случае знак получаем в скрытой форме. Поэтому визуально мы не можем определить с каким числом положительным или отрицательным мы имеем дело. Следовательно, даже определение знака числа становится немодульной операцией. В этой работе остановимся именно на этом подходе, что связано с тем, что подобное построение позволяет максимально воспользоваться разрабо-

танными алгоритмами для неотрицательных чисел и имеющуюся архитектуру по построению каждого модуля, а также учесть возможность системы остаточных классов к самокоррекции результата при выходе из строя одного из модулей при наличии достаточного количества контрольных оснований.

При построении модулярной арифметики для чисел разных знаков воспользуемся методом связанным с понятием искусственной формы числа, описанном основоположниками модулярной арифметики Акушским И.Я. и Юдицким Д.И. в [1].

Наиболее простой способ введения знака числа в скрытом виде предполагает наличие чётного основания среди модулей СОК, наилучший вариант, когда одно из оснований, например, $p_1 = 2$. Итак, пусть $p_1,...p_n$ - основания СОК, объём диапазона $\rho = \prod_{i=1}^{n} p_i$. Обозначим $\frac{\rho}{2} = \prod_{i=2}^{n} p_i = P$. Разбиваем этот диапазон на два поддиапазона $[0, P)$ для обозначения отрицательных чисел и $[P, \rho)$ - для неотрицательных чисел, а число P играет роль нуля. Причём в выбранной СОК $P = (1, 0, ...0)$. Будем представлять положительные числа $N = |N|$ в виде $N' = P + |N|$, отрицательные числа $N = -|N|$ в виде $N' = P - |N|$. Такое представление чисел разных знаков и получило название искусственной формы. Превращение положительного числа в отрицательное и обратно, т.е. образование его дополнительного кода, производится вычитанием данного числа из числа $(1, p_2, p_3, ..., p_n)$.

Применяя искусственную форму представления кодов можно проводить операции сложения (вычитания) и умножения над искусственными формами, получая правильный результат, как по величине, так и по знаку, хотя знак скрыт в форме представления числа и визуально его не определить. Эти операции являются модульными и соответственно легко реализуемыми в системе остаточных классов.

Перейдём к рассмотрению немодульных операций для чисел разных знаков. Сразу заметим, что само определение знака числа, а значит, и операция сравнения чисел в СОК принадлежит к немодульным операциям. Это связано с тем, что разряды числа, представленные в СОК, не несут информации о знаке числа, поэтому для определения знака необходимо перейти к определению таких позиционных характеристик, которые позволили бы решить поставленную задачу. Если дано представление $(\alpha_1, \alpha_2, ..., \alpha_n)$, то для того, чтобы установить знак числа, которое оно представляет, достаточно решить задачу о принадлежности этого числа к той или иной половине диапазона $[0, \rho)$. С этой целью проанализируем известные методы определения позиционных характеристик, к которым относятся метод ортогональных базисов, метод интервальных оценок и метод с использованием коэффициентов обобщенной позиционной системы счисления (ОПСС).

Определение знака числа методом ортогональных базисов состоит в переходе к позиционному представлению числа $A = \left| \sum_{i=1}^{n} \alpha_i B_i \right|_\rho$, где $B_i = \frac{m_i \rho}{p_i} = m_i P_i, i = \overline{1, n}$ и $P_i m_i \equiv 1 (\mathrm{mod}\, p_i)$, причём результат надо вводить в требуемый диапазон по модулю всей системы $\rho = p_1 \cdot p_2 ... \cdot p_n$, что разрушает идею модулярной арифметики.

Для определения знака числа удобнее будет применять метод интервальных оценок, к характеристикам которого можно отнести позиционную характеристику номер интервала. Процесс определения знака числа сводится к операции выявления принадлежности интервала, в котором находиться число, представленное в СОК, к группе по-

ложительных или отрицательных интервалов по данному основанию p_i, на которые разбит диапазон ρ. Если нам задано число A в СОК с основаниями $p_1, p_2, ..., p_n$ в виде набора остатков $(\alpha_1, \alpha_2, ..., \alpha_n)$, тогда номер интервала l_A по отношению к дробирующему модулю p_i определяется из соотношения $i = \overline{1,n}$, т.е. $l_A = \left[\frac{A}{p_i}\right]$. В [8, 9, 10] предложена формула для вычисления номера интервала $l_A = \left|\sum_{i=1}^{n} |l_{Ai} \cdot \alpha_i|_{P_i}^{+}\right|_{P_i}^{+}$, где $l_{Aj} = \frac{P_j^{\varphi(p_1)}}{p_i}, j \neq i; l_{Ai} = \frac{P_i^{\varphi(p_i)} - 1}{p_i}$, $P_i = \frac{\rho}{p_i} = p_1 \cdot p_2 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_n$, $\varphi(p_i)$ - функция Эйлера. Число интервалов определяется величиной ρ / p_i.

Например, для СОК с основаниями $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ и объёмом диапазона $\rho = 210$ выберем в качестве нового нуля число $P = \rho / 2 = 105$. Целые числа из интервала $[0;105)$ будем считать изображением отрицательных целых чисел промежутка $[-105;0)$, а целые числа из $[105;210)$ будут означать целые числа интервала $[0;105)$. Для числа $A = (0,1,4,3)$ можно определить номер интервала, выбрав в качестве дробирующего модуля $p_4 = 7$, тогда $P_4 = 30$. Предварительно вычисляя $l_{A_1} = \left|\frac{105}{7}\right|_{30}^{+} = 15$, $l_{A_2} = \left|\frac{70^2}{7}\right|_{30}^{+} = 10$, $l_{A_3} = \left|\frac{42^4}{7}\right|_{30}^{+} = 18$, $l_{A_4} = \left|\frac{30^6 - 1}{7}\right|_{30}^{+} = 17$, получаем $l_A = |15 \cdot 0 + 10 \cdot 1 + 18 \cdot 4 + 17 \cdot 3|_{30}^{+} = 13$. Учитывая, что $l_A = 13 < 15$, мы имеем дело с отрицательным числом. Действительно, $A = 13 \cdot 7 + 3 = 94$ есть при наших допущениях изображение числа $94 - 105 = -11$.

Изложенный подход для определения знака числа предполагает, что $p_1 = 2$. Это удобно с точки зрения простоты выполнения операции, но является некоторым ограничением. Может оказаться, что при решении вопросов, связанных с оптимизацией набора модулей, в состав набора модулей не войдет модуль, равный двум.

В случае, если диапазон разбивается на нечетное число интервалов по выбранному p_i, т.е. все основания нечетные, кроме может быть дробирующего модуля, то имеется критический интервал, который является границей между положительным и отрицательным интервалами. В этом случае критический интервал делится на две части, и процесс определения знака числа при этом сводится к сравнению остатка по модулю p_i. Если число попало в критический интервал $(\rho / p_i - 1)/2$, тогда критический интервал делится на две части и процесс определения знака числа сводится к сравнению остатка α_i с величиной $p_i / 2$, если p_i - чётное, и с $(p_i + 1)/2$, если p_i - нечётное. Определение номера интервала, в котором расположено число, позволяет получить оценку исследуемого числа по величине интервала, что, в свою очередь, позволяет найти эффективные алгоритмы выполнения большинства немодульных процедур. Удобнее пронаблюдать указанный процесс, если среди оснований есть чётное число большее 2. Так как наличие в качестве оснований 2 и выбор его в качестве дробирующего модуля приводит к разбиению на $P = \rho / 2$ интервалов и в критический интервал

попадает всего два числа, одно из которых есть изображение нуля, а другое есть отрицательное число на единицу меньшее, чем число изображающее ноль. Здесь рассмотрим в качестве примера СОК с основаниями $p_1 = 10, p_2 = 3, p_3 = 7$. Эти основания закрывают тот же диапазон, что и в предыдущем примере. Выбирая в качестве дробирующего модуля чётное основание $p_1 = 10$, получаем разбиение диапазона на 21 интервал. В критический интервал $l_A = 10$ попадают числа 100, 101, …, 109, среди которых содержится число 105 являющееся изображением нуля в выбранной системе. Так, например, для числа $103 = (3,1,5)$ имеем $\alpha_1 = 3 < 5$, поэтому это число есть изображение отрицательного числа, а для числа $109 = (9,1,4)$ получаем $\alpha_1 = 9 > 5$, поэтому $(9,1,4)$ есть число положительное в выбранной системе.

Заметим, что иногда при вычислении номера интервалов полезно уменьшить число модулей системы, заменив пару модулей на их произведение. Для числа $(\alpha_1, \alpha_2, ..., \alpha_n)$ можно воспользоваться формулой вычисления цифры $A_{i,j}$ по модулю $p_i \cdot p_j$. Согласно [8] получаем $A_{i,j} = p_i \cdot \left| \left(p_j - p_i\right)^{\varphi(p_j)-1} \right|_{p_j}^{+} \cdot \left(\alpha_i - \alpha_j\right) \Big|_{p_j}^{+} + \alpha_i$. Эта операция бывает полезна, так как в качестве дробирующего модуля в алгоритме нахождения номера интервала рекомендуют выбирать наибольший модуль системы.

В качестве примера для числа $A = (0,1,4,3)$ в СОК $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ перейдём к системе $p_1' = 10, p_2' = 3, p_3' = 7$, т.е. $p_1' = p_1 \cdot p_3$. Получаем $A_{1,3} = 2 \cdot \left| (5-2)^{\varphi(5)-1} \right|_5^{+} \cdot (0-4) \Big|_5^{+} + 0 = 2 \cdot \left| 3^3 \right|_5^{+} \cdot (-4) \Big|_5^{+} = 4$. Действительно, $|94|_{10}^{+} = 4$.

Для случая, когда среди оснований СОК нет чётных, можно воспользоваться построением искусственной формы представления чисел согласно [1, 2, 5]. А далее определять номер интервала согласно указанного замечания о наличии критического интервала, содержащего как положительные, так и отрицательные числа.

Перейдём к рассмотрению метода определения знака числа с использованием коэффициентов обобщенной позиционной системы счисления (ОПСС). Наличие одного и того же набора оснований для СОК и ОПСС позволяет получить алгоритм преобразования модулярного кода в позиционный. Если $p_1, p_2, \ldots, p_n$ – основания ОПСС, тогда число A можно представить в виде $A = a_n p_1 p_2 \ldots p_{n-1} + a_{n-1} p_1 p_2 \ldots p_{n-2} + \ldots + a_3 p_1 p_2 + a_2 p_1 + a_1$, где $0 \le a_i < p_i (i = \overline{1,n})$ – коэффициенты (цифры) ОПСС. Фактически значение старшей цифры ОПСС определяет интервал расположения числа. Однако, если число, изображающее ноль не является границей интервала, то опять возникает критический интервал, содержащий числа разных знаков. Так, например, в СОК с основаниями $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ от числа $90 = 3 \cdot 30 + 0 \cdot 6 + 0 \cdot 2 + 0$ до числа $119 = 3 \cdot 30 + 4 \cdot 6 + 2 \cdot 2 + 1$ все числа имеют старшую цифру $a_4 = 3$, а интервал содержит изображения как положительных, так и отрицательных чисел. Для этой системы гарантированно, что если $a_4 < 3$, то число отрицательное, а если $a_4 > 3$, то число положительное. Можно перестроить этот алгоритм, исключив критический интервал. Если выбрать $p_1 > p_2 > \ldots > p_n$, а $p_n = 2$, тогда старший коэффициент ОПСС α_n может принимать два значения: 0 или 1. И знак числа будет совпадать со значением старшего коэффициента ОПСС α_n, т.к. весь диапазон

делится на два интервала. Как и выше будем считать, что если $\alpha_n = 1$, то число положительное, а если $\alpha_n = 0$, то число отрицательное.

Следует заметить, что наше разделение на положительную и отрицательную части диапазона было весьма условным. С самого начала можно было бы считать числа из $[0, P)$ неотрицательными, а числа из $[P, \rho)$ - отрицательными. При таком отображении диапазонов для получения представления отрицательного числа A в СОК к нему добавляют число, равное ρ, то есть получают число $A + \rho$, которое и попадает в интервал $[P, \rho)$. Рассмотрим возможность организации такой немодульной операции как деление на модуль или произведение модулей СОК для чисел разных знаков, опираясь на последний вариант отображения диапазонов, считая, что один из модулей СОК есть чётное число. В качестве базового возьмём алгоритм деления на модуль (произведение первых степеней модулей) [3, 7], состоящий из двух основных процедур - деления без остатка для модулей взаимно-простых с делителем и расширения системы оснований для остальных модулей. Алгоритм расширения системы оснований удобно взять опирающийся на перевод в ОПСС,

При выполнении операции деления отрицательного числа A на число Y, которое является одним из модулей СОК, или произведением модулей СОК, то есть Y – положительное число, в результате должны получить отрицательное число. Для его нахождения необходимо найти $\left[\frac{A}{Y}\right]$, предварительно выразив A из $A + \rho$. Затем результат представить в виде $\rho + \left[\frac{A}{Y}\right]$. Однако, если с самого начала неизвестен знак числа, то можно получить неверный результат, то есть вместо $\frac{\rho}{Y} + \left[\frac{A}{Y}\right]$ получить $\rho + \left[\frac{A}{Y}\right]$ или наоборот.

Решить поставленную проблему можно определив знак числа A до деления, используя один из приведённых выше способов.

Другой путь основан на следующем факте: деление на A отображает все числа интервала $\left[0; \frac{\rho}{2}\right]$ в интервал $\left[0; \frac{\rho}{2Y} - 1\right]$, а все числа интервала $\left[\frac{\rho}{2}; \rho - 1\right]$ в интервал $\left[\frac{\rho}{2Y}; \frac{\rho - 1}{Y}\right]$. Поэтому число можно разделить сначала на Y. Затем определить в какой интервал попадает число $\left\|\left[\frac{A}{Y}\right]\right\|_\rho$, тем самым находя знак числа A. Если окажется, что A – отрицательное число, тогда необходимо добавить величину $\left|-\frac{\rho}{Y}\right|_\rho$ к $\frac{\rho}{Y} + \left[\frac{\rho}{Y}\right]$ для получения верного результата $\rho + \left[\frac{A}{Y}\right]$. Так как в указанном алгоритме деления присутствовала операция расширения системы оснований, которая позволяет указать цифры числа в ОПСС, то можно использовать результаты этой операции для нахождения интервала расположения числа $\left[\frac{A}{Y}\right]$.

Таким образом, алгоритмы выполнения немодульных операций в СОК для чисел разных знаков можно построить используя известные алгоритмы этих операций для неотрицательных чисел и алгоритмы определения знака числа, заключающиеся в опре-

делении интервала расположения, опирающиеся на одну из позиционных характеристик.

Литература:

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. 440 с.

2. Копыткова Л.Б., Абакумова Н.И. Исследование деления в СОК чисел разных знаков. Поиск моделей социально-экономического развития юга России в новом геополитическом формате / Сборник Материалов международной научно-практической конференции Институт Дружбы народов Кавказа. Ставрополь: РИО ИДНК, 2015. С. 618-623.

3. Копыткова Л.Б. Построение модулярной модели для целых чисел разных знаков Актуальные проблемы современной науки / IV Международная научно-практическая конференция (Алушта, 27-30 апреля 2015 г.) Вып.4. Том II. Алушта, 2015. С. 237-241.

4. Онищенко С.М. Применение гиперкомплексных чисел в теории инерциальной навигации. Автономные системы. – Киев: Наукова думка, 1983. – 208 с.

5. Сабо Н. Определение знака в неизбыточных системах счисления остаточных классов // Кибернетический сборник. М.: Мир, 1964. Вып.8. С. 149-165.

6. Торгашев В.А. Система остаточных классов и надёжность ЦВМ. М.: Советское радио, 1973. 120 с.

7. Червяков Н.И., Копыткова Л.Б. Реализация деления чисел в системе остаточных классов на модули системы Вестник Ставропольского государственного университета. Вып. 34. – Ставрополь: изд-во СГУ, 2003. – С. 7-11.

8. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов (СОК). Учебное пособие. Ставрополь: Издательство Северо-Кавказского федерального университета. 182 с.

9. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Ряднов С.А. Модулярные вычислительные структуры нейропроцессорных систем. М.: Физматлит, 2003, 288 с.

10. Червяков Н.И., Сахнюк П.А., Копыткова Л.Б. и др. Применение нейрокомпьютеров для обработки сигналов (коллективная монография)/ под ред. Гуляева Ю.В. и Галушкина А.И. М.: ИПРЖ “Радиотехника”, 2003, 224 с.

Королев Г.И.
Рязанский филиал
Московского университета МВД России имени В.Я. Кикотя

ГРАФОАНАЛИТИЧЕСКИЙ МЕТОД ИНТЕГРАЛЬНОЙ ОЦЕНКИ УРОВНЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА

В настоящее время при оценке уровня экономической безопасности страны и ее регионов в основном используются индикативные методы [3, 4]. Их преимущества состоят в том, что с их помощью удается оценить уровень экономической безопасности в количественной форме, они более чувствительны к изменениям индикаторов социально- экономических ситуаций и способны дать обобщенную интегральную оценку состояния экономической безопасности и возникающих угроз.

Еще одно существенное преимущество состоит в том, что результаты анализа достаточно легко визуализируются, в частности, с помощью лепестковых диаграмм. Благодаря этому математические модели экономической безопасности становятся более понятными практическим работникам, что способствует их внедрению в практику на всех уровнях административного управления.

Необходимость перехода на новый уровень экономико-математического анализа состояния экономической безопасности как страны в целом, так и ее регионов четко определена Указом Президента РФ от 13 мая 2017 г. № 208 “О Стратегии экономической безопасности Российской Федерации на период до 2030 года” [1]. По сути дела Указ определяет непрерывный мониторинг экономической безопасности как необходимую часть повседневной работы регионов.

Важнейшим положением принятой Стратегии является официальное утверждение 40 показателей экономической безопасности (пункт 27 Указа). Заметим, что в существующих публикациях диапазон анализируемых или рекомендуемых для анализа индикаторов по регионам колеблется от 16 до 150 (например, [4]). Это делает практически невозможным как сравнение интегральных показателей между регионами, так и получение на их основе интегральных показателей по отраслям и по стране в целом. В то же время для целей текущего внутреннего экспресс-анализа Указом не исключается использование лишь части наиболее весомых индикаторов из утвержденных 40. Каким должен быть объем этой выборки? Критерии «весомый», «важный» и пр. носят качественный характер и являются в определенной мере субъективными. Необходим количественный критерий. В случае использования лепестковых диаграмм мы предлагаем метод выбора количества индикаторов по критерию методической погрешности построения самих диаграмм.

Предварительно напомним геометрию некоторой условной лепестковой диаграммы, построенной (для простоты) всего для восьми индикаторов (рис. 1).

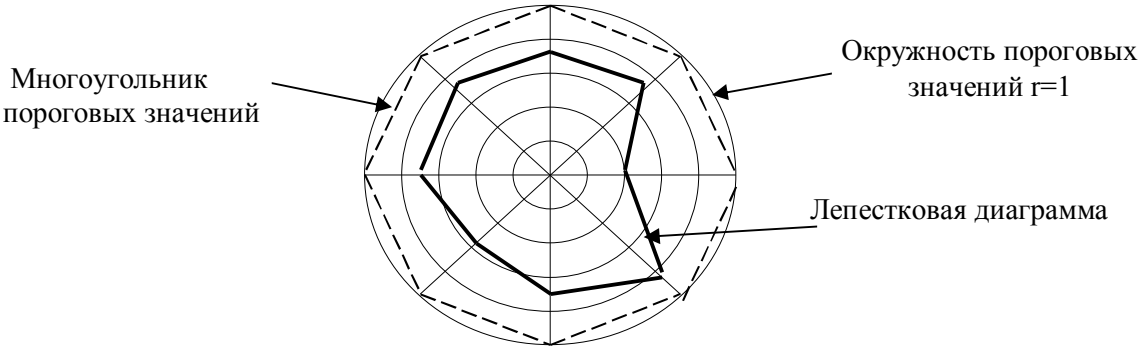


Рис.1. Геометрия условной лепестковой диаграммы.

Внешний контур рис.1. представляет собой окружность нормированных пороговых значений индикаторов. Штриховой линией выделен вписанный в окружность равносторонний многоугольник, который бы соответствовал идеальному случаю равенства всех реальных нормированных индикаторов своим пороговым значениям. Утолщенной линией обозначена собственно лепестковая диаграмма для восьми условных нормированных индикаторов. Концентрические окружности соответствуют количественным характеристикам зон экономической безопасности.

Обратим внимание на то, что многоугольник пороговых значений отсекает от окружности сегменты, площадь которых зависит от количества индикаторов. Чем больше используется индикаторов, тем меньше отсекаемая площадь, тем точнее многоугольником отражается площадь окружности пороговых значений. Этот факт можно использовать для выбора числа индикаторов при заданной методической погрешности анализа.

«Вырежем» из диаграммы один из «*n*» ее секторов (рис. 2).

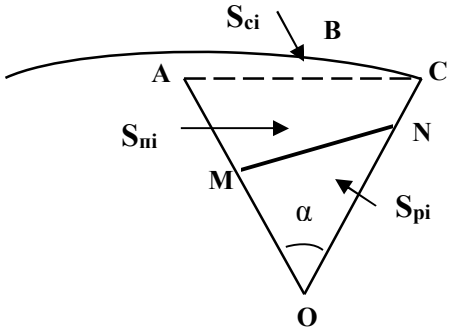


Рис.2. Фрагмент (сектор) лепестковой диаграммы.

На рис.2 обозначены:

S_{ni} – пороговая площадь, образованная двумя соседними пороговыми индикаторами, для которой ОА = ОС = r = 1.

S_{pi} – площадь, образованная реальными рассчитанными индикаторами.

S_{ci} – площадь отсекаемого сегмента диаграммы.

MN – граница площади фрагмента, образованная рассчитанными индикаторами.

α – угол сектора диаграммы.

Обозначим также через $S_{сек.i}$ площадь всего i-го сектора, через $S_к$ – площадь круга пороговых значений с радиусом r = 1, через n - число секторов (равно числу индикаторов).

Тогда:

а) площадь порогового нормированного круга $S_к = \pi \cdot r^2 = \pi;$

б) площадь сектора ОАВСО $S_{сек.} = \frac{\pi}{n};$

в) пороговая площадь треугольника ОАС $S_n = \frac{1}{2} r \cdot r \cdot Sin\alpha = \frac{Sin\alpha}{2};$

г) площадь сегмента $S_c = S_{сек.} - S_n = \frac{\pi}{n} - \frac{Sin\alpha}{2};$

д) угол сектора $\alpha = \frac{360^0}{n}.$

Относительная методическая погрешность, вызванная конечным числом индикаторов:

$$\Delta = \frac{\frac{\pi}{n} - \frac{Sin\alpha}{2}}{\frac{\pi}{n}} = 1 - n\frac{Sin\alpha}{2\pi}$$

Рассчитаем величины методических погрешностей, задавая конечные значения числа индикаторов, поместив результаты расчетов в таблицу 1.

Таблица 1

К выбору необходимого числа индикаторов экономической безопасности

Параметры	Значения						
n	8	10	12	15	18	…	40
α^0	45	36	30	24	20	…	9
$Sin\alpha$	0,707	0,588	0,50	0,407	0,342	…	0,156

Параметры	Значения						
$n\frac{Sin\alpha}{2\pi}$	0,900	0,936	0,955	0,972	0,98	…	0,993
Δ, %	10,0	6,4	4,5	2,85	2,0	…	0,7

Поскольку в практических расчетах по экономической статистике погрешность не более пяти процентов считается вполне допустимой, для текущей пилотной оценки уровня экономической безопасности, согласно данным таблицы 1, достаточно выбрать 12 показателей - индикаторов. Увеличение их числа будет способствовать снижению погрешности. На наш взгляд, при промежуточном анализе практического уровня экономической безопасности среднего по масштабам региона двенадцати основных показателей будет вполне достаточно.

Второй важнейшей задачей является получение интегрального показателя экономической безопасности на основе рассчитанных локальных индикаторов. Как известно, под интегральным показателем понимается некоторая обобщенная, сводная количественная характеристика объекта или процесса, объединяющая в единое целое (от лат. integer – целый) систему частных индикаторов. В настоящее время в большинстве случаев интегральные показатели рассчитываются как средние или средние взвешенные.

При применении лепестковой диаграммы нами предлагается объединять рассчитанные локальные индикаторы через вычисление площади, ограниченной на диаграмме многоугольником их значений. В этом случае интегральный индикатор экономической безопасности ($I_{эк.без.}$) может быть определен путем сопоставления двух площадей лепестковой диаграммы: площади, ограниченной пороговыми индикаторами ($S_п$), и площади, ограниченной реальными расчетными индикаторами ($S_р$):

$$I_{эк.без.} = \frac{S_p}{S_n}$$

При этом погрешность определения интегрального показателя будет соответствовать методической погрешности выбора количества индикаторов.

Для демонстрации практического применения предлагаемого метода проведем оценку уровня экономической безопасности региона за 2010 – 2014 гг на примере Рязанской области, выбрав для простоты всего 8 показателей.

1. Уровень безработицы (по методологии МОТ),%.
2. Число зарегистрированных преступлений на 100 000 чел. населения.
3. Доля населения с доходами ниже величины прожиточного минимума,%.
4. Инвестиции в основной капитал на душу населения,% к ВРП.
5. Отношение средней пенсии к средней заработной плате,%.
6. Отношение СДДД к прожиточному минимуму, раз.
7. Объем ВРП на душу населения, % от среднего по РФ.
8. Степень износа основных фондов, %.

Исходные статистические данные взяты нами из официальной статистики, а временной интервал – относительно «спокойные» годы до начала действий западных санкций, поскольку оценка уровня экономической безопасности в санкционные годы может носить особый характер.

В качестве нормирующих выбраны функции, предложенные Е.С. Митяковым [3], где x – реальное значение индикатора, а – его пороговое значение:

а) для соотношения реального значения индикатора и его порогового значения типа «не менее»

$$v=\begin{cases} 2^{(1-\frac{x}{a})/\ln\frac{10}{3}}, \text{если } \dfrac{x}{a}>1; \\ 2^{-\log_{\frac{10}{3}}\frac{a}{x}}, \text{ если } \dfrac{x}{a}\le 1, \end{cases}$$

б) для соотношения реального значения индикатора и его порогового значения типа «не более»

$$y=\begin{cases} 2^{(1-\frac{x}{a})/\ln\frac{10}{3}}, \text{если } \dfrac{x}{a}<1; \\ 2^{-\log_{\frac{10}{3}}\frac{a}{x}}, \text{ если } \dfrac{x}{a}\ge 1, \end{cases}$$

Напомним, что значения нормированных индексов формируют такие зоны лепестковой диаграммы: при $y < 0,25$ – зона «катастрофического риска», при $0,25 < y < 0,5$ –зона «критического риска», при $0,5 < y < 0,75$ – зона «значительного риска», при $0,75 < y < 1$ – зона умеренного риска, при $y > 1$ – зона «стабильности. Результаты нормирования приведены в таблице 2.

Таблица 2.

Нормированные индикаторы по РО (2010-2014 гг.)

Номер показателя	Год				
	2010	2011	2012	2013	2014
1	0,652	0,713	0,923	0,911	0,947
2	1,279	1,312	1,318	1,310	1,311
3	0,645	0,621	0,716	0,744	0,775
4	0,879	0,926	0,956	0,973	0,807
5	1,089	1,087	1,070	1,047	1,033
6	0,835	0,809	0,891	0,914	0,934
7	0,736	0,735	0,769	0,779	0,773
8	0,886	0,875	0,861	0,869	0,852

Таблица 3

Сравнительная таблица значений нормированных интегральных индикаторов

Год	2010	2011	2012	2013	2014
Как средние из локальных	0,875	0,885	0,938	0,943	0,929
По соотношению площадей	0,742	0,759	0,871	0,881	0,859

Для сравнения методик проведем расчет интегральных показателей дважды:

а) как средних величин из равновесовых локальных индикаторов;

б) по предлагаемой нами методике по соотношению площадей реальной и пороговой лепестковых диаграмм.

Результаты расчетов приведены в таблице 3 и представлены графически на рис. 3.

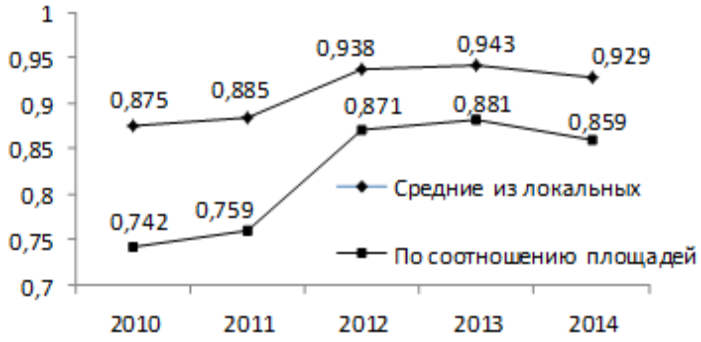


Рис. 3. Графическое сравнение интегральных индикаторов.

Нетрудно видеть, что графики индикаторов изменяются практически синхронно, но график индикаторов, рассчитанных как средние, проходит значительно выше. Есть основания предположить, что существующая методика завышает реальные индикаторы экономической безопасности из-за их «однокоординатного» расчета (отрезки), в то время как предлагаемая методика использует «двухкоординатный» расчет (площади).

В целях обнаружения тенденций в изменении динамики графиков целесообразно проводить их аналитическое сглаживание в соответствии с методикой эконометрического моделирования [2]. Сглаживание значений индикаторов проведем методом простой скользящей средней (таблица 4), а результаты моделирования представим графически (рис.4).

Отметим несколько принципиальных моментов, вытекающих из модели динамики интегральных индикаторов экономической безопасности, рассчитанных по предлагаемой нами методике.

1. Р В 2010 году область находилась в зоне «значительного риска». В дальнейшем экономика области перешла в зону «умеренного риска» и оставалась в этой зане все последующие (по 2014 г) годы.

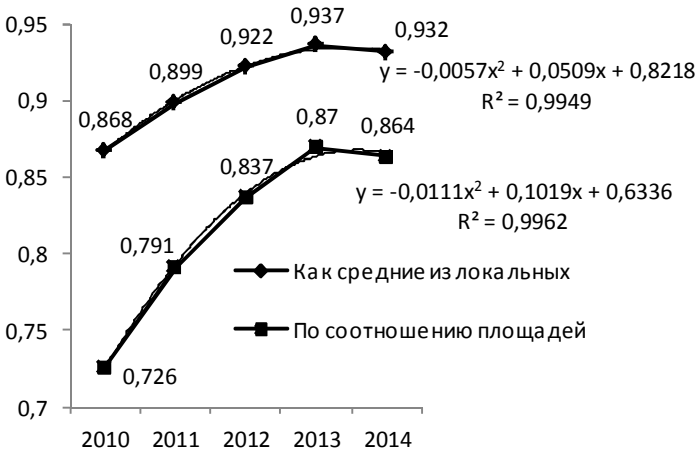


Рис. 4. Эконометрические модели интегральных индикаторов.

Таблица 4

Сглаженные значения нормированных индикаторов

Год	2010	2011	2012	2013	2014
Как средние из локальных	0,868	0,899	0,922	0.937	0,932
По соотношению площадей	0,726	0,791	0,837	0,870	0,864

2. Заметно последовательное уменьшение темпа роста интегрального индикатора, т.е. проявляет себя экономический закон убывающей эффективности. Это характерно

для случаев, когда слабо используются достижения научно-технического прогресса в производственной и технологической областях,

3. К 2014 году в уровне экономической безопасности наметился отрицательный тренд. Логично предположить, что это связано с введением против России западных санкций. Пока уровень их влияния в последующие годы оценить сложно из-за постоянного ужесточения санкционной политики Запада. Тем не менее, по нашему мнению, развитие аналитики экономической безопасности позволит не только выявить степень этих угроз, но и найти методы их блокирования.

Литература:

1. Указ Президента РФ от 13 мая 2017 г. № 208 “О Стратегии экономической безопасности Российской Федерации на период до 2030 года”. Режим доступа kremlin.ru > acts/bank/41921.

2. Королев Г.И. Эконометрика: Основы эконометрического моделирования: Учебное пособие для вузов. – Рязань: Рязанский филиал Московского университета МВД России, 2011.-304 с.

3. Митяков Е.С. Разработка математических методов анализа и прогнозирования поведения индикаторов экономической безопасности: Автореферат диссертации на соискание ученой степени кандидата экономических наук. - Нижний Новгород, 2012.

4. Сенчагов В.К., Иванов Е.А. Структура механизма современного мониторинга экономической безопасности России: доклад д.э.н. Сенчагова В.К., к.э.н. Иванова Е.А. на заседании секционного Ученого совета научного направления «Экономическая политика» ИЭ РАН. - М., 2015. – 46 с.

Кочетов Д.А., Лукащик Е.П.
Кубанский государственный университет

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Одной из основных тенденций последних лет в сфере компьютерных преступлений является рост количества и сложности атак на ресурсы автоматизированной системы.

Сетевая атака – действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, пользующихся этой удалённой/локальной вычислительной системой. По причине того, что проведение удаленной атаки достаточно трудно выявить, а провести ее относительно просто (из-за избыточной функциональности современных систем) этот вид неправомерных действий выходит на первое место по степени опасности.

По характеру воздействия атаки бывают пассивные и активные. К первым относятся те, что не оказывают прямое влияние на работу вычислительной системы, но способны нарушить ее политику безопасности. Именно из-за отсутствия прямого влияния на систему, такую атаку обнаружить сложно. Активное воздействие на работу вычислительной системы – это такое, которое оказывает непосредственное влияние на работу системы, нарушает ее работоспособность, изменяет конфигурацию и т.д. При активном типе атаки в системе возникают некоторые изменения, в то время как при пассивном воздействии не остается видимых следов.

При любой атаке главная цель, как правило – это получение несанкционированного доступа к информации. Получение информации бывает двух видов: перехват и искажение. При перехвате получают информацию без возможности ее изменения. Искажение или подмен данных ведет к нарушению их целостности. Таким образом, по цели воздействия сетевые атаки можно разделить на те, которые нарушают функцио-

нирование системы, и те, которые нарушают целостность информационных ресурсов или же их конфиденциальность.

Для защиты системы от сетевых атак нужно устанавливать специальные программы, которые контролируют всё, что уходит и приходит по сети, защищают систему от взломов и атак из сети, а также предотвращают передачу личной информации.

Защитные механизмы

Обнаружение атак – это процесс распознавания и реагирования на подозрительную деятельность, направленную на сетевые или вычислительные ресурсы. Эффективность технологии во многом зависит от того, какие методы анализа полученной информации применяют. В настоящее время в системах безопасности наряду со стандартными статичными механизмами, такими как *разграничение доступа*, *системы аутентификации,* используется ряд новых защитных методик, использующих некоторую форму анализа контролируемого пространства на основе правил или статистического подхода. В качестве контролируемого пространства могут выступать журналы регистрации или сетевой трафик. Анализ опирается на набор заранее определённых правил, которые создаются администратором или самой системой обнаружения атак.

Статистический анализ имеет два основных преимущества: использование зарекомендовавшего себя аппарата математической статистики и адаптация к поведению субъекта. В самом начале использования данного метода определяются профили для каждого субъекта анализируемой системы. Любое отклонение используемого профиля от эталона рассматривается как несанкционированная деятельность. Статистические методы универсальны, так как не требуют знаний о возможных атаках и уязвимостях системы. Однако при их использовании могут возникать некоторые трудности, связанные, например, с тем, что их можно «обучить» воспринимать несанкционированные действия как нормальные. Поэтому наряду со статистическим анализом применяются дополнительные методики.

Весьма распространенным методом обнаружения атак являются *экспертные системы*. При их использовании информация об атаках формулируется в виде правил, которые, зачастую, записывают в виде последовательности действий или в форме сигнатуры. Если выполняется любое из этих правил, то тут же принимается решение о наличии несанкционированной деятельности. Одно из главных достоинств этого метода – практически полное отсутствие ложных тревог. Для того чтобы экспертные системы всегда оставались актуальными, необходимо постоянно обновлять применяемые базы данных. Недостаток такого метода заключается в невозможности отражения неизвестных атак. Даже если атаку из базы данных немного изменят, а также любое разделение атаки во времени или среди нескольких злоумышленников, то это уже может стать серьезным препятствием для ее обнаружения. Из-за большого разнообразия атак и хакеров даже специальные постоянные обновления базы данных правил экспертной системы никогда не дадут гарантии точной идентификации всего диапазона атак.

Использование *нейронных сете*й является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, которые могут дать пользователю определённый ответ о соответствии рассматриваемых характеристик заложенным в базу данных правилам, нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. Искусственные нейронные сети (ИНС) – программная или аппаратная реализация математических моделей, которые построены по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма [1]. Понятие возникло при изучении процессов, протекающих в мозге, и при попытках смоделировать эти процессы. Единицей измерения является искусственный нейрон.

ИНС представляют собой систему соединённых и взаимодействующих между собой простых процессоров (искусственных нейронов). Каждый процессор подобной сети имеет дело только с сигналами, которые он периодически получает, и сигналами, которые он периодически посылает другим процессорам. И будучи соединёнными в достаточно большую сеть с управляемым взаимодействием, такие по отдельности простые процессоры вместе способны выполнять довольно сложные задачи.

✓ С точки зрения машинного обучения нейронная сеть представляет собой частный случай методов распознавания образов, дискриминантного анализа, методов кластеризации и т. п.

✓ С математической точки зрения обучение нейронных сетей – это многопараметрическая задача нелинейной оптимизации.

✓ С точки зрения кибернетики нейронная сеть используется в задачах адаптивного управления и как алгоритмы для робототехники.

✓ С точки зрения развития вычислительной техники и программирования нейронная сеть – это способ решения проблемы эффективного параллелизма.

✓ А с точки зрения искусственного интеллекта ИНС является основой философского течения коннективизма и основным направлением в структурном подходе по изучению возможности построения (моделирования) естественного интеллекта с помощью компьютерных алгоритмов.

Нейронные сети не программируются в привычном смысле этого слова, они обучаются. Обучение – это процесс, в котором свободные параметры нейронной сети настраиваются посредством моделирования среды, в которую эта сеть встроена. Возможность обучения – одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что в случае успешного обучения сеть сможет вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных и/или «зашумленных», частично искажённых данных. Способность нейронных сетей «изучать» характеристики умышленных атак и идентифицировать элементы, которые не похожи на те, что наблюдались в сети прежде, является их важным преимуществом при обнаружении злоупотреблений. Искусственные нейронные сети после обучения способны адаптироваться под новые типы угроз, распознавая их, даже если ранее до этого с ними не сталкивались. Данная особенность позволяет системе защиты стать более гибкой и независимой.

Виды сетевых атак

Среди известных угроз безопасности сетевой информационной системе можно условно выделить три группы [2]:

а) *Сканирование портов* – данные угрозы сами по себе атакой не являются, но, как правило, ей предшествуют, так как это один из способов получить информацию об удаленном компьютере. Суть данного способа заключается в сканировании UDP/TCP-портов, которые используются сетевыми сервисами на нужном компьютере для выявления их состояния. Такой процесс помогает понять, какие атаки на данную систему могут быть удачными, а какие нет. Более того, сканирование дает злоумышленнику необходимые сведения об операционной системе, что позволяет подобрать еще более подходящие типы атак.

б) *DoS-атаки* – они еще известны, как «отказ в обслуживании». Это такие атаки, в результате действия которых атакуемая система приходит в нестабильное или же полностью нерабочее состояние. Их последствия могут включать в себя повреждение или разрушение информационных ресурсов и невозможность их использования. DoS-атаки бывают двух типов:

✓ компьютеру-жертве отправляются специально сформированные пакеты, которые приводят к перезагрузке системы или ее остановке;

✓ компьютеру-жертве отправляется большое количество пакетов в единицу времени, он не справляется с их обработкой. Следствие – исчерпание ресурсов системы.

DoS, без всякого сомнения, является наиболее известной формой атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Этот тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения сети, не остановить у провайдера, то на входе в сеть это сделать уже невозможно, потому что вся полоса пропускания будет занята. Когда атака этого типа проводится одновременно через множество устройств возникает распределенная атака DoS (DDoS - distributed DoS).

Снижение угрозы атак типа DoS может быть достигнуто тремя способами:

- Функцией анти-спуфинга – применением меры по борьбе с вторжениями, основанными на подделке исходящего IP-адреса. Правильная конфигурация функций анти-спуфинга на маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827.
- Функцией анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.
- Ограничением объема трафика (traffic rate limiting). Организация может попросить провайдера ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по сети.

Одним из наиболее эффективных и перспективных методов обнаружения DDoS-атак является механизм работы нейронных сетей, широко применяющийся в современных средствах защиты.

в) *Атаки-вторжения*. Их цель – «захват» системы. Такой тип атак самый опасный, так как при успешном их выполнении злоумышленник получает максимально полную информацию о системе. Атаки-вторжения применяются в тех случаях, когда есть необходимость в получении конфиденциальных данных с удаленного компьютера, такие как пароли или доступ к кредитным картам. Также целью таких атак может быть закрепление в системе для того, чтобы впоследствии в целях злоумышленника использовать ее вычислительные ресурсы. К данной группе относится самое большое количество атак. Более распространенные виды атак, которые используют сетевые сервисы операционной системы:

- Атаки на переполнение буфера. Этот тип уязвимостей в программном обеспечении, который возникает из-за отсутствия или недостаточной меры контроля при работе с массивами данных.

• Атаки, основанные на ошибках форматных строк. Такой тип возникает из-за недостаточной степени контроля значений входных параметров функций форматного ввода-вывода. В том случае, если такая уязвимость находится в программном обеспечении, то злоумышленник может получить абсолютный контроль над системой.

Структура системы защиты

Для обнаружения сетевых атак был разработан программный комплекс, который захватывает поток данных из сети, классифицирует данные и, в случаи обнаружения атаки, сообщает об этом пользователю (администратору). Данная система защиты состоит из трех компонентов:

• Модуль сбора информации о пакетах в сети;

• Модуль классификации;

• Модуль оповещения.

Для тестирования проблем обнаружения сетевых вторжений в данной системе обнаружения сетевых атак применялся набор данных KDD Cup 1999 [3], представляющий собой совокупность смоделированных необработанных данных дампа TCP. Данный набор содержит около 5 миллионов классифицированных по 22 типам экземпляров атак (классов) записей, каждая запись состоит из 41 параметра, характеризующего сетевое подключение и метку о том, является подключение вредоносным или нет.

Типы атак сгруппированы в четыре категории:

• Denial of Service Attack (DoS) – отказ в доступе легальному пользователю;

• User to Root Attack (U2R) – злоумышленник, получив доступ к системе в качестве рядового пользователя, пытается эксплуатировать уязвимость системы и стать суперпользователем;

• Remote to Local Attack (R2L) – злоумышленник пытается получить удаленный доступ к системе с неавторизированной машины;

• Probe – сбор информации о вычислительной сети с целью обхода её системы управления безопасностью.

Для выполнения классификации реальных сетевых данных был разработан модуль сбора информации. При разработке данного модуля использовался монитор сетевой безопасности Bro [4], представляющий собой платформу для сетевого мониторинга. Написание сценариев обработки исключительных ситуаций производилось на языке программирования Python.

Вначале монитор Bro выполняет сбор и журналирование сетевого трафика. Каждая запись в журнале характеризует одно сетевое соединение. Монитор Bro кроме стандартных параметров дампа сетевого соединения выполняет вычисление продолжительности соединения, размера переданных и принятых пакетов, определяет флаг соединения. По завершении соединения с источником информации Bro выполняет запись вычисленных параметров в журнал.

На языке Python был реализован класс, реализующий возможность чтения постоянно обновляющегося журнала, фиксирующего активность сети. При появлении новой записи о подключении вызывается функция, выполняющая дальнейшую обработку данных, аргументом которой является список параметров сетевого трафика. Для определения параметров сетевого трафика, которые извлекаются из содержимого сетевых пакетов, были определены фильтры на основе знаний эксперта.

По порту назначения для протоколов TCP, UDP определяется сервис, с которым выполняется соединение. Для протокола ICMP порт источника является типом ICMP сообщения, а порт назначения – кодом ICMP сообщения.

Для определения данных параметров было реализовано два класса, в которых накапливалась статистика по подключениям за указанное число соединений. Первый класс использовался для получения статистики для одинаковых хостов, второй класс –

для получения статистики для одинаковых сервисов. Данные классы являются значениями словаря, ключи которого определяются парой IP адресов источника и назначения или именем сервиса подключения.

При логировании нового соединения монитором Bro выполняется определение окна, равного 100 подключениям или 2 секундам. Подключения, не попадающие в данный промежуток, удаляются, а новое соединение добавляется, при этом происходит обновление статистических данных активного окна соединений, а затем расчет значений атрибутов трафика. Далее полный набор параметров трафика передается в модуль классификации для анализа и определения метки - является ли подключение сетевой атакой или нет.

Таблица 1

Точность и полнота определения сетевых атак

ГРУППА	КЛАСС	ПОЛНОТА	ТОЧНОСТЬ
PROBE	SATAN	0,9895	0,9795
U2R	ROOTKIT	0,1429	0,1667
PROBE	PORTSWEEP	0,9842	0,9987
DOS	BACK	0,6633	0,7224
U2R	BUFFER_OVERFLOW	0,7500	0,0325
R2L	FTP_WRITE	0,25	0,9852
R2L	GUESS_PASSWD	0,9623	0,1683
R2L	IMAP	0,8333	0,3030
PROBE	IPSWEEP	0,9704	0,9920
DOS	LAND	0,9566	0,9245
U2R	LOADMODULE	0,5	0,9536
R2L	MULTIHOP	0,5714	0,7265
DOS	NEPTUNE	0,9996	0,991
PROBE	NMAP	0,9253	0,6871
NORMAL	NORMAL	0,9966	0,9969
U2R	PERL	0,5	0,6666
R2L	PHF	0,3333	0,0240
DOS	POD	0,7843	0,2492
DOS	SMURF	0,9992	0,9925
R2L	SPY	0,5	0,444
DOS	TEARDROP	0,9975	0,6552
R2L	WAREZCLIENT	0,9612	0,8226
R2L	WAREZMASTER	0,95	0,8913

Для анализа трафика была применена гибридная нейронная сеть, состоящая из самоорганизующейся сети Кохонена и многослойного персептрона [5]. При применении сети Кохонена происходит кластеризация входных данных в узлы матрицы, в которых будут сгруппированы события аналогичных числовых символов. Фактически, отдельные узлы представляют собой определённые сценарии атак. Входной вектор данной сети содержит 35 компонентов, соответствующих параметрам записи в базе данных KDD99, на выходе матрица содержит 22 узла, которые соответствуют типам атак.

После этого набор параметров трафика и информация о номере узла из сети Кохонена подается на вход многослойного персептрона, обученного распознавать аномальный трафик, но уже с учетов информации о событии, то есть принадлежности пакетов той или иной группе. Это позволяет не только обнаружить сетевые вторжения в единичных пакетах, но и выявить принадлежность пакета к распределённой по времени

атаке. Результаты данного анализа представлены в таблице 1. В данной таблице приведены показатели точности и полноты определения класса атаки. Всего в обучающем наборе данных содержится 22 типа экземпляра атак, сгруппированных в 4 категории.

После выполнения анализа сетевых данных, полученных из модуля сбора информации, при обнаружении сетевой атаки выполняется отправка e-mail сообщения в модуле оповещения. В данном сообщении указываются IP адрес и порт источника соединения, IP адрес и порт назначения, название сервиса подключения и тип сетевой атаки.

В целях тестирования программного комплекса для обнаружения сетевых атак был развернут виртуальный сервер у хостинг-провайдера Flops. Для генерации различного рода сетевого трафика на сервере также были использованы различные сервисы, такие как почтовые и веб. В ходе эксперимента было выполнено 150 подключений, из них 100 – были распознаны как нормальные, остальные – были отнесены к тому или иному типу атаки.

Результаты проведенного анализа и эксперимента показывают, что представленная интеллектуальная система обнаружения сетевых атак на основе нейросетевых технологий способна с высокой точностью и в кратчайшие сроки выявлять сетевые угрозы, что позволит эффективно применять ее в информационных системах сетевой безопасности.

Литература:

1. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. – М.: Горячая линия - Телеком, 2002

2. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). - Уфа: Лето, 2011. – С. 8-13.

3. KDD Cup 1999 Data, http: //kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Дата обращения: 05.05.2017.

4. The Bro Network Security Monitor, https://www.bro.org/. Дата обращения: 29.05.2018.

5. Тарасов Я.В. Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. 2014. №8. URL: https://cyberleninka.ru/article/n/metod-obnaruzheniya-nizkointensivnyh-ddos-atak-na-osnove-gibridnoy-neyronnoy-seti (дата обращения: 13.05.2018).

Крыгин С.В., Кульпанов А.И.
Нижегородская академия МВД России

ИСПОЛЬЗОВАНИЕ МЕТОДОВ DATA MINING В АНАЛИЗЕ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Data Mining или «добыча данных», есть не что иное, как алгоритм исследования больших объемов информации, целью которого является выявление взаимосвязей и тех или иных закономерностей между переменными, с последующим применением полученной информации к новым массивам данных [1]. Data Mining понимается как «совокупность статистики, методов искусственного интеллекта и анализа баз данных», и до последнего времени этот метод не признавался полноценной областью интереса для специалистов в области статистики, а порой его даже величали «задворками статистики»[1]. Тем не менее, вследствие своей не малой практической значимости, указанная выше проблематика в настоящее время интенсивно прорабатывается и имеет большой интерес, в том числе и в её статистических аспектах.

Методы Data Mining заслуженно обретают популярность и интерес со стороны специалистов в роли механизма для проведения анализа «сырых» данных, когда есть предположение, что в дальнейшем из них можно извлечь полезную информацию для принятия конкретных решений в условиях неопределенности. Применительно к целям исследования этот аналитический метод используется здесь для выявления структуры и содержания типовых сценариев в расследовании преступлений в области компьютерной информации [2].

В основе систем «добычи данных» лежат принципы разведочного анализа информации и построения моделей и в них используются аналогичные подходы и методы [3]. Но стоит отметить существенное отличие процедуры Data Mining от разведочного анализа данных: системы добычи данных ориентированы не на установление природы явлений, а в большей степени на практическое применение собранных результатов. Большое значение придается поиску решений, опираясь на эти решения, появлялась бы возможность построения достоверных прогнозов, правил, версий [4].

Из этого следует, что в сфере добычи данных имеет место такой подход к анализу информации и извлечению знаний, который иной раз характеризуют как «черный ящик». При этом применяются не только методы разведочного анализа информации, но и другие методы, именуемые как нейронные сети, позволяющие построение достоверных прогнозов без уточнения зависимостей на которые это прогноз опирается.

Data Mining состоит из трех основных этапов: проведение исследования, построение модели и её проверку. При идеальных начальных условиях, то есть при достаточном количестве информации, есть возможность организации итеративной процедуры для построения устойчивой (робастной) модели. Наряду с этим в реальной ситуации на стадии анализа проверить математическую модель практически невозможно и поэтому начальные результаты носят характер эвристик, которые можно применять при принятии решения (например, «Если преступление совершено путем компьютерного взлома, то его мог совершить только программист»).

В противовес классической проверки гипотез, основным назначением которой является проверка априорных подозрений, касающихся связей между переменными (например: «Имеется положительная корреляция между возрастом человека и его нежеланием рисковать»), анализ исходной информации методами добычи данных осуществляется для нахождения связей между переменными в тех ситуациях, когда недостаточны или отсутствуют совсем априорные представления о природе этих связей.

Как правило, при этом виде анализ происходит учет и сравнение достаточно большого количества переменных, а для нахождения закономерностей применяются различные методы. При анализе преступной деятельности было использовано два метода Data Mining: «деревья классификации» и нейронные сети [5].

Сначала опишем методику перехода от эмпирических данных к представляющей их абстрактной системе. В основном объекты могут обладать чуть ли не бесконечным количеством свойств, каждое из которых представляется возможным изучить в отдельности, а следствием этого является то, что произвольный объект невозможно изучить полностью. Это определяет необходимость отбора ограниченного (и вероятнее всего довольно малого) количества характеристик, наиболее полно описывающих выбранный объект как явление [6]. Концептуальное и методологическое обоснование выбора характеристик метода совершения преступлений в области компьютерной информации как объекта мы уже осуществили.

На рассматриваемом объекте система будет задана тогда, когда набору определенных нами свойств будет назначена определенная переменная. Термин переменная, о котором идет речь выше используется с целью абстрактного образа свойства. С каждым свойством связано множество его появлений (проявлений).

Итак, каждая конкретная переменная имеет определенное имя (метку), отличающее её от других рассматриваемых переменных, и связывается с определенным множеством величин, через которые она себя проявляет. Эти величины будем называть состояниями (значениями) переменной, а все множество – множество состояний.

Три значительных методологических отличия имеет данная представляющая система от других систем: а) все переменные определены на качественном множестве состояний; б) экземпляр данных относительно базы представляет собой отдельное преступление и, в) вектор (профиль) номинальных состояний многомерный.

Статистики качественных переменных разработаны достаточно хорошо. Однако вместе с тем они не применимы именно к многомерными данным, и вычисляют только характеристики табулированных (группированных) данных. В терминах постановки нашей задачи при группировке данных концептуальная и методологическая сущность базы разрушается. При этом связать в единую систему боле 2-х переменных (за исключением группировки) нельзя. А для построения версий, нам необходимо одновременное проявление всех переменных следовой картины преступления. Именно этот факт и послужил методологическим основанием выбора методов моделирования: деревьев классификации и нейронных сетей.

Один из наиболее важных методов, используемых при «добыче данных» – это разработка деревьев классификации. В данном методе представляется возможным предсказать принадлежность наблюдений и объектов к определенному классу категориальной зависимой переменной в зависимости от значений одной или нескольких предикторных (от английского predict – предсказывать) независимых переменных.

Предсказание значений категориальной зависимой переменной является основной целью создания деревьев классификации и в связи с этим используемые средства тесно связаны с классическими методами дискриминантного и кластерного анализа, и нелинейного оценивания непараметрической статистики. Возможность широкого применения деревьев классификации представляет этот метод достаточно привлекательным инструментом анализа информации.

Деревья классификации хорошо подходят для графического представления, отсюда следует, что сделанные на их основе заключения легче интерпретировать, чем, если бы заключения были представлены только в числовой форме.

Есть еще одна характерная черта метода классификации деревьев – присущая этому методу гибкость. Последовательное объяснение эффекта влияния отдельных переменных, вот статистическая сущность деревьев классификации. Существуют еще причины доказывающие гибкость деревьев классификации по сравнению с традиционными методами анализа. Возможность деревьев классификации проводить одномерное ветвление для анализа вклада отдельных переменных дает возможность работать с предикторными переменными различных типов: категориальными (номинальными), порядковыми (ранговыми), интервальными, непрерывными [7].

Тем временем измерение предикторных переменных как минимум в интервальной шкале, является обязательным условием при классическом линейном дискриминантном анализе [8]. В случае же деревьев классификации с одномерным ветвлением по переменным, измеренным в порядковой шкале, любое монотонное преобразование предикторной переменной (т. е. любое преобразование, сохраняющее порядок в значениях переменной) создаст ветвление на те же самые предсказываемые классы объектов (наблюдений). Поэтому построение деревьев классификации, основываясь на одномерном ветвлении допустимо независимо от того, соответствует ли единичное изменение непрерывного предиктора единичному изменению лежащей в его основе величины или нет, достаточно, чтобы предикторы были измерены в порядковой шкале. Другими сло-

вами, накладываются более лояльные ограничения на способ измерения предикторной переменной.

Для целей классификации нами строились деревья по алгоритму одномерного ветвления по методу «Classification And Regression Trees» – CART [9]. CART – это программа, производящая перебор всех возможных вариантов одномерного ветвления, при построении дерева.

У этого метода есть один незначительный недостаток. Проявляется он в случае наличия предикторных переменных с большим количеством уровней и тогда поиск с применением CART может оказаться весьма продолжительным. Помимо этого метод склонен выбирать для ветвления предикторные переменные с большим числом уровней. Тем не менее, так как имеет место быть полный перебор вариантов, есть вероятность нахождения варианта ветвления, дающего наилучшую классификацию.

Обладая уникальными возможностями для обработки больших многомерных массивов качественных данных, деревья классификации обладают одним существенным недостатком. Они не могут выделять классы по отношению к многомерной зависимой переменной (отклика). Деревья классификации не могут, схватывая следовую картину обстоятельств в целом, по одним и тем же следам и выдать версию о субъекте сразу по трем признакам: профессии, отношению к чему-либо и степени организованности. При этом на практике имеющаяся следовая картина может быть неполна (или противоречива), и поэтому не подходить в целом ни к одной из типовых версий.

Литература:

1. Pregibon D. Data Mining. Statistical Computing and Graphics, 7, 8. – 1997.

2. Астафьев Е.Р. Математические методы социально-криминологических исследований: курс лекций / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарский университет МВД России, 2006. –78 с.

3. Михайленко Е.В. Методы оптимизации: сборник задач / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2015. – 140 с.

4. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Классификация и снижение размеренности. – М.: «Финансы и статистика», 1989.

5. Крыгин С.В., Чикина Т.Е. Нейросетевой подход при математическом моделировании преступной деятельности // Математические методы и информационно-технические средства : материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И. Н. Старостенко и др. – Краснодар: Краснодарский университет МВД России, 2017. – С. 140–143.

6. Клир Дж. Системология. Автоматизация решения системных задач: Пер. с англ. – М.: Радио и связь, 1990. – С. 234 .

7. Миркин Б.Г. Анализ качественных признаков и структур. – М., 1989.

8. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Классификация и снижение размеренности. – М.: «Финансы и статистика», 1989.

9. Breiman, L., Friedman, J. H., Olshen, R. A., & Stone, C. J. Classification and regression trees. Monterey, CA: Wadsworth & Brooks/Cole Advanced Books & Software, 1984.

Лейцина А.В., Хромых А.А.
Краснодарский университет МВД России

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ПИТАНИЯ В ВЕДОМСТВЕННЫХ ВУЗАХ

Каждый из нас время от времени оказывается в ситуации, когда достижение некоторого результата может быть достигнуто не единственным способом. В подобных случаях приходится выбирать наилучший способ из всех возможных. Однако, в зави-

симости от ситуации, наилучшими могут быть совершенно разные решения. На практике оказывается, что в большинстве случаев понятие «наилучший» может быть выражено количественными критериями – минимум затрат, минимум времени, максимум прибыли и т.д. В связи с этим возможна постановка математических задач нахождения оптимального (optimum – наилучший) результата, так как принципиальных различий в нахождении наименьшего или наибольшего значения нет. Задачи на нахождение оптимального решения называются задачами оптимизации. Чтобы решить практическую задачу надо перевести ее на математический язык, то есть составить ее математическую модель.

Методов решения задач оптимизации достаточно много. При постановке и решении задач оптимизации возникают два вопроса: что и как оптимизировать?

В первую очередь необходимо изучить проблему, которую предстоит решить. Затем необходимо выявить тот параметр, который определяет степень совершенства решения возникшей проблемы. Этот параметр обычно называют целевой функцией или критерием качества. Далее устанавливается совокупность величин, которые определяют целевую функцию. Формулируются все ограничения, которые должны учитываться при решении задачи. После этого строится математическая модель, заключающаяся в установлении аналитической зависимости целевой функции от всех аргументов и аналитической формулировки сопутствующих задаче ограничений. Далее приступают к поиску решения.

Постановка задачи. Пусть в результате формализации прикладной задачи установлена целевая функция $f: X \to R$, $X \subset R^n$, где множество X – обобщение ограничений (множество допустимых решений). Необходимо найти оптимальное решение $x^0 = \left(x_1^0; x_2^0; \ldots; x_n^0\right)$ на множестве X, при котором целевая функция f достигает наименьшего или наибольшего значения.

Т.е. необходимо максимизировать (минимизировать) линейную функцию

$$f(X) = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n,$$

где $X = \left(x_1; x_2; \ldots; x_n\right)$

при ограничениях

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \le b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \le b_2, \\ \ldots\ldots\ldots\ \ldots\ldots\ldots\ \ldots\ldots\ldots\ \ldots\ldots\ldots\ \ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \le b_m, \end{cases}$$

причем

$$x_j \ge 0,\ j = 1, 2, \ldots, n.$$

В теории оптимизации существует несколько способов решения такого вида задач. Первым является графический метод. Он применяется в том случае, когда задача содержит две неизвестные переменные. Однако на практике, когда приходится сталкиваться с неограниченным количеством переменных, его использование не представляется возможным.

В случае с неограниченным числом переменных применяется способ связанный с построением специальных таблиц, известный как симплексный метод решения задач линейного программирования (ЗЛП). Данный метод заключается в целенаправленном переборе опорных решений. Он позволяет за конечное число шагов либо найти оптимальное решение, либо установить, что оптимальное решение отсутствует.

Рассмотрим актуальную для нашей жизни задачу – организация питания в ведомственных ВУЗах МВД России. Как известно, такие высшие учебные заведения являют-

ся казенными и питание осуществляется организовано в соответствии с нормативно-правовыми актами. К основному относится Постановление Правительства РФ от 29 декабря 2007 г. № 946 «О продовольственном обеспечении военнослужащих и некоторых других категорий лиц, а также об обеспечении кормами (продуктами) штатных животных воинских частей и организаций в мирное время», в соответствии с которым курсанты и слушатели, не имеющие званий офицеров и специальных званий среднего и старшего начальствующего состава, профессиональных образовательных организаций и образовательных организаций высшего образования, подведомственных федеральным органам государственной власти должны обеспечиваться продовольствием в соответствии Нормой №1 (общевойсковым пайком) (рис. 1).

Продукты	Количество на 1 чел. в сутки, г
Хлеб из смеси ржаной обдирной и пшеничной муки первого сорта	350
Хлеб белый из пшеничной муки первого сорта	400
Мука пшеничная второго сорта	10
Крупа разная	120
Макаронные изделия	40
Мясо	200
Рыба	120
Жиры животные, топленые, маргарин	20
Масло растительное	20
Масло коровье	30
Молоко коровье	100
Яйца куриные, штуки в неделю	4
Сахар	70
Соль пищевая	20
Чай	1,2
Лавровый лист	0,2
Перец	0,3
Горчичный порошок	0,3
Уксус	2
Томатная паста	6
Картофель и овощи (всего)	900
В том числе:	
Картофель	600
Капуста	130
Свекла	30
Морковь	50
Лук	50
Огурцы, помидоры, коренья, зелень	40
Соки плодовые и ягодные	50
Напитки фруктовые	65
Концентрат киселя на плодовых и ягодных экстрактах	30
Фрукты сушеные	20

Рис. 1. Общевойсковой пайок

Однако, при детальном рассмотрении данной нормы становится понятно, что ряд продуктов остаются неопределенными и могут варьироваться в пределах видов. К таким категориям относятся крупы, рыба и мясо. В этом случае появляется необходимость выбора наиболее подходящих продуктов для достижения минимизации издержек и обеспечения сбалансированного рациона питания.

В данной работе произведены расчеты исходя из суточной потребности мужчины 20 лет среднего роста и комплекции, а также из характеристик продуктов, закрепленных в общевойсковом пайке.

В первую очередь, таблицу продуктов необходимо дополнить данными о содержащихся в них питательных веществах и средних ценах из расчета на 100 грамм и на порцию.

В условиях организации питания в образовательных учреждениях рационально использовать закупочные цены, однако рассмотрим минимальные розничные.

Нас интересует тот перечень продуктов, который не поддается строгой регламентации.

Составим достаточно простую ЗЛП, где x_i – продукт, количество которого нас интересует, а n – количество порций соответствующего продукта в заданный период времени (для удобства будем использовать неделю).

Полученная ЗЛП решается симплексным методом, однако, с учетом большого количества переменных, перебор базисных переменных становится весьма трудоемким.

Рассмотрим решение построенной задачи с помощью табличного процессора *MS Excel*, который позволяет избавиться от всех промежуточных этапов перебора и перейти сразу от задания условий ЗЛП к нахождению оптимального решения. Для этого достаточно воспользоваться встроенным пакетом «Поиск решения».

«Поиск решения» – это надстройка для *MS Excel*. С ее помощью можно определить максимальное или минимальное значение одной ячейки, изменяя другие ячейки.

Шаг 1.

Необходимо создать форму для ввода условий задачи и заполнить ее исходными данными (рис. 2).

Задача оптимального выбора

	Крупы, бобовые								Мясо				Рыба									
	Гречневая каша	Кукурузная каша	Манная каша	Овсяная каша	Перловая каша	Пшенная каша	Рисовая каша	Ячневая каша	Баранина	Говядина	Свинина нежирная	Куры	Килька	Минтай	Мойва	Сайра	Сельдь					
Количество продукта (порция	0	2	0	0	0	5	0	0	0	0	1	6	0	0	0	0	7				Целевая функция	
Стоимость	4,296	3,378	3,5856	3,816	5,52	2,508	4,968	2,916	112,25	67,25	37,25	24,0625	5,516	10,43	5,88	19,222	4,004				228,949	min
Ограничения:																						Итого:
белки	5,4	7,8	3	3,84	3,84	3,6	1,8	1,68	40,5	46,75	40,75	51	10,01	10,99	9,17	12,81	12,11	≥	400,0	=		465,12
жиры	1,92	3,48	0,36	2,16	0,6	0,96	0,24	0,36	38,25	31,5	69,75	21,5	6,44	0,42	8,19	14,35	13,93	≥	300	=		308,02
углеводы	32,88	100,56	19,68	18,48	27,24	20,64	20,76	22,44	0	0	0	2	0	0	0	0	0	≥	200	=		316,32
калории	164,4	446,4	92,4	111,6	122,4	110,4	94,8	100,8	502,5	477,5	795	402,5	99,4	46,9	111,3	179,9	173,6	≥	5500	=		5870
сумма порций круп	7	необходимое кол-во порций круп				7																
сумма порций мяса	7	необходимое кол-во порций мяса				7																
сумма порций рыбы	7	необзодимое кол-во порций рыбы				7																

Рис. 2. Исходные данные ЗЛП

Шаг 2.

Заполняется диалоговое окно надстройки «Поиск решения» табличного процессора *MS Excel* (рис. 3).

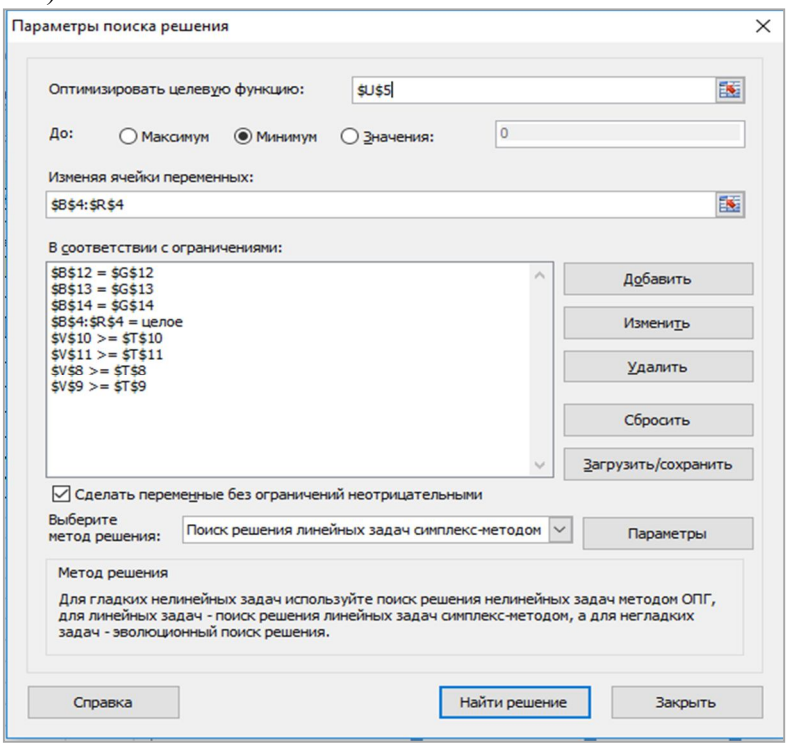


Рис. 3. Активация надстройки «Поиск решений»

В результате получено оптимальное количество порций, при который затраты минимизируются: $Z = 228{,}949$.

В данной работе представлены расчеты на количества порций каждого продукта в неделю. В результате установления ограничений по питательным веществам и по количеству порций, получились данные, которые удобно графически представить с помощью гистограммы (рис.4).

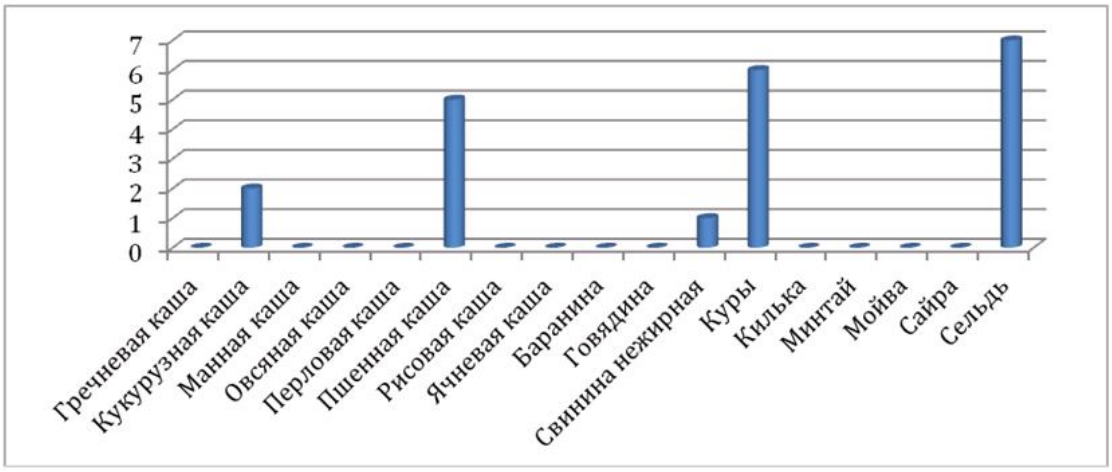


Рис. 4. Наименование и количество продуктов рациона питания

Как уже говорилось ранее, общевойсковой паек состоит из фиксированной и нефиксированной частей.

Стоимость фиксированной части на человека в день и в неделю составляет 170 и 1190 рублей соответственно.

Минимальная стоимость нефиксированной части составляет около 230 рублей в неделю.

Итого: 1190+230=1420 рублей в неделю на каждого курсанта.

Такой набор продуктов позволяет максимизировать получение организмом питательных веществ при минимальных затратах.

Литература:

1. Михайленко Е.В., Методы оптимизации: сборник задач / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2015.

2. Михайленко Е.В., Прикладная математика: курс лекций / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2014.

3. Постановление Правительства РФ от 29 декабря 2007 г. № 946 «О продовольственном обеспечении военнослужащих и некоторых других категорий лиц, а также об обеспечении кормами (продуктами) штатных животных воинских частей и организаций в мирное время» // http://www.consultant.ru

4. Бойченко А.А. Симплексный метод решения задач линейного программирования / А.А. Бойченко, Н.Н. Гусев, Е.В. Михайленко // Математические методы и информационно-технические средства: материалы X Всерос. науч.-практ. конф. 20–21 июня 2014 г. / редкол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, Ю.Н. Сопильняк, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2014. – С. 43 – 45.

Лемайкина С.В., Петрищева Е.Н.
Ростовский юридический институт МВД России

ОСОБЕННОСТИ И НЕКОТОРЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА «РОЗЫСК-МАГИСТРАЛЬ» В БОРЬБЕ С ЭКСТРЕМИЗМОМ, ТЕРРОРИЗМОМ И ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ

Современный этап мирового развития характеризуется тем, что информация, средства информатизации и связи, а также общественные отношения, складывающиеся в процессе сбора, обработки, хранения, передачи и распространения информации оказывают непосредственное и все более возрастающее влияние на экономическое, социальное и духовное развитие как отдельных государств, так и мирового сообщества в целом. Это показывает то, что в современных условиях информация и управление ею становится основанием и главным инструментом достижения целей в новом мироустройстве.

Мировая информационно-технологическая революция создала принципиально новые потенциальные угрозы жизнедеятельности государств и их граждан и мирового сообщества в целом. Это касается терроризма, экстремизма и организованной преступности, мутация которых, и происходят именно в информационной сфере.

Многие элементы общественных отношений не могут функционировать без обратной отдачи информации, необходим его постоянный оборот. На сегодняшний день использование научно-технических средств в деятельности органов внутренних дел значительно активизировалось. Так можно заметить рост технической оснащенности, совершенствование техники, используемой в деятельности сотрудника ОВД. Деятельность органов внутренних дел напрямую связана с информацией, ведь оттого, насколько она полна, точна, достоверна и будет зависеть эффективность раскрытия преступлений.

Совершенствование информационного обеспечения органов внутренних дел на основе оснащения их современными программно-техническими комплексами и системами, а также внедрения в практическую деятельность новых и перспективных информационных технологий является одним из приоритетных направлений повышения эффективности правоохранительной деятельности.

Опыт борьбы с преступностью свидетельствует, что для успешного проведения оперативно-розыскных мероприятий в ОВД в отношении преступлений, связанных с экстремизмом, терроризмом и организованной преступностью необходима эффективная информационная поддержка. Основным инструментом такой поддержки процесса раскрытия и расследования преступлений являются информационные системы, созданные и ведущиеся в органах внутренних дел.

Важным событием в этой сфере стала разработка и внедрение автоматизированной информационно-поисковой системы оперативно-розыскного назначения программно-технический комплекс (ПТК) «Розыск-Магистраль».

Программно-технический комплекс «Розыск-Магистраль» – это комплекс МВД России по выявлению лиц, находящихся в розыске. В режиме реального времени система выявляет пассажиров, находящихся в розыске, с транслитерацией фамилии, введенной в запросе: после получения списка бронирования, в процессе регистрации, а также в архиве отправок. Программно-технический комплекс и информационные базы, содержащихся в них данных, помогают сотрудникам полиции ежегодно разыскивать и задерживать тысячи злоумышленников, скрывающихся от правосудия, в считанные часы раскрывать преступления "по горячим следам", отслеживать перемещение лиц с возможной окраской «терроризм», «экстремизм». Одна из особенностей данной систе-

мы, сопровождением "Розыск-Магистраль" занимаются сотрудники подразделений оперативно-розыскной информации ОВД на транспорте.

Целью создания программно-технического комплекса «Розыск-Магистраль» являлся сбор, накопление и обработка информации о пассажиропотоке с использованием современных информационно-коммуникационных технологий в интересах обеспечения деятельности подразделений органов внутренних дел (в первую очередь органов внутренних дел на транспорте) в сфере обеспечения правопорядка на объектах транспорта России.

Контроль за перемещением людей железнодорожным и воздушным транспортом ведется круглосуточно, а с 2013 года еще и за автомобильным, морским и внутренним водным транспортом. [4] Сейчас возможности ПТК позволяют не только выявить любого человека в пассажиропотоке, но и проследить всю его "криминальную биографию". При использовании контроля пассажиропотока особое внимание уделяется перемещению лиц, подозреваемых в пособничестве терроризму, экстремизму и организованной преступности путем сравнения информации о продаже и бронировании билетов, предоставляемой предприятиями транспорта с розыскными и оперативными учетами.

В системе "Розыск-Магистраль" также реализовано использование программных модулей – автоматизированных рабочих мест (АРМ), позволяющих выявлять и раскрывать различные преступления. В основу работы аналитических модулей заложен принцип отраслевой интеграции информации. Существует свой отдельный модуль, способный посредством специально разработанных алгоритмов извлекать из общего банка информации, накопленного в ПТК «Розыск-Магистраль» анализировать данные, необходимые для выявления и раскрытия конкретных видов преступлений, в том числе и таких видов преступлений как терроризм, экстремизм и организованная преступность [1].

Вместе с этим при использовании ПТК «Розыск-Магистраль» следует учитывать ряд имеющихся проблем, влияющих на ее эффективность. Лица, в том числе и подозреваемые в данных преступлениях, приспосабливаются к техническим разработкам противодействия преступности. Ими применяются методы сокрытия своих персональных данных при перемещении по стране: использование документов посторонних лиц и поддельных документов, приобретение билетов за 5-10 минут до отправления транспортного средства или просто передвижение на перекладных, минуя основные транспортные маршруты, которые не учитываются системой. Изучая эту тенденцию, разработчики ПТК «Розыск-Магистраль» включили в состав комплекса подсистему биометрической идентификации лиц человека «АТИГ». Подсистема позволяет в режиме реального времени выявлять во входящем или выходящем пассажиропотоке лиц, находящихся в розыске или представляющих оперативный интерес [2].

На эффективность работы системы «Розыск-Магистраль» отрицательно также сказывается следующие факторы:

Разнообразие документов, по которым могут приобретаться проездные документы на все виды транспорта и смена паспортов при достижении гражданином определенного возраста, утрата (порча) документа.

Эффективность поиска лиц, находящихся в розыске и представляющих оперативный интерес, в пассажиропотоке была бы значительно выше, на наш взгляд, если бы на территории России действовала система персональной идентификации гражданина. Данная система построена не на фамилии, имени, отчестве и дате рождения человека, а на уникальном числовом коде, который присваивался бы ему один раз и обеспечивал однозначную идентификацию гражданина независимо от предъявляемого им документа, например, так как это осуществляется в ряде государств СНГ (Казахстан, Кыргызстан). Другим, возможным вариантом является использование для идентификации личности биометрических данных, как в загранпаспортах нового образца, но при этом воз-

никает проблема перевода биометрических данных в числовую форму, пригодную для автоматизированного поиска.

В отличие от системы министерства путей сообщения (МПС) РФ, система учета продажи билетов водным, воздушным, автомобильным транспортами не является единой. Множество существующих перевозчиков хранят информацию в разных расчетно-кассовых центрах и используют различные информационные системы. Предоставление данных перевозчиками информации осуществляется в электронной форме в автоматическом режиме по расписанию путем отбора требуемых данных из информационной системы субъекта транспортной инфраструктуры или перевозчика и их выгрузки в обменный файл (сообщение) согласованного формата. [4]

В результате из-за различия информационных систем, не всегда персональные данные о пассажирах корректно поступают в автоматизированные централизованные базы Минтранса и соответственно в ПТК «Розыск-Магистраль», то есть при формировании списка пассажиров в отдельные поля не попадает нужная информация.

Не смотря все выше сказанное, можно отметить, что на сегодняшний день ПТК «Розыск-Магистраль» - является одной из самых эффективных автоматизированных информационных систем, разработанных и используемых в органах внутренних дел России. Дальнейшее развитие ПТК «Розыск-Магистраль» нацелено на развитие аналитических возможностей, оперативное предупреждение преступлений и обеспечение безопасности пассажирских перевозок, а также на совершенствование имеющихся баз данных и повышение их потенциала.

Литература:

1. Бочкарев А.В., Морозова Е.В., Сластенов В.В. Система «Розыск-Магистраль» в оперативно-розыскной деятельности органов внутренних дел на транспорте // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов XVI Международной научной конференции, 22-23 мая 2007 г. - М.: Академия управления МВД России, 2007. С. 196-198

2. Коровкин Д. Современные технологии на службе правопорядка // Правопорядок на транспорте, 2012, № 1. С. 18-21.

3. Федеральный закон от 9 февраля 2007 г. (ред. от 06.07.2016) «О транспортной безопасности» № 16-ФЗ (с изм. и доп., вступ. в силу с 21.12.2016) // СПС «КонсультантПлюс».

4. Приказ Министерства транспорта Российской Федерации от 19 июля 2012 г. № 243 «Об утверждении Порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных» // СПС «КонсультантПлюс».

Литвинов В.А.

Барнаульский юридический институт МВД России

О НЕКОТОРЫХ СВОЙСТВАХ АЛГОРИТМОВ МОДЕЛИРОВАНИЯ МЕТОДОМ МОНТЕ-КАРЛО МНОГОЧАСТИЧНЫХ РАСПРЕДЕЛЕНИЙ

В данной работе рассматриваются некоторые свойства многочастичных распределений, моделируемых методом Монте-Карло на основе одночастичных инклюзивных распределений. Классическим примером такой задачи многие годы являлось моделирование глубоко неупругих ядерных взаимодействий при сверхвысоких энергиях. В настоящее время квантовая хромодинамика сделала большой шаг в области описания динамики взаимодействия элементарных частиц при сверхвысоких энергиях, но, как отмечается в работе [1, с.18], «квантовая хромодинамика в состоянии описывать только жесткие процессы и совершенно неприменима при рассмотрении низкоэнергетиче-

ской части спектра». С развитием ЭВМ все большое число исследователей предлагают для описания адронных взаимодействий при сверхвысоких энергиях использовать гибридные математические алгоритмы, которые дают неплохое описание наблюдаемых процессов.

Одной из важнейших характеристик всех видов взаимодействий в природе являются законы сохранения. Для указанных выше ядерных взаимодействий – сохранение энергии и импульса, в экономике – сохранение материальных (финансовых) ресурсов, и т.д. Поэтому особенностью алгоритмов Монте-Карло, используемых для математического моделирования таких процессов, является учет этих законов сохранения.

Учет законов сохранения приводит к наличию во многочастичных функциях распределения дельта функции Дирака:

$$P_n(x_1, x_2, \cdots, x_n) = F_n(x_1, x_2, \cdots, x_n)\delta(\sum x_i - E), \quad (1)$$

где E — некоторая константа, например, суммарный исходный ресурс (энергия).

Проблема заключается в том, что отсутствуют как теоретические модели для многочастичных распределений $F_n(x_1, x_2, \cdots, x_n)$, так и эмпирическое описание экспериментальных наблюдений. Применительно к указанным выше ядерным взаимодействиям хорошо изученными являются одночастичные инклюзивные распределения:

$$f(x_1) = \int dx_2 \cdots \int dx_n \, P_n(x_1, x_2, \cdots, x_n), \quad (2)$$

а также распределения по множественности (количеству частиц, рождающихся в одном взаимодействии). Именно эта информация используется для построения различных математических алгоритмов моделирования методом Монте-Карло.

Рассмотрим свойства одночастичных распределений (2) и получаемых на их основе многочастичных распределений при различных алгоритмах моделирования, учитывающих ограничения, накладываемые законами сохранения. Из наличия во многочастичном распределении (1) дельта функции и определения одночастичного инклюзивного распределения (2) следует соотношение:

$$\int_0^E xf(x)dx = E. \quad (3)$$

Предположим, что в некотором моделируемом случайном событии в среднем рождается N объектов, которые в дальнейшем будем называть частицами. В этом случае должно выполняться соотношение:

$$\int_0^E f(x)dx = N. \quad (4)$$

Не нарушая общности рассуждений, константу E в выражениях (1), (3) и (4) можно положить равной единице. Из общих соотношений (3) и (4) следует свойство асимптотического поведения одночастичного распределения при малых значениях x. Предположим, что $f(x) = Cx^{\alpha-1}$. Тогда из (3) следует, что $C = \alpha + 1$, а $N = (\alpha + 1)/\alpha$. При $N \gg 1$ следует $\alpha \sim 1/N \ll 1$. Если ограничить область возможных минимальных значений параметром ε, что находит естественное объяснение в физических и экономических процессах, то допустимыми будут значения $\alpha \leq 0$. Во всех этих случаях мы имеем дело с распределениями, быстро возрастающими при $x \to 0$. Экспериментальные и теоретические исследования ядерных взаимодействий при сверхвысоких энергиях показывают, что при малых значениях x инклюзивные одночастичные функции $f(x) \sim 1/x$, а $N \sim -\ln \varepsilon$ [2].

В отсутствие многочастичного распределения $P_n(x_1, x_2, \cdots, x_n)$ для моделирования множественного рождения возникает желание воспользоваться известным одночастичным распределением (2). В ряде ранних алгоритмов множественного рождения предлагалось делать выборку случайных значений $\xi_1, \cdots, \xi_n$ из нормированного распределения (2) пока сумма смоделированных значений не превысит 1. Значение последней случайной величины переопределяется с учетом закона сохранения, так чтобы сумма всех значений оказалась равной единице. Назовем этот алгоритм первым.

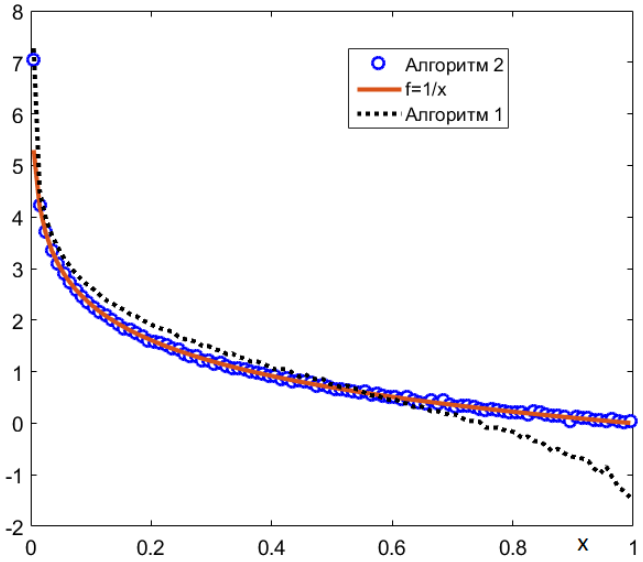


Рис. 1. Сравнение результатов моделирования распределений по двум алгоритмам

Казалось бы для событий с большой средней множественностью изменение значения всего оной случайной величины в ансамбле не должно повлиять на общий вид распределения. Но простое моделирование показывает несостоятельность такого утверждения. Соответствующий результат можно увидеть на рис. 1. Описанный алгоритм приводит к существенному занижению модельного распределения в области $x>0.5$. Это связано с тем, что чаще всего приходится нормировать (переопределять) значения случайной величины, которое должно быть более 0,5. Для устранения данного эффекта применялись различные модификации алгоритма, например, в работе [3] предложено первоначально разыгрывать значение случайной величины из интервала [exp(–1), 1], а в дальнейшем использовать описанный выше алгоритм для области [ε, exp(–1)]. Такой алгоритм позволяет получить несмещенную оценку одночастичного распределения при $x>\exp(-1)$, но «провал» смещается левее.

В данной работе предлагается алгоритм несмещенного моделирования множественного рождения частиц с инклюзивным распределением $f(x)=1/x$. Для того, чтобы получить наборы случайных величин с фиксированным суммарным значением, распределенных по указанному выше закону, пригоден простейший алгоритм. Каждое новое случайное значение необходимо выбирать из равномерного распределения шириной, равной недостающей сумме значений. То есть первая случайная величина ξ_1 выбирается из равномерного распределения на отрезке [0,1]. Вторая случайная величина выбирается равномерно из отрезка $[0{,}1-\xi_1]$ и так далее, пока недостающая сумма не окажется менее заданного ε. Назовем этот алгоритм вторым.

Докажем, что данный алгоритм позволяет получать наборы случайных величин, распределенных по закону $1/x$. Выполнение закона сохранения при таком моделировании очевидно.

Для доказательства сформулированного утверждения рассмотрим распределения частиц по поколениям. Как следует из алгоритма, частицы первого поколения будут иметь равномерное распределение на отрезке [0,1]. Распределение частиц второго поколения будет определяться интегралом:

$$\varphi_2(x)=\int_0^{1-x}\frac{dx_1}{1-x_1}=-\ln x. \qquad (5)$$

Распределение частиц $n+1$ поколения будет определяться n-кратным интегралом:

$$\varphi_{n+1}(x) = \int_0^{1-x} dx_1 \int_0^{1-x-x_1} dx_2 \cdots \int_0^{1-x-x_1-\cdots-x_n} dx_n \prod_{k=1}^{n} \frac{1}{1-\sum_{j=1}^{k} x_j} = \int_0^{1-x} F_n(x_1, x)dx_1.$$

Докажем методом индукции, что

$$F_n(x_1, x) = \frac{1}{(1-x_1)(n-1)!}\ln^{n-1}\left(\frac{1-x_1}{x}\right). \quad (6)$$

Для n = 1справедливость выражения (6) вытекает из (5). Предположим, что оно верно для n–1, тогда

$$F_n(x_1, x) = \int_0^{1-x-x_1} \frac{dx_2}{(1-x_1)(1-x_1-x_2)(n-2)!}\ln^{n-2}\left(\frac{1-x_1-x_2}{x}\right) =$$

$$= -\int_0^{1-x-x_1} \frac{1}{(1-x_1)(n-2)!}\ln^{n-2}\left(\frac{1-x_1-x_2}{x}\right) d\ln\left(\frac{1-x_1-x_2}{x}\right) =$$

$$= \frac{1}{(1-x_1)(n-1)!}\ln^{n-1}\left(\frac{1-x_1}{x}\right).$$

Используя выражение (6), получим распределение для частиц n-го поколения.

$$\varphi_n(x) = \int_0^{1-x} \frac{1}{(1-x_1)(n-2)!}\ln^{n-2}\left(\frac{1-x_1}{x}\right) dx_1 = \frac{1}{(n-1)!}\ln^{n-1}\left(\frac{1}{x}\right).$$

Итоговое одночастичное распределение получается суммированием выше приведенного выражения для $\varphi_n(x)$ по n от 1 до ∞. Нетрудно убедиться, что

$$f(x) = \sum_{n=1}^{\infty} \frac{1}{(n-1)!}\ln^{n-1}\left(\frac{1}{x}\right) = \frac{1}{x}.$$

На рис. 1 приведены результаты моделирования по данному алгоритму в сравнении с одночастичным распределением.

Другой важной характеристикой множественных процессов является распределение по множественности и дисперсия числа рождающихся в одном событии частиц. Можно показать, что рассматриваемый алгоритм приводит к пуассоновскому распределению по числу частиц.

Вероятность того, что число частиц со значением $x > \varepsilon$ будет равно единице, определяется событиями, когда для первой частицы $x > 1 - \varepsilon$. Учитывая, что распределение по x для первой частицы равномерное на отрезке от 0 до 1, получим $p_1 = \varepsilon$. События завершающиеся рождением всего двух частиц определяются вероятностями событий $x_1 > \varepsilon$, $x_2 > \varepsilon$, $x_1 + x_2 > 1-\varepsilon$.

С учетом полученных ранее выражений для спектров частиц первого и второго поколений получим вероятность событий с двумя частицами.

$$P_2 = \int_{\varepsilon}^{1-\varepsilon} dx \int_{1-\varepsilon-x}^{1-x} \frac{dy}{1-x} = \int_{\varepsilon}^{1-\varepsilon} \frac{\varepsilon dx}{1-x} = \varepsilon \ln\frac{1-\varepsilon}{\varepsilon} \approx -\varepsilon\ln\varepsilon\ .$$

Можно показать, что, пренебрегая величинами порядка ε по сравнению с единицей, распределение по числу частиц в одном событии определяется вероятностями:

$$\mathrm{P}_n = \frac{\mu^{n-1}}{(n-1)!}\exp(-\mu), \quad \mu = -\ln\varepsilon.$$

Численное моделирование подтверждает справедливость приведенной выше формулы. Соответственно дисперсия числа случайных величин одного ансамбля будет убывать пропорциональна их среднему числу. Данное свойство распределения по числу частиц

не является универсальным кинематическим эффектом, хотя и присуще ряду алгоритмов моделирования. В работе [4] было показано, дисперсия числа случайных величин в ансамбле, ограниченном законом сохранения, может определяться асимптотическим поведением одночастичного распределения, используемого для моделирования случайных величин. Но это не единственный фактор, способный повлиять на дисперсию числа частиц. Рассмотрим несколько модернизированный предложенный выше алгоритм.

Предположим, что значение первой случайной величины распределено не равномерно, а по некоторому закону $\rho(1-x)$. Дальнейшее моделирование будет производиться по описанному выше алгоритму. В этом случае среднее число частиц и второй момент в одном ансамбле будут определяться выражениями:

$$\bar{n} = \int_0^1 \left(1 + \ln\frac{x}{\varepsilon}\right)\rho(x)dx = 1 + \int_0^1 \mu(x)\rho(x)dx,$$

$$\overline{n^2} = \int_0^1 \sum_{k=1}^{\infty}(k+1)^2 P_k(x)\rho(x)dx = \int_0^1 \sum_{m=0}^{\infty}(m^2+4m+4)\frac{\mu^m}{m!}\exp(-\mu)\,\rho(x)dx =$$

$$= \int_0^1 (\mu^2 + \mu + 4\mu + 4)\rho(x)dx.$$

При записи последнего равенства были учтены свойства распределения Пуассона. При этом с учетом полученных ранее выражений $\mu(x) = \ln(x/\varepsilon)$. Легко убедиться, что для $\rho(x) = 1$ дисперсия числа случайных величин в ансамбле будет пропорциональна их среднему числу, что соответствует распределению Пуассона. Для того, чтобы относительные флуктуации числа частиц оставались постоянными с ростом среднего числа случайных величин в ансамбле, необходимо выполнение условия:

$$\int_\varepsilon^1 \ln^2\left(\frac{x}{\varepsilon}\right)\rho(x)dx \Big/ \left[\int_\varepsilon^1 \ln\left(\frac{x}{\varepsilon}\right)\rho(x)dx\right]^2 > 1 \text{ при } \varepsilon \to 0.$$

Исследования показывают, что для широкого класса функций приведенное выше отношение равно единице, что соответствует Пуассоновскому характеру флуктуаций. Но при $\rho(x)\sim 1/x$ указанное выше соотношение выполняется, и флуктуации числа случайных величин в ансамбле остаются постоянными с ростом их среднего значения.

$$-\int_\varepsilon^1 \ln^2\left(\frac{x}{\varepsilon}\right)\frac{1}{x\ln\varepsilon}dx = \frac{1}{3}\ln^2\frac{1}{\varepsilon}, \text{ а } \left[\int_\varepsilon^1 \ln\left(\frac{x}{\varepsilon}\right)\frac{dx}{x\ln\varepsilon}\right]^2 = \frac{1}{4}\ln^2\frac{1}{\varepsilon}.$$

Таким образом, вид распределения первой случайной величины в алгоритмах, учитывающих закон сохранения на каждом шаге, может существенным образом изменить характер относительных флуктуаций числа случайных величин в ансамбле. Следует отметить, что асимптотическое поведение одночастичного распределения при малых значениях *x* при этом сохраняется.

Введение распределения $\rho(1-x)$ для первой случайной величины может существенно исказить одночастичное распределение при $x > 0.5$, сопровождающееся уменьшением средней множественности. Скорректировать данное изменение можно, проведя дополнительное случайное деление значения первой случайной величины на фиксированное число составных частей.

Литература:

1. Былинкин, А.А. Двухкомпонетная модель для рождения адронов при столкновении частиц высокой энергии: дис. кан. физ.-мат. наук., 01.04.16 – Физика атомного

ядра и элементарных частиц / А.А. Былинкин. – М.: Институт теоретической и экспериментальной физики, 2014. – 88 с.

2. Сарычева Л.И. Физика фундаментальных взаимодействий: Спецкурс / Л.И. Сарычева. – М.: КДУ, 2008. – 220 с.

3. Литвинов, В.А. Независимое использование множественности и коэффициентов неупругости в эмпирической модели ядерных взаимодействий / В.А. Литвинов // Известия высших учебных заведений. Физика, 1986. – Т.29. – №1. – С.127.

4. Uchaikin, V.V., Litvinov V.A. The model of independent particles emission in the multiparticle production theory / V.V. Uchaikin, V.A. Litvinov.– Proc. 19th Inter. Cosmic Ray Conf.– 1985.– V.6.–P.266–269.

Ловцов Д.А.
Российский государственный университет правосудия

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ НАДЕЖНОСТИ ТЕЛЕМАТИЧЕСКОЙ СЕТИ ГАС РФ «ПРАВОСУДИЕ»

Обоснована и декомпозирована математическая постановка задачи ситуационного управления защищённым обменом привилегированной информацией в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов в телематической сети с произвольной топологической структурой; предложен способ решения поставленной сложной задачи, а также определены организационно-правовые и технологические мероприятия в рамках международно-правовой стандартизации основных сетеобразующих протоколов глобальной сети Интернет как одного из эффективных путей решения проблемы обеспечения информационной надежности телематической сети ГАС РФ «Правосудие».

Ключевые слова: информационная надежность, телематическая сеть, привилегированная информация, система доменных имён, протокол пограничного шлюза, международные технико-правовые стандарты, инфраструктура открытых ключей, криптографические алгоритмы

Телематическая сеть (ТМС) Государственной автоматизированной системы Российской Федерации (ГАС РФ) «Правосудие», в которой осуществляется защищённый обмен привилегированной информацией, иерархически объединяет множество территориально распределенных информационно-вычислительных сегментов объектов автоматизации: Верховного Суда РФ, судов общей юрисдикции, органов Судебного департамента, центров подготовки и обучения, центров поддержки и др. Каждый сегмент практически представляет собой локальную информационно-вычислительную сеть с единой точкой подключения (через узлы защиты) к глобальной вычислительной сети Интернет.

Поскольку оборудование и каналы связи общедоступной сети Интернет не контролируются средствами защиты корпоративной сети ГАС РФ «Правосудие», в целях обеспечения информационной безопасности следует предполагать наличие внешнего нарушителя, способного перехватывать, модифицировать, подделывать или уничтожать информационные массивы (ИМ), передаваемые по общедоступной сети. В связи с этим при построении и развитии корпоративной сети ГАС РФ «Правосудие» необходимо применение средств защиты, препятствующих взаимодействию внешнего нарушителя с узлами корпоративной сети, а также обеспечивающих конфиденциальность, аутентичность и целостность [8] информации, передаваемой между сегментами. Кроме того, следует учитывать также возможность различных возмущающих воздействий случайного характера на информационные ресурсы корпоративной сети.

Таким образом, телематическая сеть ГАС РФ «Правосудие» функционирует в условиях ситуационной неопределённости среды, определяемой всевозможными дестабилизирующими (возмущающими) факторами $\omega_i \in \Omega$, i = 1,2…, двух типов:

случайными, т. е. технической ненадёжностью средств ТМС, различными видами погрешностей криптопреобразования и др.;

преднамеренными – воздействиями нарушителя политики безопасности (противника) на аппаратно-программные средства ТМС, осуществляемыми как по традиционным, так и по нетрадиционным (скрытым) информационным каналам (НИК) [5].

Алгебраическую модель процесса защищённого обмена привилегированной информацией (включая криптопреобразования и маршрутизацию) в ТМС можно представить в виде [3]:

$$\begin{cases} < M_0, M_1, \Phi, \Omega, f(M_0, M_1, \Omega), \tau >, \\ a_M(Q) : M_0 \times \Omega \longrightarrow M_1 \times \Omega, \end{cases} \quad (1)$$

где M_0 – множество исходных информационных массивов (ИМ) – оригиналов, предназначенных для защищённой передачи посредством ТМС потребителю; M_1 – множество ИМ, преобразованных с использованием некоторого алгоритма $a_M(Q) \in A_M$ криптопреобразования и маршрутизации и переданных потребителю; Ф – структура алгебраической модели ТМС (определяет количество структурной – преобразующей информации [4]); $\Omega = \{\omega_i\}$, i=1,2… – множество факторов неопределённости; f – конкретный вид ситуационного (характеризуется Ω) распределения сложных событий, состоящих в том, что на входе ТМС действует ИМ $m_{0i} \in M_0$, а на выходе через определённый промежуток времени τ появляется ИМ $m_{1j} \in M_1$.

Согласно модели (1) алгоритмического процесса криптопреобразования и маршрутизации ИМ в ТМС меру (оценку) технологического эффекта, получаемого от данной ТМС как совокупности взаимосвязанных информационных узлов в результате выполнения процесса криптопреобразования и маршрутизации ИМ, можно определить в виде функции

$$E\{f(M_0, M_1, \Omega)\}. \quad (2)$$

Кроме традиционного требования аддитивности к функции (2) можно предъявить следующие требования:

$$E(f) = \begin{cases} 0, \text{ если } p(m_{0i}, m_{1j}) = p(m_{0i})\, p(m_{1j}), \\ \max, \text{ если } p(m_{1j} \mid m_{0i}) = p(m_{0i}, m_{1j}) / p(m_{0i}) = 1. \end{cases} \quad (3)$$

Первое равенство в требовании (3) соответствует случаю полной статистической независимости событий, состоящих в поступлении на вход ТМС $m_{0i} \in M_0$, и событий, состоящих в образовании на выходе $m_{1j} \in M_1$. Второе равенство соответствует идеальному случаю, когда m_{1j} является результатом применения алгоритма $a_M(Q) \in A_M$ к ИМ m_{0i}. Всем перечисленным требованиям удовлетворяет функция

$$E(f) = \ln\{p(m_{0i}, m_{1j}) / p(m_{0i})\, p(m_{1j})\}. \quad (4)$$

Усреднение по всем парам $<m_{0i}, m_{1j}>$ даёт меру технологического эффекта функционирования ТМС:

$$E = \sum_i \sum_j p(m_{0i}, m_{1j}) \ln\{p(m_{0i}, m_{1j}) / p(m_{0i})\, p(m_{1j})\}. \quad (5)$$

Выражение (5) преобразуется к виду [4, 11]:

$$E = H(M_1) - \sum_i p(m_{0i})\, H(M_1 \mid m_{0i}), \quad (6)$$

где $H(M_1) = \sum_j p(m_{1j}) \ln\{p(m_{1j})\}$; $H(M_1 \mid m_{0i}) = \sum_j p(m_{1j} \mid m_{0i}) \ln\{p(m_{1j} \mid m_{0i})\}$.

С учетом (6) определим выражение для имеющего практическое значение показателя информационной надёжности функционирования ТМС:

$$Q = E / H(M_1), \quad (7)$$

где $Q \in (0, 1]$ – информационная надёжность равна 1 в случае отсутствия дестабилизирующих факторов.

При этом под информационной надежностью [3, 6, 8] функционирования ТМС понимается свойство подсистемы контроля и защиты информации выполнять требуемые функции криптопреобразования, маршрутизации и доставки информационных массивов, циркулирующих в ТМС в условиях информационного соперничества, характеризующее степень защищённости обмена привилегированной информацией и заключающееся в способности не допускать случайного или целенаправленного искажения, разрушения, раскрытия, модификации или переадресации информационных массивов.

Числовой пример. Посредством ТМС в VPN-подсети осуществляется защищённая передача (преобразование, маршрутизация и доставка) ИМ (сообщений, пакетов) m_{0i}, i = 1,…,3 в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов Ω. Преднамеренные помехи, осуществляемые, главным образом, по НИК, направлены на переадресацию (ложную маршрутизацию через внешние для VPN-подсети информационные узлы) отдельных авторизованных ИМ m_{0i}, i = 1,…,3, а также на инфильтрацию ложных ИМ m_{0i}, i = 4,…,5. Результатами работы алгоритма a_M криптопреобразования, маршрутизации и доставки ИМ m_{0i}, i = 1,…,3 потребителю являются ИМ m_{1j}, j = 1,…,3. Распределение $f(M_0, M_1, \Omega)$ описывается матрицей совместных вероятностей ИМ m_{0i} и m_{1j} (которую можно составить непосредственно перед реализацией защищённого обмена привилегированной информацией на основе проведения сеансов маскирующего обмена):

$$f = \begin{Vmatrix} 0{,}12 & 0{,}02 & 0{,}04 & 0{,}04 & 0{,}02 \\ 0{,}05 & 0{,}08 & 0{,}12 & 0{,}10 & 0{,}03 \\ 0{,}10 & 0{,}05 & 0{,}03 & 0{,}12 & 0{,}08 \end{Vmatrix}$$

Отсюда с учетом (6) получим: E = 0,14 бит;

$P(M_1) = < 0{,}24 \quad 0{,}38 \quad 0{,}38 >$, что даёт $H(M_1) = 1{,}55$ бит.

Тогда: $Q = E / H(M_1) = 0{,}1$.

Выражения (5) – (7) получены на основе общепринятых методов, основанных на том, что само понятие технологической эффективности имеет статистический характер [7].

В отношении показателя (7) доказана [6] справедливость следующего утверждения-теоремы: уровень Q информационной надёжности ТМС с произвольной топологической структурой определяется соответствующим локальным показателем выходного информационного узла L (l = 1,…,L) при любых условиях, т. е. $Q \le Q_L$.

Таким образом, математическую постановку задачи ситуационного управления защищённым обменом привилегированной информацией в условиях воздействия значительных случайных и преднамеренных дестабилизирующих факторов [7] в ТМС с произвольной топологической структурой сети можно представить в виде:

$$K: Q(w^*, \tau) = \max_{\{W\}}, \quad (8)$$

$$Q(w) = E / H(M_1) = 1 - \{\sum_i p(m_{0i}) H(M_1 | m_{0i})\}/H(M_1), \; i = 1,\ldots,I;$$

$$Q \in (0, 1]; \; W = \{w_j\}, \; j = 1,\ldots,J; \; t_p < \tau < T,$$

где $w_j = <R, C, t_p>$ – набор ключевых параметров; $R \ge R^0$ – результативность (стойкость к взлому, случайному сбою, воздействию НИК и др.); $C \le C^0$ – ресурсоемкость алгоритмов криптопреобразования и маршрутизации; t_p – временные затраты на криптопреобразование и маршрутизацию, τ – время доставки ИМ; $T \le T^0$ – время актуальности ИМ.

Задача в данной постановке (8) является сложной многопараметрической многоэтапной оптимизационной задачей оперативного стохастического программирования, методов решения которой в настоящее время не существует. Особенностью данного

типа задач является, в частности, то, что её надо решать каждый раз заново, учитывая сложившуюся ситуацию (ситуационное описание ТМС). Логическая декомпозиция сформулированной задачи выявила следующие частные (относительно простые) прикладные подзадачи:

- формализации ситуации (настройки расчётных алгоритмов);
- распределения наборов w_j, $j = 1,\ldots,J$ ключевых параметров;
- модификации криптопреобразования ИМ (по отечественным ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94);
- выработки усиленной электронной подписи (возведения в степень по модулю, умножения чисел по модулю, сложения чисел по модулю);
- проверки усиленной электронной подписи (вычисления обратного элемента по модулю (может быть вычислен путём возведения в степень Q-2 по модулю Q), двух возведений в степень по модулю P, двух умножений по модулю Q);
- хэширования (вычисления Ψ^k – k-й степени преобразования Ψ применяемой в составе шифрующего преобразования алгоритма вычисления шаговой функции хэширования);
- модификации сетеобразующих протоколов:

разрешения доменных имён DNS (Domain Name System – система доменных имён) – защищённой трансляции символьных доменных имён в IP-адреса узлов сети Интернет; хранения и передачи подписей служебной информации, хранения и передачи открытых ключей, защиты отрицательных ответов;

глобальной динамической маршрутизации BGP (Border Gateway Protocol – протокол пограничного шлюза) – «проверки источника» информации о блоках сетевых адресов, опирающейся на существующую систему региональных интернет-регистратур (в выделенном регионе регистрирует домены, выдаёт *IP*-адреса, выделяет адреса автономных систем и др.), основанной на использовании усиленной электронной подписи и требующей использования расширения инфраструктуры публичных ключей PKI (Public Key Infrastructure – инфраструктура открытых ключей) для аутентификации; разделения принятия решений о маршрутизации и реализации собственно транзита трафика между двумя различными элементами – платформой управления маршрутами и собственно маршрутизатором) [7].

Для обеспечения (повышения) информационной надежности функционирования ТМС представляется целесообразным разработать соответствующую методику, реализующую алгоритмы и протоколы выполнения перечисленных частных прикладных подзадач и обеспечивающую численную оценку соответствующих показателей следующих трёх групп, имеющих практическое значение: результативности (стойкости к взлому, к случайному сбою, к воздействию НИК), оперативности (времени реализации алгоритмов криптопреобразования и маршрутизации) и ресурсоёмкости (расходования оперативной памяти сетевых процессоров).

В настоящее время известно множество относительно надёжных (безопасных, достоверных, устойчивых) вариантов сетеобразующих протоколов, принятых интернет-сообществом в форме RFC ("Requests for Comments" – «требования к обсуждению»), играющих роль международных технико-правовых стандартов.

В частности, стандартизирующей международной организацией (СМО) IETF (Internet Engineering Task Force – Инженерный совет Интернета) принят стандарт (RFC) защищённого протокола разрешения доменных имен DNSSec (DNS Security), предлагающий весьма надёжную криптографическую защиту протокола DNS и сохраняющий полную обратную совместимость с ним, т.е. обеспечивающий возможность в защищённом от искажений виде выполнять трансляцию символьных доменных имен в IP-адреса узлов ТМС. При этом основными вспомогательными протоколами являются: RRSIG –

протокол хранения и передачи подписей служебной информации протокола DNS, DNSKEY – протокол хранения и передачи открытых ключей, NSEC – протокол защиты отрицательных ответов.

Существуют принятые СМО IETF международные стандарты модифицированного протокола глобальной маршрутизации BGP:

- SIDR-RPKI (Resource PKI) – предусматривает построение системы «проверки источника» (origin validation) информации о блоках сетевых адресов, опирающейся на существующую систему региональных интернет-регистратур (при европейской региональной интернет-регистратуре *RIPE* (*Reseaux IP Europeens* – Европейские *IP*-сети) создана наиболее развитая база информации об актуальных связях автономных систем между собой), основан на использовании электронной цифровой подписи (обеспечивая невозможность подделки информации по пути её следования к потребителю) и требует использования расширения инфраструктуры публичных ключей);

- RCP (Route Control Platform – платформа управления маршрутами) – предусматривает концептуальное разделение принятия решений о маршрутизации и реализации транзита трафика между двумя различными элементами: платформой (процессором) управления маршрутами и собственно маршрутизатором.

Вместе с тем проблема информационной надежности телематической сети ГАС РФ «Правосудие» и ее абонентов-пользователей остаётся актуальной, что обусловлено как несовершенством традиционных и предлагаемых СМО IETF модифицированных сетеобразующих протоколов, так и возможностью несанкционированного доступа к циркулирующей привилегированной информации с использованием НИК.

Например, в результате несанкционированного воздействия на протокол BGP возможно изменение маршрутов передачи привилегированной информации с выходом из контролируемой зоны для её сбора и содержательного анализа (криптоанализа), что может остаться незамеченным для взаимодействующих абонентов используемого сегмента телематической сети. При несанкционированном воздействии на протокол DNS и искажении таблиц IP-адресов (необходимых для трансляции символьных доменных имён) ряда серверов возможна задержка и даже потеря передаваемых сообщений, а также их замена и инфильтрация нелигитимных данных.

Всё это обусловливает возможность отдельным государствам управлять работоспособностью крупномасштабных ТМС в других государствах того же региона. Поскольку угроза попыток влияния на региональную интернет-регистратуру со стороны властей страны, в которой она расположена, представляется вполне реальной, так как соответствующая организация является, как правило, юридическим лицом, подчиняющимся законам страны пребывания, в том числе и её силовым органам и спецслужбам, и отказ, в частности, выполнения требования спецслужб об изъятии какой-либо записи из базы данных (что приведёт к прекращению маршрутизации для соответствующего блока сетевых адресов) представляется маловероятным.

Более того, существует риск «политических» деструктивных атак как на DNSSec, так и на SIDR. Причём, если в первом случае атаки возможны только как прямое недружественное действие по отношению к соответствующему государству или владельцу зоны DNS, а значит, последствия и резонанс такой атаки будут максимальны, то во втором случае местом проведения атаки является база данных региональной интернет-регистратуры, а объектом может быть отдельный блок сетевых адресов, содержащий конкретные сетевые ресурсы в конкретной стране, т.е. такая атака может направляться на конкретный ресурс, организацию и др. и не позиционироваться как недружественный акт на международном уровне. Однако и в первом случае для атак такого рода все возможности имеются, поскольку управление корневой (root) зоной DNS осуществляет американская организация ICANN (Internet Corporation for Assigned Names and Numbers

– Международная корпорация по присвоению имён и номеров), а техническое сопровождение работ по созданию наполнения зоны осуществляет американская компания Verisign, Inc (компания в г. Рестон, штат Вирджиния, поддерживающая разнообразные сетевые структуры, включая два из тринадцати существующих корневых серверов *DNS*, и др.).

Вообще говоря, все атаки, типичные для SIDR, имеют смысл и для DNSSec, в частности, это уничтожение валидной записи искажением одного бита при ее передаче (электронная цифровая подпись будет неверна), имитация отказа держателя зоны от использования DNSSec (“downgrade attack”), атаки на «центр» инфраструктуры и на каналы, по которым он распространяет информацию и др.

Кроме того, применение криптографических средств в данных сетеобразующих протоколах вносит в них множество новых возможных «уязвимостей», связанных со стойкостью используемых криптографических алгоритмов, с используемыми процедурами генерации, распределения, хранения и смены ключей [8]; процедурами выпуска и отзыва сертификатов электронной цифровой подписи и др. В этой связи необходимо заметить, что если в протоколе DNSSec предусмотрена возможность выбора и использования различных криптографических алгоритмов, то проект SIDR предусматривает использование только одного криптографического алгоритма и даже необходимость (в случае его компрометации) наличия механизма его смены (algorithm rollover) не осознавалась до недавнего времени разработчиками этого проекта.

Наиболее тревожным представляется то, что последовательное внедрение валидации информации с помощью криптографических средств приведёт к выделению в ТМС определённых «центров», которые будут выполнять роль и функции «центров доверия». Такие «центры» станут, очевидно, привлекательной целью для различного рода атак, как технологических, так и организационно-политических. Также важным представляется то, что надёжность сетеобразующих протоколов после их модернизации становится зависимой от надёжности использованных в них криптографических алгоритмов, а также уверенности в их высоком качестве и отсутствии недекларированных возможностей.

Наконец, процесс внедрения разрабатываемых модернизаций займёт, скорее всего, значительный период времени (возможно, несколько лет), и всё это время телематические сети будут должны обеспечивать функционирование протоколов одновременно и в «модернизированном» и в «немодернизированном» режимах, что открывает различные возможности проведения “downgrade attacks”, а также сохраняет возможности для различных форм киберпреступности (включая крэкинг, спаминг, фишинг, кибersквотинг и др.).

В связи с наличием принципиально неустранимых уязвимостей современных сетеобразующих протоколов, снижение вероятности отказов сети Интернет на территории России можно обеспечить только комплексом организационно-правовых и технологических мероприятий, направленных либо на снижение вероятности реализации уязвимостей за счёт ограничений, накладываемых на информацию, циркулирующую в сетеобразующем протоколе, либо на уменьшение негативного эффекта при её реализации (уменьшение времени обнаружения причин уязвимости, локализацию области распространения неверной информации, уменьшение времени восстановления сетевой связности и др.).

В такой комплекс мероприятий в частности, входят:

- разработка регламентов для основных операторов национального сегмента сети Интернет по конфигурированию протокола глобальной маршрутизации BGP, учитывающих мировую практику и имеющих целью уменьшить вероятность реализации уязвимостей протокола BGP;

- разработка регламентов для операторов национального сегмента сети Интернет, обеспечивающих использование операторами локальных баз данных и локальной системы корневых серверов;
- разработка регламентов (например: *RFC* 5830. *GOST* 28147-89. *Encryption, Decryption, and Message Authentication Code Algorithms. March* 2010; *RFC* 5831. *GOST* R 34.11-94. *Hash Function Algorithm. March* 2010; *RFC* 5832. *GOST* R 34.10-2001. *Digital Signature Algorithm. March* 2010; *RFC* 5933. *GOST* R 34.10-2001. *Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC. July* 2010) по использованию в системах защиты сетеобразующих протоколов сети Интернет и обеспечивающих служб сертифицированных криптографических средств защиты информации, опирающихся на отечественные криптографические алгоритмы;
- разработка регламентов по внесению информации о критически важных ресурсах сети Интернет в сетеобразующие протоколы и мерах по обеспечению её неискаженного состояния для операторов сети Интернет, предоставляющих соединение с сетью Интернет для подобных ресурсов;
- создание распределённой системы мониторинга и предупреждения о фактах распространении недостоверной информации по сетеобразующим протоколам;
- создание распределённой системы мониторинга актуальной сетевой информации о критически важных ресурсах сети Интернет, а также о ресурсах, поддержание непрерывной работоспособности которых считается важным с экономической, политической или социальной точек зрения;
- создание локальной системы корневых серверов протокола DNS, синхронизированной по содержанию с глобальными корневыми серверами, но находящейся под национальным контролем и управлением;
- внедрение средств обеспечения целостности и непротиворечивости информации в базах данных регистратур DNS, защиты этих баз данных от возможных атак, а также средств и методик контроля целостности информации в этих базах;
- внедрение средств контроля целостности и непротиворечивости информации в базах данных региональных интернет-регистратур;
- организация локальной базы данных о существующих блоках сетевых адресов, синхронизированной по содержанию с базами данных региональных интернет-регистратур, но находящейся под национальным контролем и управлением.

Целесообразным представляется также активное участие в процессе модернизации существующих сетеобразующих протоколов российских специалистов и экспертов, с целью обеспечения учёта требований, необходимых для обеспечения безотказной работы национального сегмента сети Интернет в Российской Федерации, противодействия внедрению технологий, ведущих к концентрации возможностей глобального управления сетью Интернет, в том числе на территории и за пределами Российской Федерации. При этом следует поддерживать модернизации существующих сетеобразующих протоколов и обеспечивающих их служб, направленные на усиление защиты и повышение достоверности информации, циркулирующей в протоколах и обеспечивающих службах.

Как правило, такие модернизации в настоящее время существенно опираются на использование криптографических алгоритмов, в связи с чем представляется целесообразным продвижение отечественных криптографических алгоритмов как стандартных элементов соответствующих протоколов, с целью обеспечения возможности их использования в модернизированных сетеобразующих протоколах как минимум в пределах национального сегмента сети Интернет.

Соответствующий комплекс эффективных алгоритмов и протоколов, отвечающих требованиям отечественных ГОСТ и предлагаемых RFC, в составе специализированной

(проблемно-ориентированной) функциональной базы данных и знаний подсистемы контроля и защиты информации в ГАС РФ «Правосудие» позволит снизить деструктивное влияние возможных дестабилизирующих (возмущающих) факторов, и, прежде всего, преднамеренных, что позволит повысить (на 20 – 25%) общий уровень информационной надёжности телематической сети ГАС РФ «Правосудие».

Вместе с тем, поскольку в настоящее время среди вновь разрабатываемых и исследуемых протоколов нет чётко выраженных «преемников» для существующих сетеобразующих протоколов BGP и DNS, следует активно принимать участие в правовых и технологических исследованиях и разработках по данной тематике, чтобы формировать направления развития новых протоколов, их свойства и характеристики так, чтобы они по принципам их построения и реализации обеспечивали более высокую защищённость, надёжность и устойчивость функционирования национального сегмента сети Интернет по сравнению с настоящим временем.

Таким образом, представляется необходимым для обеспечения требуемого уровня информационной надежности функционирования телематической сети ГАС РФ «Правосудие» и её абонентов-пользователей:

принимать активное участие в разработке новых сетеобразующих протоколов и модернизации существующих;

модификацию сетеобразующих протоколов с целью повышения их эффективности тесно связать с модификацией криптографической части этих протоколов, в связи с чем Российской Федерации следует принять все предлагаемые СМО IETF модификации сетеобразующих протоколов при условии замены использующихся криптографических алгоритмов на отечественные алгоритмы ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001;

определить порядок использования криптоалгоритмов в сетеобразующих протоколах национального сегмента сети Интернет, а также порядок работы с криптографическими ключами и обеспечить выполнение этих требований операторами связи;

вести целенаправленную работу по международно-правовой стандартизации используемых криптографических алгоритмов.

Литература:

1. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. – 2012. – № 4. – С. 3 – 7.

2. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. – М.: Наука, 2005. – 248 с.

3. Ловцов Д. А. Информационные показатели эффективности функционирования АСУ сложными динамическими объектами // Автоматика и Телемеханика. – 1994. – № 12. – С. 143 – 150.

4. Ловцов Д. А. Модели измерения информационного ресурса АСУ // Автоматика и Телемеханика. – 1996. – № 9. – С. 3 – 17.

5. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ РАН. Сер. 2. Информ. процессы и системы. – 2005. – № 2. – С. 1 – 7.

6. Ловцов Д. А. Информационные оценки технологической эффективности переработки информации // НТИ РАН. Сер. 2. Информ. процессы и системы. – 1997. – № 11. – С. 22 – 26.

7. Ловцов Д. А., Кабелев Д. Б. Ситуационное управление защищённым обменом привилегированной информацией в АСУ специального назначения // Труды XXX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (30 июня – 1 июля 2011 г.) в 5-и т. Т. 4 / РАН, РАО. – Серпухов: Серп. воен. ин-т, 2011. – С. 166 – 169.

8. Ловцов Д. А., Кабелев Д. Б. Технология и проблемы рационального управления ключевой информацией в АСУ специального назначения / // Труды XXIX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (24 – 25 июня 2010 г.) в 5-и т. Т. 4 / РАН, РАО. – Серпухов: Серп. воен. ин-т, 2010. – С. 144 – 148.

9. Шилейко А. В., Кочнев В. Ф., Химушин Ф. Ф. Введение в информационную теорию систем. – М.: Радио и связь, 1985.

Майлатов И.С., Швец Н.А., Щербаков В.А., Васин О.И.
Краснодарское высшее военное училище
имени генерала армии С.М.Штеменко

АНАЛИЗ СПОСОБОВ И СРЕДСТВ ЗАЩИТЫ КАНАЛОВ ПЕРЕДАЧИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ

Передача телеметрической информации (ТМИ) по радиоканалу сопряжена с угрозой ее перехвата и модификации. Трафик радиоканала может быть перехвачен и проанализирован атакующей стороной с помощью приемника, настроенного на частоту передающего устройства.

Целью данной статьи является исследование путей защиты каналов передачи ТМИ от угрозы её перехвата и модификации на основе анализа существующих способов и средств, выбора наиболее перспективных их них и выработке предложений и рекомендаций по их практическому применению.

Для передачи информации о значениях измеряемых параметров, контролируемых и управляемых объектов методами и средствами телемеханики, используются каналы ТМИ. В качестве среды передачи данных используются как беспроводные (радио, GSM/GPRS, ZigBee, Wifi, WiMax, LTE), так и проводные (телефонные, ISDN, xDSL, компьютерные) сети. Сущность телеизмерения заключается в том, что измеряемая величина, предварительно преобразованная в ток или напряжение, дополнительно преобразовывается в сигнал, который затем передается по каналу связи. Таким образом, передается не сама измеряемая величина, а эквивалентный ей сигнал, параметры которого выбирают так, чтобы искажения при передачи были минимальными [1].

Для проектирования телеметрической системы удобно пользоваться иерархическим представлением, которое позволяет логически группировать функции телеметрической системы в уровни и устанавливать связи между этими уровнями.

Рисунок 1 иллюстрирует телеметрическую систему, представленную в виде семиуровневой иерархической модели, построенной по образцу модели OSI (open system interconnection).

Так как одно из основных требований, предъявляемых к телеметрической системе - безошибочная доставка данных, для их защиты от ошибок, вызванных шумами радиоканала, используется кодирование канала. Для этого в передаваемое сообщение вставляются дополнительные биты. При повреждении сообщения дополнительные биты помогают восстановить исходное сообщение. Для защиты данных от шумов физического канала битовый поток кодируется одним или обоими следующими кодами:

- блочный код Рида-Соломона
- сверточный код

Рис. 1. Иерархическая модель телеметрических служб

Благодаря комбинации этих кодов, канал практически освобождается от ошибок [2].

Исходя из иерархической модели телеметрических служб и того, что ТМИ может передаваться беспроводным путем, защита информации возможна только на уровне прикладного процесса. В диссертационной работе [3] представлены следующие требования к защите каналов передачи информации:

1. Защита от несанкционированного дешифрования информации, передаваемой по каналу передачи.
2. Целостность данных при передаче.
3. Защита внутренней структуры сети при передаче сообщений.
4. Надежная система аутентификации.
5. Криптографически стойкий алгоритм аутентификации.
6. Взаимная аутентификация обеих сторон.
7. Механизм смены секретных ключей.

К каждому требованию принято выделять отдельные способы и средства для их удовлетворения.

Для защиты от несанкционированного дешифрования информации используются криптографические алгоритмы. Они делятся на симметричные (один ключ для шифрования и дешифрования) и ассиметричные (два различных ключа) шифры. Симметричные шифры обладают меньшей степенью защищенности, так как при раскрытии ключа одной из сторон, другая сторона становится также раскрытой.

Шифры могут быть сконструированы так, чтобы возможно было либо шифровать сразу весь текст, либо шифровать его по мере поступления. Таким образом, они разделяются на блочные (шифруют сразу весь блок текста) и поточные (шифруют информацию и выдают шифротекст по мере поступления) шифры.

Поточные шифры RC4 (Rives Cipher 4), A5, Mosquito были взломаны и не могут использоваться для защиты каналов передачи ТМИ.

Блочные шифры ГОСТ 28147-89, AES (Advanced Encryption Standard), Blowfish, Des обладают высокой криптостойкостью, но даже их возможно взломать с помощью криптоанализа, если иметь необходимое количество шифротекста. Решить эту проблему помогает механизм смены секретных ключей.

Для противодействия атакам типа «повторное использование ключей» и «изменение содержимого передаваемых пакетов» были разработаны механизмы смены секретных ключей TKIP (Temporal Key Integrity Protocol) и CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Вместо использования одного статического ключа для каждого передаваемого пакета создается новый ключ, который автоматически создается и рассылается сервером аутентификации. CCMP более надежный, чем TKIP, так как использует алгоритм шифрования AES вместо RC4.

Протоколы TKIP и CCMP используют сервер аутентификации для рассылки сгенерированных ключей. Аутентификация пользователя может производиться с помощью пароля или по сертификату пользователя. Чтобы не отправлять в открытом виде, их шифруют одним из алгоритмов шифрования, как правило AES. Так как для передачи сообщения нужен приемник и передатчик, то их необходимо аутентифицировать, после чего сервер сможет разослать в обе стороны ключи шифрования и дешифрования. Без аутентификации работа в сети будет запрещена. База зарегистрированных пользователей и система проверки в больших сетях расположены на специальном сервере (чаще всего RADIUS - Remote Authentication in Dial in User Service).

RADIUS - сервер является интерфейсом взаимодействия с телекоммуникационной системой и может реализовать для такой системы следующие сервисы:

Общие

- Создание и хранение учетных записей пользователей
- Сбор и анализ статистической информации о сессиях пользователя и всей обслуживаемой системы

Аутентификация

- Проверка учетных данных пользователя по запросу обслуживаемой системы

Авторизация

- Выдача разрешений к той или иной услуге

Совокупность всех этих способов и средств способна защитить каналы передачи ТМИ. Уязвимость хотя бы одного средства снижает защиту всей системы в целом. Для защиты каналов ТМИ, на основе проанализированных методов и средств, предлагается:

1. Настроить сервер аутентификации (например, RADIUS) для проверки учетных записей приемников и передатчиков информации. Процесс аутентификации должен проходить по защищенному каналу с использованием алгоритмов шифрования AES или ГОСТ 28147-89.

2. После аутентификации устройству выдаются права доступа к определенным ресурсам. Вместе с правами доступа передатчик получает ключ шифрования и может отправлять зашифрованные сообщения серверу отправки сообщений. Приемник после аутентификации получает ключ дешифрования и в дальнейшем способен получать сообщения от сервера отправки сообщений.

3. С помощью CCMP, через заданный интервал времени или при превышении лимита отсылаемых сообщений, сервер аутентификации отправляет приемнику и передатчику новые ключи шифрования по защищенному каналу.

Для передачи сообщений необходимо наличие специальных аппаратных средств. Такие средства получают зашифрованный входной пакет сообщений и отправляют его беспилотным робототехническим комплексам (БРК). Один такой передатчик способен отправлять пакеты сообщений сразу нескольким приемникам, находящимся в его зоне действия. С другой стороны, БРК может передвигаться из зоны действия одного передатчика в зону действия другого. Наличие передатчика за местом работы пользователя является при этом необязательным. Несколько пользователей способны передавать одному передатчику свои зашифрованные пакеты сообщений. Это приводит к схеме централизованного сервера рассылки сообщений (рис. 2).

Рис. 2. Схема отправки пакетов сообщений БРК

Предложенные методы и средства позволяют обмениваться секретными ключами между приемником и передатчиком. Постоянная смена секретных ключей обеспечивает криптостойкость алгоритма шифрования, так как снижает риск подбора ключа шифрования путем криптоанализа трафика сообщений. Сервер аутентификации ограничивает несанкционированный доступ к приёмнику. В случае распознавания противником информации для аутентификации пользователя, сервер аутентификации способен закрыть доступ на получение ключей шифрования. Передача информации на удаленные расстояния, особенно через беспроводные каналы связи, играет важную роль в развитии управления беспилотными робототехническими комплексами. В военной области эта задача усложняется высокими требованиями по защите информации. Множество существующих способов и средств защиты информации не удовлетворяют этим требованиям и являются уязвимыми, поэтому их дальнейшее развитие является актуальной задачей.

Литература:

1. Сорока Н.И., Кривинченко Г.А. Телемеханика: Конспект лекций для студентов специальности «Автоматическое управление в технических системах». ЧІ: Сообщения и сигналы, Мн.: БГУИР, 2000 - 133с.

2. Назаров А.В. Современная телеметрия в теории и на практике. Учебный курс. - Спб.: Наука и Техника, 2007. - 672 с.

3. Успенский А.Ю. Защита информации в радиоканалах мобильных робототехнических комплексов. дис. канд. тех. наук, Москва, 2006

Майлатов И.С., Швец Н.А., Щербаков В.А., Васин О.И.
Краснодарское высшее военное училище
имени генерала армии С.М.Штеменко

ОПРЕДЕЛЕНИЕ ВОЗМОЖНОСТИ ПРОВЕДЕНИЯ ПОИСКА ТЕХНИКИ И ДРУГИХ НОСИТЕЛЕЙ, СОДЕРЖАЩИХ ГОСУДАРСТВЕНУЮ ТАЙНУ, ПРИ ИХ ЗАТОПЛЕНИИ НА РАЗЛИЧНЫХ ГЛУБИНАХ

Одной из актуальных задач, стоящей перед службой ЗГТ является обеспечение сохранности ВВСТ и недопущение завладения ее противником при их преднамеренном и не преднамеренном затоплении.

Для решения такой задачи необходимо оценить возможности существующих и перспективных подводных технических средств Российского и иностранного производства по поиску и подъему ВВСТ и других носителей, содержащих сведения, составляющие ГТ, при их затоплении на различных глубинах.

Подводные аппараты, предназначенные для поиска и подъёма затонувших объектов, разделяются на обитаемые (ОПА) и необитаемые (НПА). ОПА предназначены для погружения с человеком на борту, поэтому такие аппараты крупнее в размерах, весят больше и обладают функциями жизнеобеспечения. Их основное преимущество заключается в том, что человек имеет непосредственный доступ к управлению аппаратом. НПА дистанционно управляются оператором, находящимся на судне или на берегу (телеуправляемый НПА - ТНПА), или работают самостоятельно по программе (автономный НПА - АНПА)

Морские необитаемые робототехнические комплексы военного назначения, находящиеся на эксплуатации в Вооруженных Силах Российской Федерации

1. Телеуправляемый необитаемый подводный аппарат (ТНПА) среднего класса «ВЕНОМ 1 К-100» (Разработчикизготовитель: ОАО «Тетис Про», г.Москва)

Назначение: обследование контактов, полученных поисковыми силами флота при поиске затонувших, аварийных, лежащих на грунте объектов; опознание и обследование подводных объектов; выполнение подводно-технических работ (ПТР) в объёме возможностей манипуляторного устройства, доставка на грунт или подъём на поверхность грузов;

Целевые нагрузки: 8 светильников по 250 Вт; до 8 видео или фотокамер; 2 ГБО; батиметрическая система; датчик катодного потенциала (CB-probe); гидроакустический маяк-ответчик (для позиционирования аппарата относительно судна-носителя при наличии на судне-носителе соответствующей системы позиционирования); гирокомпас; пяти и семи-функциональные манипуляторы; подводный гидравлический инструмент для выполнения широкого спектра ПТР; дополнительный контур гидравлической системы для привода гидравлического инструмента; гидромонитор;

Технические данные: система управления - дистанционная по кабелю; масса на воздухе - 3500 кг; размеры (ДхШхВ) - 3,2х1,8х1,8 м; глубина погружения - 3000 м; скорости - 3 узла; дальность действия - ограничена длиной кабеля 1500 м.

2. Телеуправляемый необитаемый подводный аппарат легкого класса «ТАЙГЕР» (разработчик/изготовитель: ОАО «Тетис Про», г. Москва, 2006; является адаптированной версией аппарата «Tiger» фирмы Saab Seaeye Ltd., UK)

Назначение: обследование контактов, полученных поисковыми силами флота при поиске затонувших и аварийных, лежащих на грунте, объектов. Документирование видео и гидроакустической информации;

Целевые нагрузки: цветная фотокамера высокой четкости; бортовая навигационная система с доплеровским лагом; инерциальная навигационная система с лазерными гироскопами; ГБО; гидроакустический донный профилограф, гидроакустическая система связи и др. ОАО «Тетис Про» поставляет 3 варианта ТНПА «Тайгер», различающиеся комплектацией вспомогательного оборудования: «Тайгер-1Т,-2Т,-3Т»;

Рис. 1. ТНПА «ВЕНОМ» 1 К-100

Технические данные: система управления - дистанционная по кабелю; масса на воздухе - 150 кг; размера (ДхШхВ) - 1,0х0,7х0,6 м; глубина погружения - 1000 м; скорость - 3 узла; дальность действия ограничена длиной кабеля; время непрерывной работы - неограниченно.

Рис. 2. ТНПА «ТАЙГЕР»

3. Малогабаритный телеуправляемый необитаемый подводный аппарат сверхлегкого класса «Обзор-150» (Разработчик/изготовитель: ОАО «Тетис Про», г. Москва, 2007)

Назначение: поиск подводный объектов и выполнения осмотровых и обследовательских работ под водой в прибрежных морских или внутренних водах, Аппарат может применяться для установки гидроакустических маркеров и подъёма предметов, захваченных манипулятором;

Целевые нагрузки: цветная видеокамера на платформе с изменяемым углом наклона; ч/б видеокамера на платформе с изменяемым углом наклона; компас; глубиномер; датчик температуры и др.;

Технические данные: система управления - дистанционная, через витую пару и оптоволоконный кабель; предусмотрен режим автоматического поддержания курса, глубины и скорости движения; масса на воздухе - 12кг; размеры (ДхШхВ) - 0,5х0,3х0,3 м; глубина погружения - до 600 м; скорость - 4 узла; максимальный радиус действия - 750 м.

4. Малогабаритные автономные необитаемые подводные аппараты среднего класса типа «РАЗУМ», 1992 (Разработчик/изготовитель: ФБГУ «ИПМТ ДВО РАН» г. Владивосток)

Назначение: обеспечение глубоководных аварийно-спасательных работ;

Целевые нагрузки: информационно-измерительный комплекс, включающий в себя ГБО, фотосистему, магнитометр, радиометр, датчики среды; передатчик гидроакустической навигационной станции, аналого-цифровой накопитель данных;

Технические данные: система управления - автономная с предварительной загрузкой программы в бортовой вычислитель АНПА; возможно переключение в режим телеуправления; масса на воздухе - 1200 кг; размеры (Д х диаметр) - 4,2 х 0,7 м; глубина погружения - 6000 м; скорость - 2 узла; время непрерывной работы - 6,0 ч[1].

Глубоководных подводных аппаратов, способных опускаться до 6000 метров в глубину, в мире немного. К отечественным относятся: «Мир-1» (находится в качестве экспоната в калининградском Музее Мирового океана) и «Мир-2» (базируется на борту научно-исследовательского судна «Академик Мстислав Келдыш»), «Русь» и его модернизированная версия «Консул».

Эти аппараты имеют маневренность, ход по горизонтали и вертикале, могут поворачиваться, нагибаться, брать образцы со дна, грузить их в небольшие контейнеры, исследовать окружающее пространство. Технические данные: запас энергообеспечения - 100 кВт*ч; запас плавучести - 290 кг; скорость (подводная) - 5 узлов; рабочая глубина погружения - 6000 м; предельная глубина погружения - 6500 м; экипаж - 2+1 человек; запас жизнеобеспечения - 246 чел. час; сухой вес - 18,6 т; размеры (ДхШхВ) 7,8х3,8х3 м[3].

Рис. 3. Подводный аппарат «Русь»

«Русь» принадлежит ВМФ РФ и предназначен для проведения исследований и подводных работ. Он может выполнять подводные технические работы с помощью манипуляторного устройства, обследовать подводные сооружения и объекты, доставлять на грунт или поднимать на поверхность предметы массой до 200 кг. Кроме того, он может перемещаться не только вертикально, но и горизонтально со скоростью до 3 узлов[4].

Кроме того, на вооружение военно-морского флота России поступают обитаемые подводные комплексы на основе аппаратов зарубежного производства - канадские батискафы АРС-600, способные работать на глубине до 1,5 тыс. м. АРС-600 в двухместной модификации весит чуть более 3 т и может использоваться с любого судна, где есть подходящий кран. Можно также транспортировать комплекс при помощи любого военного вертолета — в этом случае аппарат просто сбрасывается в море. На глубине он способен проводить осмотр аварийного объекта, передавая изображение с гидролокатора и камер высокого разрешения на поверхность в течение восьми часов.

Подводные технические средства иностранного производства по поиску и подъёму объектов.

Одним из востребованных обитаемых подводных аппаратов является «Глубоководный рабочий» (Deep Worker), разработанный канадской компанией Nuytco Research. Его особенностью является размеры, которые по кругу решаемых задач и своим способностям занимают промежуточное положение между жёсткими скафандрами для водолазных работ и двух- трёхместными исследовательскими глубоководными аппаратами. В воздухе робот весит 1.3 тонны, если в корпусе использован по большей части алюминий; и 1,75 тонны, если основной материал - сталь.

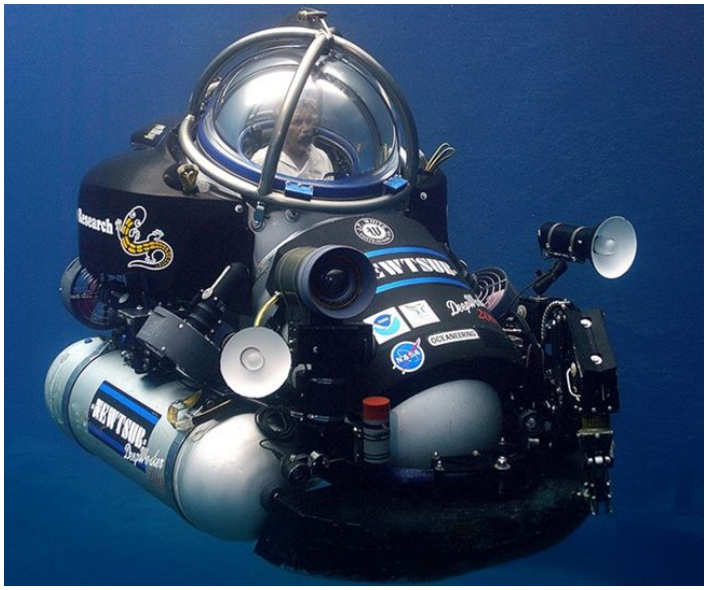


Рис. 4. Подводный аппарат «DeepWorker»

Компания-производитель предлагает своим клиентам выбор между более тяжёлой, но сравнительно недорогой, стальной субмариной и алюминиевым её аналогом, который, соответственно, дороже. Во всём остальном — это совершенно одинаковые подлодки. Рабочая глубина Deep Worker составляет внушительные для такого небольшого аппарата 600 метров. Полезный груз — 114 килограммов. Системы жизнеобеспечения рассчитаны на 106 часов. Его главный инструмент — две механические «руки», на которые можно устанавливать разнообразные «кисти». «Руки» эти превосходят в подвижности руки человека. Здесь применено псевдоконическое соединение звеньев манипулятора, дающее много степеней свободы. Для привода манипуляторов применена гидравлическая система, работающая на окружающей машину морской воде. Предел подъема полезного груза не позволит поднимать со дна тяжелые предметы, но наличие «рук» сможет компенсировать эти недостатки. Например, закрепив объект тросом к лебедке судна. Максимальную скорость в 4 узла машине обеспечивают четыре винта с электроприводом по 1 лошадиной силе каждый. Два из них поворачиваются и дают машине возможность двигаться по вертикали или смещаться боком[5].

В США создана система для подъёма тяжёловесных крупногабаритных грузов с больших глубин, основу которой составляет судно «Гломар Эксплорер» и погружаемая баржа НМВ-1. Основные характеристики судна: длина 188,3 м, ширина 35,2 м, осадка 14 м; водоизмещение 36000 т; мощность энергетическом установки 12 тыс. л. с., наибольшая скорость хода 12 узлов. Специальная динамическая система стабилизации, разработанная фирмой «Ханиуэлл», удерживает судно в период работ над затонувшим объектом с точностью ± 15 м. Она включает несколько водомётных движителей и винтов, размещённых вдоль борта. «Гломар Эксплорер» оснащено современным навигационным оборудованием для точного кораблевождения и удержания места, гидролокаци-

онной и телевизионной аппаратурой, а также стробированными осветителями для поиска объектов на морском дне. Управление энергетическом установкой и системой удержания места осуществляется с помощью ЭВМ. Управление судном на ходу осуществляется с носового ходового мостика, а при проведении глубоководных работ — с кормового мостика. Судно оборудовано высоким деррик-краном большой грузоподъёмности (до 7000 т), установленным в средней части корпуса для подъема грузов с помощью гидравлической системы. В средней части корпуса прорезана сквозная шахта, через которую от крана в воду проходит система тросов, труб и электрических кабелей. Экипаж судна 170 человек, из которых 40 входят в состав команды, обслуживающей систему подъёма. Второй составной частью системы подъёма являются погружаемая баржа НМВ-1, предназначаемая для крепления грейферов и транспортировки поднятых объектов. На ней имеются балластные цистерны, позволяющие ей погружаться и всплывать[2].

Самый новый и самый большой НПА от компании ATLAS Elektronik GmbH (г. Бремен, Германия) – универсальный аппарат «SeaOtter Mk II». «Морская выдра» – автономный НПА, выполняющий задачи разведки и наблюдения (включая разведку подводных лодок), обнаружения подводных угроз, сбора гидрографических данных, уничтожения мин. Кроме того, возможно скрытное обеспечение сил специального назначения и проведение спасательных мероприятий.

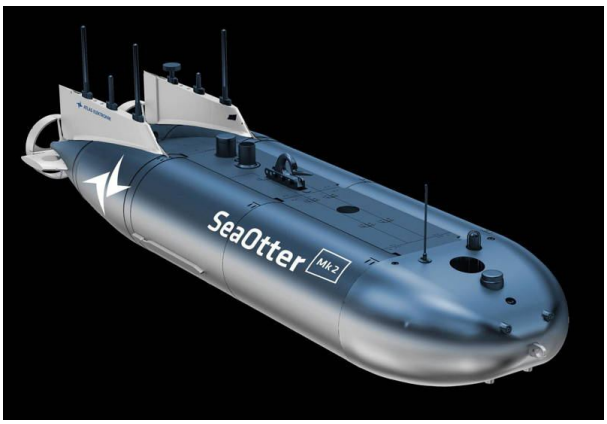


Рис. 5. НПА «SeaOtter Mk II»

Дрон длиной 3,65 м имеется водоизмещение 1200 кг, возможность использования 160 кг полезной нагрузки и продолжительность работы 24 часа. Оборудование НПА включает гидролокатор высокого разрешения с синтетической апертурой (SAS – Synthetic Aperture Sonar). Сонар обеспечивает обнаружение и идентификацию движущихся и неподвижных объектов. Антенна НПА позволяет вблизи от поверхности воды устанавливать радио и WiFi-связь с кораблем-носителем, а также навигацию по GPS. В дополнение к GPS, дрон использует автономную инерционную навигацию и электромагнитную систему доплеровского контроля скорости. В автономном режиме работы питание электропривода производится литиевыми полимерными батареями. Для их зарядки требуется четыре часа, но возможна замена для экономии времени.

ВМС Индии в настоящее время также используют разработанный в стране автономный подводный аппарат AUV-150. НПА имеет длину 4,8 м и достигает глубины 150 м. В прибрежных водах он используется для разведки и наблюдения, а также для разведки мин.

Рис. 6. Автономный подводный аппарат AUV-150

Студенты индийского технологического института в г. Мумбаи с 2011г.в свободное время разрабатывают названный в честь морского бога Матсья (Matsya) НПА с передовыми характеристиками по производительности. Если AUV-150 строго придерживается запрограммированных задач, то «Матсья» должен иметь более высокую степень автономии.

Круг задач в интересах ВМС Индии планируется расширить. НПА «Матсья», как ожидается, будет способен – наряду с ведением визуальной и акустической разведки – устанавливать и извлекать объекты с помощью манипулятора, а также поражать торпедами подводные лодки противника[6].

Представленные образцы ПА способны осуществлять подъем затонувших объектов, содержащих сведения, составляющих ГТ. ПА, предназначенные для поиска затонувших объектов, обладают большим преимуществом перед ПА для их подъема - они меньше в размерах и их можно использовать как «стаю», большое количество небольших аппаратов позволит быстрее найти затонувший объект. После нахождения затонувшего объекта стоит задача его поднятия со дна. Представленные образцы ПА для поднятия объектов со дна обладают различными характеристиками, такими как: предельная глубина и максимальная полезная нагрузка. Из-за различий в рельефе дна в разных частях океана необходимо использовать различные типы ПА. Так при глубине 6000 м. необходимо использовать глубоководные ПА. Тяжелые объекты, которые ПА не способен поднять, возможно поднять с помощью троса, закрепленного на судне. Но это требует наличие ПА способного закрепить трос на объекте. Множество деталей, возникающих при решении задачи поднятия объекта со дна, требуют разработки новых и многофункциональных ПА.

Анализ существующих и перспективных подводных робототехнических комплексов России и других стран, предназначенных для выполнения различных задач в интересах ВС в том числе задач по обнаружению и подъему затонувшей техники и других носителей, содержащих сведения, составляющие ГТ, позволил выделить следующие тенденции их развития:

- Автономности: первые беспилотные системы обычно были дистанционно управляемыми. За ними последовали системы, способные самостоятельно выполнять детально запрограммированную задачу. В перспективе будут востребованы полностью автономные системы, способные самостоятельно выполнять целевые задания в различных условиях обстановки.
- Координации действий между несколькими беспилотными системами различного назначения, а также скоординированное применение пилотируемых и беспилотных систем.

- Увеличения продолжительности выполнения операций: более эффективные двигатели и аккумуляторные системы увеличивают дальность и длительность работы.
- Укрупнения систем: увеличение универсальной полезной нагрузки, дальности и продолжительности работы.
- Модульной полезной нагрузки для выполнения различных задач одним типом необитаемых подводных аппаратов (НПА)[6].

Подводные аппараты, предназначенные для поиска мин, обследования донных объектов, мониторинга морского шельфа и т.д. также могут быть использованы для поиска затонувшей техники. Они не обладают столь высокими характеристиками по поиску как специализированные подводные аппараты, но при использовании их в большом количестве они способны ускорить процесс нахождения затонувшей техники и других носителей, составляющих ГТ.

Таким образом, существующие и перспективные возможности подводных технических средств поиска и подъёма затонувшей техники и других носителей, содержащих сведения, составляющих ГТ, создают потенциальную угрозу завладения ими противником. Одним из способов ликвидации такой угрозы является гарантированная самоликвидация сведений, составляющих ГТ.

Литература

1. А.В. Лопота, А.Б. Николаев. Морские робототехнические комплексы военного и специального назначения // Современные тенденции развития робототехнических комплексов - 2017. С. 48.

2. Средства поиска и подъёма затонувших объектов [Электронный ресурс] - Режим доступа: http://zvo.su/VMS/sredstva-poiska-i-podema-zatonuvshih-obektov

3. Глубоководные аппараты «Мир» [Электронный ресурс] - Режим доступа: http://ussr-kruto.ru/2012/09/21/glubokovodnyi-apparat-mir

4. Подводные аппараты военного назначения [Электронный ресурс] - Режим доступа: https://tvzvezda.ru/news/opk/content/201707121549-v8fk.htm

5. Подводные аппараты иностранного производства по поиску объектов [Электронный ресурс] - Режим доступа: https://masterok.livejournal.com/1639636.html

6. Необитаемые подводные аппараты военного назначения [Электронный ресурс] - Режим доступа: http://invoen.ru/issledovaniya/neobitaemye-podvodnye-apparaty

Майлатов И.С., Швец Н.А., Щербаков В.А., Васин О.И.
Краснодарское высшее военное училище
имени генерала армии С.М.Штеменко

РЕКОМЕНДАТЕЛЬНАЯ СИСТЕМА ПОДБОРА НАУЧНЫХ ТРУДОВ НА ОСНОВЕ ПОЛЬЗОВАТЕЛЬСКИХ ОЦЕНОК

Ввиду большого количества информации в компьютерных сетях пользователю сложно найти интересующий его материал. Рекомендательные системы пытаются предсказать, какие объекты будут интересны пользователю, имея определенную информацию о его профиле. Среди множества научных работ пользователю сложно найти информацию по интересующей его тематике. Подбор научных работ для пользователя является частным случаем рекомендательных систем.

Развитие рекомендательных систем основывается на наблюдении того, что люди часто полагаются на рекомендации от других людей. Выработка рекомендаций основывается на собранной информации о группе людей [1]. Подход, основанный на пользователях с похожими вкусами, называется коллаборативной фильтрацией [2].

Рекомендательные системы используют явные и неявные методы сбора данных о пользователе. Явные методы используют запросы к пользователю для выявления его

предпочтений, в то время как неявные отслеживают историю поведения пользователя в реальном времени [3].

Чтобы сгруппировать пользователей по похожести их предпочтений применяются методы кластеризации, цель которых - выявление групп в больших объемах данных. В разработанной системе применяется кластеризация методом k-средних. Кластеризация методом k-средних начинается с выбора k случайно расположенных центроидов (точек, представляющих центр кластера). Каждому элементу назначается ближайший центроид. После того, как назначение выполнено, каждый центроид перемещается в точку, рассчитываемую как среднее по всем приписанным к нему элементам. Затем назначение выполняется снова. Эта процедура повторяется до тех пор, пока назначения не прекратят изменяться [2]. Для определения расстояния между центроидами кластера и объектами используется корреляция Пирсона (1). Она наиболее предпочтительна по сравнению с другими методами, так как обладает интересным свойством - коррекцией обесценивания оценок.

$$r_{xy} = \frac{\sum_{k=1}^{n}(x_k-\bar{x})(y_k-\bar{y})}{\sqrt{\sum_{k=1}^{n}(x_k-\bar{x})^2 \sum_{k=1}^{n}(y_k-\bar{y})^2}} \quad (1)$$

После кластеризации пользователей производится прогнозирование выставляемой пользователем оценки к научной работе. Для m пользователей имеется n научных работ. Обозначим пользователей через u и v, а научные работы через i. Оценка r_{ui} означает, что пользователь u выставил научной работе i оценку. Прогнозируемая оценка будет обозначаться $\overline{r_{ui}}$. Выставленные оценки будут храниться в множестве $K = \{(u, i \mid r - \text{известная оценка})\}$.

Чтобы инкапсулировать эффекты, которые не связаны с взаимодействием пользователя и научной работы, вводятся базовые предикаты. Базовые предикаты являются числом, сопоставимым с пользователем или объектом.

Обозначим через μ среднюю оценку. Базовый предикат известной оценки r_{ui} обозначим b_{ui}.

$$b_{ui} = \mu + b_u + b_i \quad (2)$$

Параметры b_u и b_i указывают наблюдаемые отклонения базовых предикат пользователя и научной работы от их среднего значения.

Для того, чтобы оценить базовые предикаты пользователей и научных работ, используют метод наименьших квадратов (3):

$$\min \sum_{(u,i)\in K}(r_{ui} - \mu - b_u - b_i)^2 + \lambda_1(\sum_u b_u^2 + \sum_i b_u^2) \quad (3)$$

где выражение $\sum_{(u,i)\in K}(r_{ui} - \mu - b_u - b_i)^2$ стремится найти b_u и b_i, которые соответствуют данным оценкам. Регулирующее выражение $\lambda_1(\sum_u b_u^2 + \sum_i b_u^2)$ избегает переобучения, штрафуя величины параметров, где $\lambda_1 = 0{,}02$ является параметром регулирования.

Вычислим параметры через расчёт пользовательских предикатов из предикатов научных работ (4):

$$b_i = \frac{\sum_{u\epsilon R(i)}(r_{ui}-\mu)}{\lambda_2+|R(i)|}; \qquad b_u = \frac{\sum_{u\epsilon R(i)}(r_{ui}-\mu-b_i)}{\lambda_3+|R(u)|} \quad (4)$$

где $\lambda_2 = 10$ и $\lambda_3 = 25$ являются параметрами регулирования.

Достижение функцией минимума возможно при использовании метода градиентного спуска. Для каждой выставляемой оценки r_{ui} вычисляется предикат $\overline{r_{ui}}$ и ассоциируется с ошибкой $e_{ui} = r_{ui} - \overline{r_{ui}}$. Для каждой оценки r_{ui} изменяются параметры, двигаясь в сторону, противоположную направлению градиента (5):

$$b_u = b_u + \gamma(e_{ui} - \lambda_1 b_u); \qquad b_i = b_i + \gamma(e_{ui} - \lambda_1 b_i) \quad (5)$$

где γ - коэффициент обучаемости.

Прогнозируемую оценку r_{ui} рассчитаем по формуле (6):

$$\overline{r_{ui}} = \mu + b_u + b_i \quad (6)$$

Зная множество прогнозируемых оценок пользователя к научным работам, можно рекомендовать ему научные работы с наивысшими оценками [1].

Рекомендательная система научных работ показана на рис. 1.

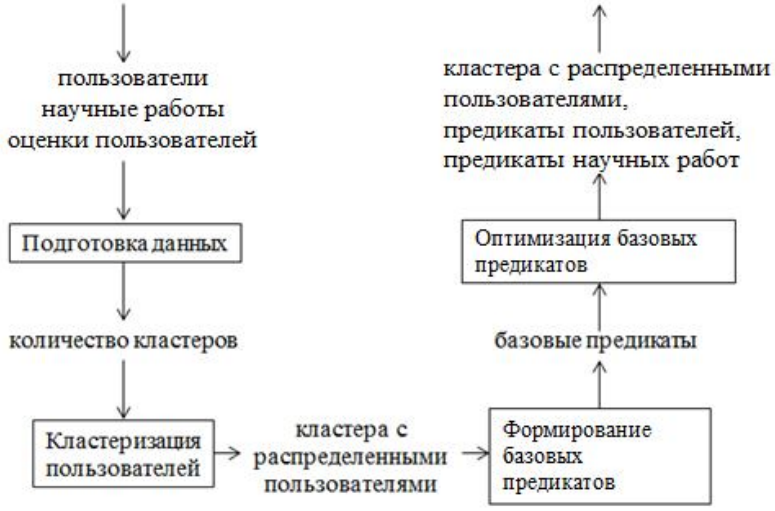


Рис. 1. Схема рекомендательной системы научных работ

Развитие рекомендательных систем играет важную роль в современном мире. Работа с большими объемами данных и выделение интересующих объектов является актуальной задачей. Рекомендация пользователю научных работ сокращает время поиска интересующей его информации. Оценки пользователями позволят выделить среди научных работ наиболее востребованные. Это позволит пользователю решать свои научные задачи, ориентируясь на качественную литературу. Классификация научных трудов по предпочтениям пользователей позволяет выделить группы научных трудов. Такое ориентирование позволит определить научные статьи по темам научных исследований. Такой метод решит проблему классификации по ключевым словам, так как в научных трудах разных тематик могут встречаться одинаковые слова. Прогнозирование научных трудов для пользователя позволит выделить более специализированный материал из множества работ рекомендованной темы научных трудов. Таким образом, рекомендательная система научных трудов является системой поиска интересующей пользователя информации, основываясь на его предпочтениях. Такая система может быть встроена в существующие системы поиска научных трудов в виде дополнительного модуля.

Литература:

1. Ricci F., Rokach L., Shapira B. Kantor PB.: Recommender System Handbook 2011 - 842p.

2. Сегаран Т.: Программируем коллективный разум - Пер. с англ. - Спб: Символ-Плюс, 2008. - 368 с.

3. Рекомендательная система - Википедия [Электронный ресурс] - Текстовые данные. Режим доступа: https://ru.wikpedia.org/wiki/Netflix-Prize

Макаревич О.Б., Басан Е.С., Степенкин А.А.
Институт компьютерных технологий и информационной безопасности
Инженерно-технологическая академия г. Таганрог

РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ ГРУППОВОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ РОБОТАМИ

Введение

Робототехника – это активно развиваемая технология, а группы мобильных роботов имеют огромный потенциал при выполнении различных задач. Для эффективного распределения и выполнения поставленных задач необходимо подготовить соответствующую систему группового управления. Системы группового управления могут применяться в неконтролируемой среде, где возможно оказание внешнего воздействия. Из чего следует проблема определения защищенности системы группового управления роботами (СГУР) от внешнего воздействия. Целью работы является разработка методики оценки защищенности системы. Для этого решаются задачи: анализ беспроводного канала и возможных атак на него, экспериментальное исследование этих атак, разработка методики на основе результатов.

Наиболее доступный беспроводной канал связи - WiFi сеть. Эта сеть реализуется с помощью протоколов 802.11. Стандарт 802.11 включает режимы работы: Basic Service Set (BSS), Extended Service Set (ESS) и Independent Basic Service Set (IBSS). Режимы BSS и ESS предполагают наличие точек доступа, к которым подключаются клиенты сети. В режиме ESS в одной сети может присутствовать несколько точек доступа, между которыми клиенты могут перемещаться. Режим IBSS – это Ad-Hoc сеть, в котором каждый клиент может быть связан напрямую с каждым клиентом. В данной работе будут рассматриваться режимы BSS и IBSS. Устройство экспериментальных стендов, использующих эти режимы описано в разделе 1. Безопасность этих сетей оценивалась по методике, представленной в разделе 2. Эта методика разработана на основе [1-4].

1 Описание экспериментального стенда

Для разработки стенда использовались мобильные роботы на основе следующих аппаратных платформ: Raspberry Pi 3 Model B 1GB RAM с ОС Raspbian, с ядром версии 4.9 и Arduino Uno + ESP8266 WiFi. В качестве точки доступа использовался TP Link tl-wa801nd. Стенд был сконфигурирован и протестирован в режиме BSS (рисунок 1 a), а затем в режиме IBSS (рисунок 1 b).

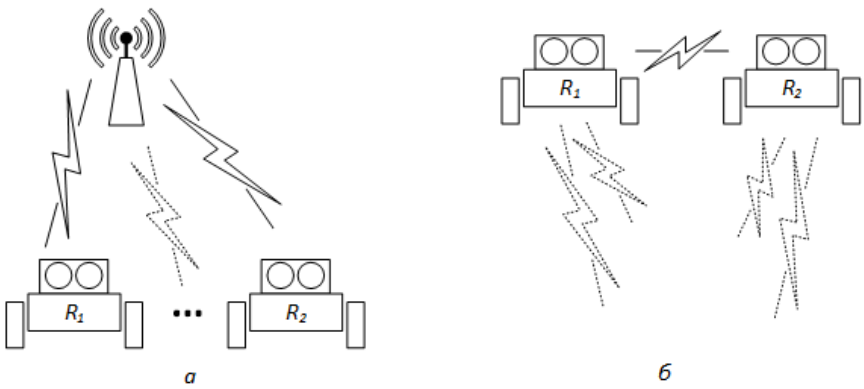


Рис. 1. Схема стенда

В режиме BSS сеть имеет топологию звезда. Каждый клиент для взаимодействия с остальными участниками сети отправляет фреймы точке доступа. В зависимости от физического расположения узлов и условий эксплуатации, сеть в режиме Ad-Hoc имеет

полносвязную или ячеистую топологию. Для обеспечения безопасности в данной работе рассматривались протоколы WEP/WPA/WPA2.

2 Оценка безопасности сети

Система группового управления роботами (СГУР) применяемая в неконтролируемой зоне может подвергаться внешнему воздействию со стороны внешнего нарушителя. Далее будут представлены атаки, доступные внешнему нарушителю. На основе возможных действий подготовлена методика для оценки подверженности системы таким атакам.

Для разработки данной методики было выбрано несколько специализированных утилит. При разработке данной методики использовался дистрибутив Linux: Kali Linux, включающий в себя программное обеспечение для тестирования на проникновение. Для реализации предложенной методики могут использоваться аналогичные утилиты, способные выполнять необходимые функции. Для реализации методики также требуется подходящее аппаратное обеспечение: сетевой адаптер, поддерживающий работу в режиме монитора и внедрение фреймов.

2.1 Пассивные атаки

Пассивные атаки реализуют угрозы обнаружения сети мобильных роботов, пассивного прослушивания и неавторизованного доступа к сети. Для перехвата сетевого трафика необходимо перевести сетевой адаптер в режиме монитора. Далее необходимо определить канал, на котором работает целевая сеть. После определения канала, используемого исследуемой системой, адаптер в режиме монитора должен быть переключен на фиксированный канал. Результаты прослушивания канала не зависят от используемого режима сети (BSS или IBSS). В стандарте 802.11 заголовок канального уровня передается в открытом виде, что позволяет получить информацию о MAC адресах используемых устройств. Из полученных MAC-адресов можно составить полный список используемых устройств. Анализируя поля Receiver, Transmitter, Destination и состояния флагов можно определить маршруты трафика в сети. На основе полученной информации можно сделать предположения о роли узлов в сети: глава кластера, исполнительный робот, принадлежащий определенному кластеру, центральное устройство, связывающее группу с внешней сетью.

Для режима BSS:

Для получения информации обо всех устройствах необходимо, чтобы анализируемая точка доступа находилась в зоне приема адаптера нарушителя. Иначе можно получить информацию только о доступных устройствах.

Для режима IBSS:

Если сеть распределена на большой территории, то не все узлы могут быть в зоне приема адаптера злоумышленника.

Полезная нагрузка каждого фрейма может передаваться в зашифрованном виде, в зависимости от используемого режима безопасности. Собранный зашифрованный трафик может быть сохранен для дальнейшего анализа. В результате анализа перехваченного трафика может быть нарушена конфиденциальность передаваемой информации.

2.2 Анализ перехваченного трафика

В протоколе 802.11 заголовок канального уровня передается в открытом виде. Структура фрейма заголовка представлена на рисунке 2. Поле Frame Control содержит тип и подтип фрейма, а также флаги использования протокола защиты, направления фрейма, переотправки фрейма. В зависимости от подтипа фрейма в заголовке присутствует от 1 до 4 полей адреса. Из этих заголовков можно получить следующую информацию:

- SSID сети передается в beacom фреймах. При использовании скрытой точки доступа, во фреймах ассоциации узла с сетью указывается SSID сети.

- На основе MAC-адресов передаваемого трафика можно проанализировать основные маршруты трафика.

- На основе этих маршрутов может быть сделано предположение о кластерах роботов и их иерархии в сети.

Рис. 2. Структура фрейма протокола 802.11.

2.3 Внешние активные атаки

Для тестирования сети необходим сетевой адаптер, поддерживающий внедрение пакетов – отправку в сеть поддельных фреймов, сформированных вручную.

Для режима BSS:

Сеть может быть подвержена DOS атаке. В данном режиме возможно применение нескольких способов атаки.

Deauth-фреймы.

На основе MAC-адресов, полученных на предыдущем шаге, формируется и отправляется управляющий фрейм деаутентификации с поддельным MAC-адресом точки доступа для конкретного клиента, что приведет к его отключению от сети. Данная атака может повторяться для списка узлов и быть распределенной во времени. В результате сеть блокируется частично.

Зашумление канала.

Непрерывная отправка широковещательных фреймов может значительно снизить пропускную способность используемого канала.

CTS/RTS флуд.

Для этого вида DOS необходимо непрерывно формировать и отправлять CTS-фреймы. В качестве источника и получателя могут использоваться сгенерированные MAC-адреса. В зависимости от интенсивности атаки в радиусе работы передатчика злоумышленника быстродействие сети может быть снижено или ее работа может быть полностью заблокирована.

Ложная аутентификация.

Вывод точки доступа из строя полностью нарушит работу всей сети. Для атаки точки доступа необходимо генерировать большое количество фреймов-аутентификации к точке доступа. В зависимости от используемого программного обеспечения на точке доступа, может произойти переполнение буфера очереди подключений, перезагрузка точки доступа или прекращение обработки новых подключений. Если точка доступа продолжает работу с уже имеющимися клиентами, то может быть проведена атака deauth-фреймами.

Для режима IBSS:

Отсутствие точки доступа исключает связанные с ней угрозы. Для этого режима применимы способы зашумления канала и CTS/RTS флуд. Отсутствие точки доступа может позволить сохранить частичную работоспособность сети.

Внешние воздействия на сеть могут оказывать влияние на доступность.

2.4 Получение доступа к сети

Метод получения доступа к сети зависит от используемого протокола безопасности.

При использовании протокола WEP необходимо собрать достаточное количество фреймов, содержащих Initial Vector. Далее для получения ключа могут использоваться такие утилиты как Aircrack, WEPcrack, либо атаки по словарям. При использовании протокола WPA необходимо перехватить рукопожатие, происходящее при подключении клиента к точке доступа. Для подбора ключа могут использоваться такие утилиты как Aircrack, CoWPAtty, Pyrit.

В случае успешного получения ключа весь, трафик, переданный с помощью WEP и тех сессий WPA, для которых перехвачено рукопожатие, может быть расшифрован. Следовательно, оказывается воздействие на конфиденциальность.

2.5 Внутренние атаки

После успешного получения ключа становится возможным подключение к сети и внедрение фреймов с полезной нагрузкой. На этом этапе действия в меньшей степени зависят от используемого режима работы сети.

Сбор информации об устройстве сети.

Для получения дополнительной информации могут об адресах работающих узлов могут применяться сканеры сетей, например nmap. Также сканирование может дать информацию об используемых ОС, открытых портов и запущенных сервисов. На основе этой информации могут быть применены сканеры уязвимостей, такие как Nessus. Возможные нарушения свойств безопасности зависят от найденных уязвимостей.

К примеру, при наличии открытого TCP-порта можно произвести SYN-флуд, что может привести к нарушению доступности. Наличие запущенных служб удаленного доступа, таких как SSH, Telnet, RDP и др. может вызвать нарушение конфиденциальности, целостности и доступности. Время работы сети мобильных роботов ограничено зарядом батарей. При наличии уязвимостей, обеспечивающих исполнение произвольного кода, может быть проведена атака на исчерпание ресурсов.

Внедрение команд

При определении используемых в сети протоколов прикладного уровня, для оказания воздействия на сеть могут внедряться поддельные команды. В случае применения неизвестного протокола может быть оценена реакция системы на атаку повтором и посылкой некорректных команд.

В результате этого шага возможно нарушение целостности

Атака Man in the middle (MITM) — продолжительная во времени атак, требующая подготовки. Для проведения атаки необходимо перенаправить трафик на контролируемый узел. Способ перенаправления трафика зависит от конфигурации сети. Может применяться ARP-spoofing, DNS-poisoning. После получения доступа к трафику, он может собираться, изменяться, сбрасываться. Что приводит к нарушениям конфиденциальности, целостности и доступности.

2.6 Методика оценки сети на основе протокола 802.11

Подготовка стенда

Для BSS режима: настройка точки доступа, выбор SSID, режима безопасности и ключа, подключение узлов к точке доступа.

Для IBSS режима: Подключение мобильных роботов к точке доступа.

Запуск роботов и их программного обеспечения.

Запуск сниффера Wireshark на тестируемых устройствах для проверки результатов выполнения методики.

Отметить с помощью Wireshark нормальное движение трафика.

Запустить непрерывный ping между тестируемыми узлами для отслеживания состояния канала.

Проведение пассивного перехвата. Цель: неавторизованный сбор сетевого трафика.

Перевод адаптера внешнего узла в режим монитора с помощью airmon-ng.

Сканирование работающих сетей для определения используемого канала с помощью airodump-ng.

Переключение адаптера на канал тестируемой сети.

Сбор трафика в файл с помощью airodump-ng.

Полученный файл содержит фреймы, переданные тестируемыми устройствами.

Для BSS режима: определение MAC-адреса точки доступа.

Составление списка MAC-адресов узлов.

Анализ открытых заголовков 802.11 для определения маршрутов движения трафика.

Для режима BSS: проведение DoS атаки на клиента. Цель: тестирование возможности нарушения доступа к узлу внешним нарушителем.

Отправка широковещательного фрейма деаутентификации с помощью airreplay-ng

Отправка фрейма деаутентификации на MAC-адрес узла в сети.

Цикличная отправка фреймов деаутентификации на каждый MAC-адрес из списка узлов.

В случае успешного выполнения тестируемые узлы теряют связь с сетью, что определяется по прекращению получения ping-запросов.

Для BSS режима: проведение DoS атаки на точку доступа. Цель: тестирование возможности нарушения доступа к сети внешним нарушителем.

С помощью mdk3 начать генерацию фреймов аутентификации с точкой доступа.

Если подключенные ранее клиенты продолжают работу — повторить отправку фреймов деаутентификации.

В случае успешного выполнения тестируемые узлы теряют связь с сетью, что определяется по прекращению получения ping-запросов.

Проведение DoS атаки на канал. Цель: тестирование возможности нарушения доступа к сети внешним нарушителем.

С помощью Metasploit Framework и модуля CTS_RTS_flood начать отправку CTS фреймов.

В результате флуда CTS фреймов время получения ping ответа должно возрасти или остановиться, в зависимости от интенсивности.

Получение ключа для доступа к сети. Цель: оценивание стойкости используемого протокола безопасности.

Для WEP: полученный с помощью airodump-ng файл с трафиком передать утилите aircrack-ng. Если не удалось получить ключ, необходимо собрать больше фреймов.

Для WPA: для подбора ключа необходимо перехватить процесс рукопожатия при подключении клиента. Если в собранном файле нет рукопожатия, то его можно спровоцировать повторением атаки деаутентификации. Успешность и время подбора ключа зависят от используемого словаря.

При получении ключа можно произвести подключение к сети.

Сканирование сети. Цель: определение доступной изнутри информации о системе.

Провести сканирование работающих IP-адресов с помощью nmap.

Провести сканирование открытых портов и работающих служб с помощью nmap.

Провести сканирование используемых ОС с помощью nmap.

Провести сканирование на наличие уязвимостей с помощью Nessus.

Сформировать список доступных узлов и уязвимостей на них на основе полученных результатах.

Воздействие на транспортный и прикладной уровни. Цель: тестирование обеспечения целостности в системе.

С помощью Ettercap произвести ARP-спуфинг между тестируемыми устройствами.

С помощью Ettercap добавить правило фильтрации передаваемых пакетов.

С помощью Ettercap добавить правило изменения передаваемых пакетов.

Внедрение пакетов протокола СГУР, созданных с помощью Scapy.

В трафике, собранном Wireshark на тестируемых узлах, должны присутствовать измененные пакеты. Оценить влияние измененных пакетов на работу системы.

3 Оценка защищенности СГУР

Основные задачи, решаемые системами группового управления роботами – распределение задач между узлами сети и планирование перемещения узлов к своим целям. Схема СГУР представлена на рисунке 3 а. G – цели, поставленные перед группой, C_r –информация, полученная от других узлов, $СУ_i$ – система управления роботом R_i, E – среда, в которой выполняются задачи. На рисунке 3, б η — множество связей данного робота с другими роботами группы; x_d — вектор координат следующей точки траектории перемещения робота; x_g — координаты выбранной цели [5]. Стратегический и тактический уровни СГУР Представлены на рисунке 4.

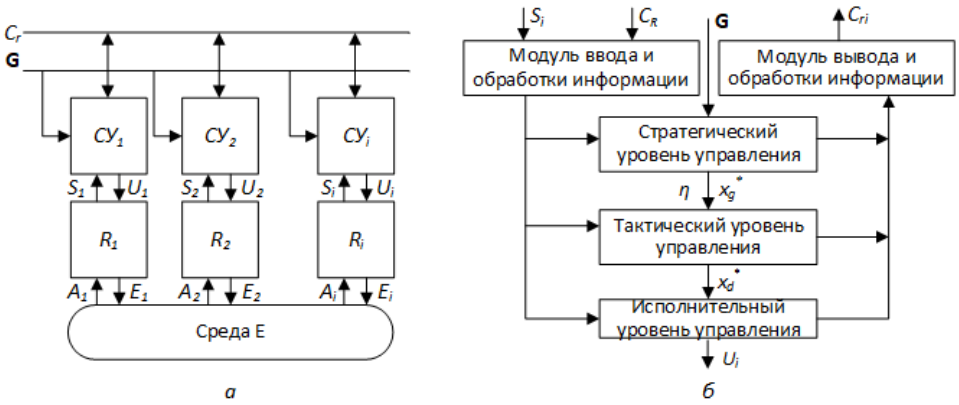


Рис. 3. Схема СГУР

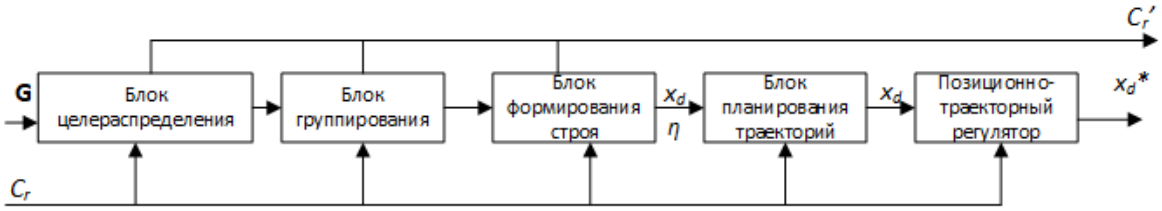


Рис. 4. Стратегический и тактический уровни

Блок целераспределения отвечает за назначение задач каждому узлу. Узлы, получившие общую задачу, объединяются в один кластер. Вне зависимости от используемого алгоритма целераспределения, блок целераспределения полагается на информацию, полученную от других узлов C_r [6]. Проведение DOS атаки любого типа на этом этапе может привести к тому, что атакованные узлы не примут участия в процессе целераспределения. Тогда цели могут быть распределены неэффективно, либо активных узлов не хватит для выполнения целей. С помощью атаки MITM можно произвести подмену данных для целераспределения, за счет чего злоумышленник может воздействовать на результат кластеризации. В результате группы будут сформированы неэффективно, из-

за чего выполнение задач потребует большие затраты временных и энергетических ресурсов, или будет невозможно.

Блок группирования отвечает за установления связи внутри кластера. Проведения DOS атаки любого типа на этом этапе может привести к выводу атакованных узлов из кластера. Недостаток узлов усложнит или нарушит выполнение цели этого кластера, в результате чего роботы потратят больше времени и энергии на выполнение задачи, либо не выполнят ее. MITM атака на этом этапе приведет к нарушению в работе следующих этапов.

Блок формирования строя и блок планирования траектории определяют положение узлов в пространстве и относительно других узлов в определенные моменты времени [7]. В результате проведения DOS атаки любого типа узел может не получить своевременно информации о своем следующем положении или об изменении выбранной ранее траектории движения. В результате чего строй может быть нарушен. В случае проведения атаки, связанной с внедрением команд, траектории некоторых узлов могут быть изменены нарушителем. В результате изменения траектории может быть нарушено решение поставленной задачи, вызвано столкновение с другими узлами, либо узел может быть перемещен в область, где он может быть перехвачен. В случае успешного перехвата, узел может подвергнуться подробному анализу и несанкционированной модификации. Модифицированный узел может быть возвращен в состав кластера. Аналогичный результат может быть достигнут в результате проведения атаки MITM.

Блок позиционно-траекторного регулирования осуществляет взаимодействие системы управления робота с механизмами исполнения. Соответственно, данный блок может быть подвержен локальному воздействию в случае, если в результате сканирования узла была найдена уязвимость, обеспечивающая удаленный доступ к ОС робота. В результате проведения такой атаки система управления может быть скомпрометирована или остановлена. Нарушитель может получить возможность передавать команды непосредственно исполнительным устройствам, в результате чего получить ручное управление над узлом. Наличие доступа к ОС также может обеспечить проведение атаки на исчерпание ресурсов. По причине повышенного потребления энергии время автономной работы узла сократиться. В результате узел может отключиться прежде, чем закончит выполнение своей задачи.

Заключение

Системы группового управления – это относительно новая область исследования. При широком применении подобных систем возникнет проблема угроз при применении в неконтролируемых зонах. Поэтому важно иметь методику для оценки безопасности сети. В этой работе предложена такая методика. Она позволяет проверить защищенность системы СГУР от атак по беспроводным каналам связи внешнего нарушителя. Основные проблемы безопасности СГУР связаны с возможностью перехвата трафика, проведения DoS атак и внедрения команд. Для решения этих проблем могут быть применены более стойкие ключи безопасности, дополнительные средства шифрования, применение VPN между узлами, системы на основе доверия между узлами [8, 9], системы обнаружения вторжений [10], а также дополнительные средства аутентификации устройств и сообщений.

Работа выполнена при поддержке Гранта РФФИ 17-07-00106 Разработка метода и эффективной системы защиты беспроводных сенсорных сетей от активных атак злоумышленников.

Литература:

1. Nwabude A. S. Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures. Blekinge Institute of Technology, Department of Telecommunications. Blekinge. 2008

2. Denis M., Zena C., Hayajneh T. Penetration testing: Concepts, attack methods, and defense strategies. Systems, Applications and Technology Conference (LISAT), 2016 IEEE Long Island

3. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. CCS'17, October 30-November 3, 2017, Dallas, TX, USA

4. Higgins F., Tomlinson A., Martin K. M. Survey on Security Challenges for Swarm Robotics. Autonomic and Autonomous Systems, 2009. ICAS '09

5. Pshikhopov V., Ali A.Hybrid motion control of a mobile robot in dynamic environments. Proc. of the IEEE Intern. Conf. on Mechatronics. 2011. 540–545.

6. Pshikhopov V. Kh., Medvedev M.Yu., Gaiduk A.R., Gurenko B.V. Control System Design for Autonomous Underwater Vehicle. Robotics Symposium and Competition (LARS/LARC). 2013

7. Pshikhopov V. Kh., Medvedev M. Y., Shevchenko V. A. Path planning for a group of vehicles in 2D obstructed environment. Control, Automation and Systems (ICCAS). 2016 16th International Conference on

8. Basan A., Basan E., Makarevich O. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2016

9. Basan A., Basan E., Makarevich O. A Trust Evaluation Method for Active Attack Counteraction in Wireless Sensor Networks. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017

10. Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. Information Forensics and Security (WIFS), 2015

Маро Е.А., Ковальчук М.М.
Южный федеральный университет

ОБХОД БИОМЕТРИЧЕСКОЙ СИСТЕМЫ БЛОКИРОВКИ МОБИЛЬНЫХ УСТРОЙСТВ

Атаки на биометрические системы аутентификации по отпечатку пальцев.

В общем виде процесс регистрации пользователя в биометрическом системе состоит из трех взаимосвязанных и выполняемых последовательно процедур: идентификации, аутентификации и авторизации. Мобильные телефоны и другие электронные устройства, оснащенные для аутентификации пользователя считывателями отпечатков пальцев, не так безопасны, как кажется на первый взгляд, что подтверждается проводимыми исследованиями [1-11]. Выделяют восемь уровней атак, направленных на системы биометрической аутентификации (рис. 1.)

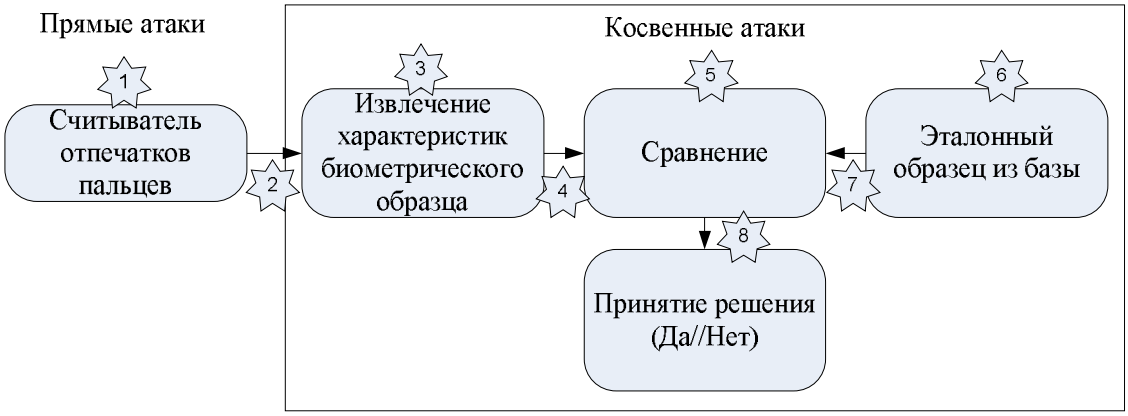


Рис. 1. Атаки на системы биометрической аутентификации на основе отпечатков пальцев.

Прямые атаки основаны на негласном сканировании отпечатков пальца владельца устройства, а затем формировании искусственного образца отпечатка пальца для обхода системы блокировки устройства. Прямые атаки могут быть осуществлены в виде атак подмены и преобразования. Атаки подмены заключаются в предъявлении копии отпечатка пальца (например, образец из силикона или другого материала). Атака преобразования основана на модификациях стандартных биометрических образцов с использованием облитерации, искажения, имитации или фальсификации. Косвенные атаки, основаны на изменении процесса обмена данными между системой аутентификации и программными/аппаратными модулями сканирующих устройств.

Существуют следующие направления атак на биометрические системы аутентификации на основе отпечатков пальцев:

получить доступ к базе данных отпечатков пальцев на устройствах (если база не зашифрована);

создать поддельный отпечаток пальца (3D-печать [5-8], печать с применением токопроводящей краски, латекса, клея, силикона или желатиновые копии отпечатков пальцев [4, 11] и т.д.);

перехват образцов отпечатков пальцев от считывателя отпечатков пальцев (атака «человек посередине», поиск уязвимостей в SDK или API, внедрение вредоносных программ, проведение атак на датчики сканера отпечатков пальцев [3, 9-11] и т.д.).

Для получения образцов отпечатков пальцев применяются специализированные сканеры. Выделяют три основных типа сканеров отпечатков пальцев: емкостные, прокатные, оптические.

Емкостные сканеры наиболее дешевы, однако не отличаются практичностью и долговечностью. Поскольку изображение отпечатка в подобных сканерах формируется за счет разницы электрических потенциалов различных участков кожи, эти сканеры чрезвычайно чувствительны к остаточному статическому электричеству. Часто выходят из строя после того, как их коснулся человек с наэлектризованной кожей, например, из-за ношения одежды из шерстяной или шелковой ткани. Кроме того, изображения отпечатков пальцев, формируемого емкостными сканерами, имеет низкое разрешение (качество).

Более эффективную технологию идентификации по отпечаткам пальцев реализуют на основе использования оптических сканеров. Данный тип сканера несколько дороже сканеров других типов, но в них устранены многочисленные недостатки, они долговечны, экономичны, удобны и просты в использовании. Изображение отпечатков пальцев в оптических сканерах характеризуется высоким качеством. Новейшие исследования доказали, что оптические сканеры отпечатков пальцев являются безопасными в антибактериальном отношении.

Прокатные сканеры занимают серединное положение по качеству получаемого образца отпечатка, в них изображение отпечатка формируется при «прокатывании» пальца по узкому окошку сканирующей области сканера, после чего целостное изображение отпечатка «сшивается» из отдельных кадров. От пользователя прокатных типов сканера требуется постоянно соблюдать единообразие в скорости и манере «прокатывания» пальца по считывателю, что бывает довольно сложно в реализации.

В рамках статьи были рассмотрены прямые атаки на биометрические системы блокировки устройств на основе создания желатиновой копии отпечатка пальца.

Методология создания искусственного отпечатка пальца.

В данном разделе статьи описывается метод создания искусственного отпечатка пальца для мобильных устройств, ноутбуков и USB-сканеров, а также использование полученного искусственного отпечатка пальца для разблокировки следующих устройств:

1. iPhone 6.
2. iPhone 8.
3. iPad Air 2.
4. Meizu m5s.
5. Samsung Galaxy S8.
6. COBO C2.
7. Schenker XMG A507.

Важная задача атаки состоит в том, чтобы получить приемлемый оригинальный отпечаток пальца владельца устройства. Для того, чтобы получить образец отпечатка владельца iPhone 6, следует снять защитное стекло так, чтобы не оставить свои отпечатки среди отпечатков владельца и не повредить их. Затем насыпать немного дактилоскопического порошка на поверхность защитного стекла с предполагаемым отпечатком пальца владельца. Как было показано в опытах, проведённых для получения отпечатков пальцев, слой дактилоскопического порошка должен быть небольшим: меньше 2-3 мм (рисунок 2).

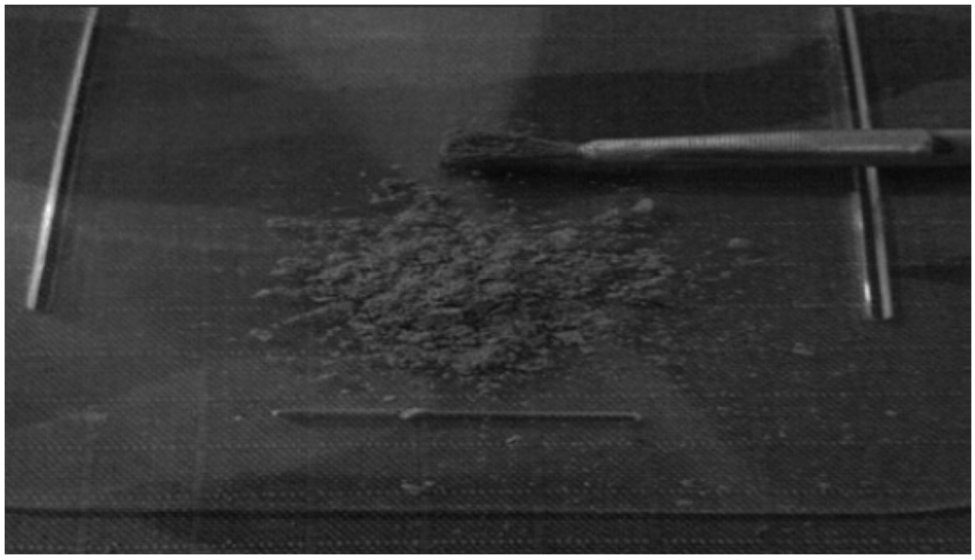


Рис. 2. Применение дактилоскопического порошка для получения отпечатка пальца

После того как был нанесен дактилоскопический порошок, следует аккуратно и медленно распределить его по поверхности защитного стекла. Произведя несколько движений мягкой кистью, мы сможем увидеть отпечатки серого цвета. Мелкодисперсный порошок прилипает к потожировым следам и создаёт видимое изображение отпечатка пальца. После разравнивания порошка мягкой кистью, мы получаем образец папиллярного узора (рис. 3).

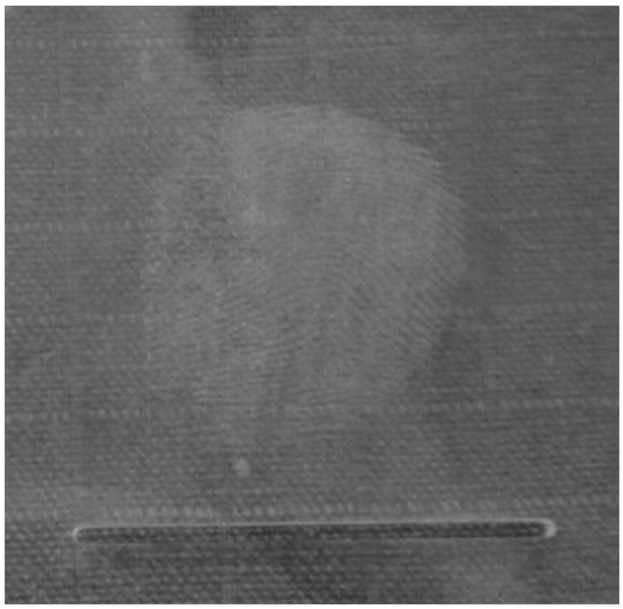


Рис. 3. Видимое изображение отпечатка пальца на поверхности защитного стекла.

Для того, чтобы работать с отпечатком пальца, необходимо перенести его на дактилоскопическую плёнку или обычный скотч. Следует наклеить пленку (скотч) без излишнего давления, чтобы не нарушить контуры папиллярного узора (рис. 4).

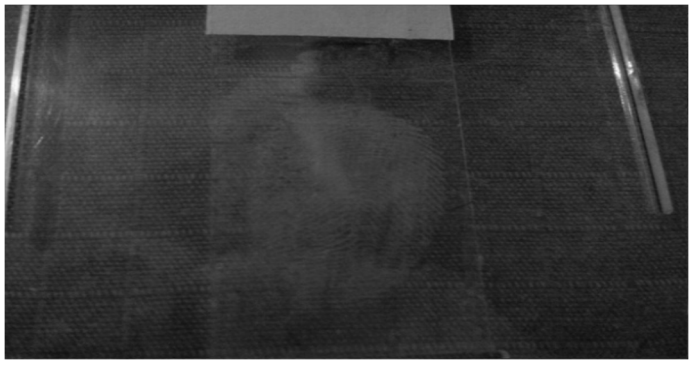


Рис. 4. Снятие отпечатка пальца с защитного стекла.

Снимая пленку не нужно удалять ее слишком быстро, чтобы не нарушить структуру клея. Если все линии четко видны на дактилоскопической плёнке (скотче), значит, снятие отпечатка пальца с высокой вероятностью было успешным. На рисунке 5 показан образец отпечатка пальца на скотче.

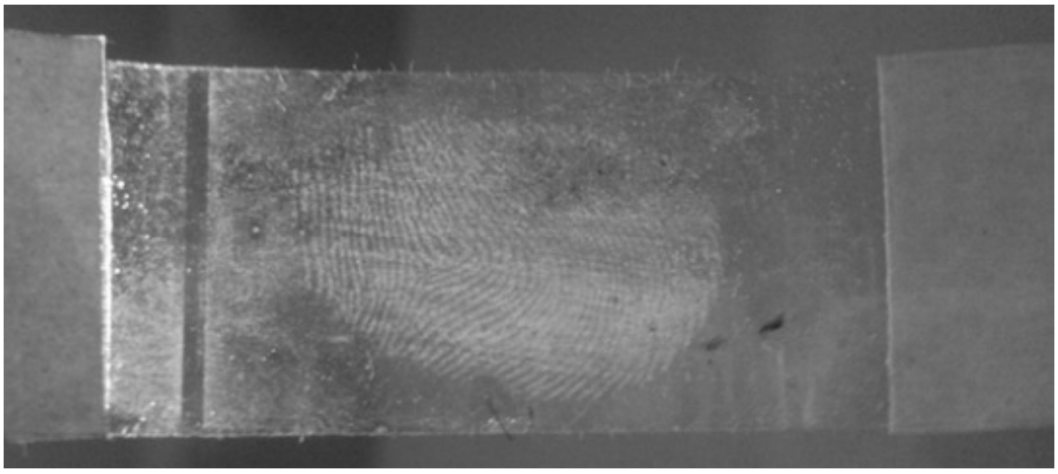


Рис. 5. Образец отпечатка на скотче

Как показал эксперимент, не требуется получение идеального образца отпечатка пальца, представленный на рисунке 5 образец подходит для дальнейшей работы по обходу блокировки телефона.

Следующим этапом является сканирование или фотографирование полученного отпечатка пальца с разрешением по крайней мере 2400 точек на дюйм. Затем с помощью графического редактора изображение поворачиваем вдоль вертикальной оси (т.к. отпечаток получается зеркальный), цвет инвертируем (отпечаток делаем белым, а фон чёрным), увеличиваем контрастность и резкость. Окончательно обработанное изображение отпечатка пальца показано на рисунке 6.

Третий этап применяемого метода заключается в создании объёмного отпечатка пальца. Существует несколько способов формирования выпуклой маски отпечатка пальца и применяемых составов заливки маски для получения искусственных отпечатков пальца. Нами был применен метод, который требует наименьшее количество времени и дополнительного оборудования для практической реализации. Нами были сделаны искусственные отпечатки пальцев с помощью маски на основе выпуклостей тонера лазерного принтера и заливки желатином.

Рис. 6. Итоговое изображение отпечатка пальца

В ходе экспериментов было установлено, что параметры принтера должны быть установлены на максимальное разрешение (1200 DPI и больше) печати и максимальный расход тонера. Затем мы залили желатин на печатное изображение (маску) и поместили его в холодильник для застывания в течение примерно 10 минут при температуре +4°C. После того, как желатин принял состояние и консистенцию резины, желатиновая форма была тщательно удален от маски (бумаги). Для получения окончательного отпечатка пальца, нами были отрезаны лишние края сделанной желатиновой формы. В результате были получены искусственные отпечатки пальцев, подходящие для разблокировки мобильного телефона и других устройств.

Результаты экспериментов.

В iPhone используется защита от перебора (подбора) отпечатков пальцев. После пяти неудачных попыток разблокировки сохранится только возможность разблокировки телефона с помощью пароля. В нашем исследовании важно предотвратить процесс смены метода блокировки на парольную, поэтому следует сразу правильно размещать искусственный отпечаток на сканере. В эксперименте удалось обойти блокировку iPhone 6 с искусственным отпечатком. Сканер отпечатков пальцев на iPhone 6 со второй попытки принял искусственные отпечатки пальцев за действительные и разблокировал

телефон. Затем был проведён эксперимент по разблокировке с iPhone 8. В этом случае потребовалось больше попыток, чтобы сканер распознал отпечаток за действительный, так как в iPhone 8 используется механический тип кнопки, а значит, важна также сила нажатия. На пятой попытке телефон iPhone 8 был разблокирован.

Разблокировка iPad Air 2 оказалась идентичной iPhone 6, так как сканеры отпечатков пальцев на iPad Air 2 и Iphone 6 одинаковые. Проблем с идентификацией при предъявлении искусственного отпечатка пальца не возникло, со второй попытки планшет был разблокирован.

Процесс разблокировки телефона Meizu m5s с помощью искусственного отпечатка оказался сложнее. Сканер отпечатка пальца Meizu m5s не воспринял предъявленный искусственный отпечаток пальца. Было сделано предположение о том, что сканер отпечатков пальцев не реагирует на сухой искусственный отпечаток пальца. Разблокировать телефон Meizu m5s удалось после того, как мы увлажнили искусственный отпечаток пальца, имитируя пот.

Эксперименты со сканером отпечатков пальцев на Samsung Galaxy S8 длились достаточно долго по сравнению с другими мобильными устройствами. Сухой и увлажнённый искусственный отпечаток пальца не воспринимался при разблокировке. Решение возникшей проблемы нашлось почти случайно, забыв про искусственный отпечаток на столе и вернувшись через небольшой промежуток времени (примерно 10 минут), нами была повторена попытка разблокировки телефона, которая оказалась успешной. Нами был сделан вывод, что искусственный отпечаток должен быть комнатной температуры. Однако нельзя сильно повышать температуру помещения, чтобы папиллярный узор на искусственном отпечатке не деформировался (растаял).

Разблокировка ноутбука с USB-сканером COBO C2 не вызвала существенных сложностей. С третьей попытки при правильном размещении искусственного отпечатка пальца на сканере считыватель одобрил вход в систему.

Таблица 1

Эксперименты по разблокировке устройств

Модель	Тип устройства	Тип сканера	Параметры отпечатка пальца	Количество попыток	Количество успешных попыток	Процент успешных попыток
iPhone 6	телефон	цельный	Исходный	20	14	70
Meizu m5s	телефон	цельный	Исходный	10	Не воспринимает как отпечаток пальца	-
			Увлажнённый	20	13	65
iPad Air 2	планшет	цельный	Исходный	20	12	60
iPhone 8	телефон	цельный	Исходный	30	14	47
Samsung Galaxy S8	телефон	цельный	Исходный	10	Не воспринимает как отпечаток пальца	-
			Увлажненный	10	Не воспринимает как отпечаток пальца	-
			Исходный, комнатной температуры	25	18	60
COBO C2	USB-сканер	цельный	Исходный	20	15	75
Schenker XMG A507	ноутбук	протяжный	Исходный	50	22	44

В последнюю очередь для эксперимента был выбран ноутбук Schenker XMG A507 со встроенным сканером отпечатков пальцев. В данном ноутбуке используется протяжный тип сканера. Потребовалось не прикладывать отпечаток пальца, а проводить отпечатком по сканеру. В данном случае была важна точная форма искусственного отпечатка пальца, потому что сканер сканировал всю область пальца. В этом эксперименте было потрачено много времени на вырезание подходящего по форме отпечатка пальца и тестирование соответствия его формы с реальным пальцем в базе ноутбука. Усилия оправдались, было потрачено 6 искусственных отпечатков пальцев до достижения успешного результата разблокировки ноутбука.

Результаты проведённых экспериментов обхода блокировки мобильных устройств, ноутбука и USB-сканера приведены в Таблице 1.

Применяемый метод не подходит для считывания отпечатков пальцев, в которых измеряется электропроводность кожи. Желатиновые отпечатки пальцев могут храниться в течение длительного времени, если условия хранения соблюдены (отпечаток пальца из желатина сохраняется только при низкой температуре). Иначе искусственные отпечатки пальцев станут непригодными для дальнейшего использования: желатин может начать таять и папиллярные узоры, которые сканируются с помощью сканера отпечатков пальцев, будут деформироваться.

Следует отметить, что способы блокировки на основе отпечатков пальцев могут быть рекомендованы для использования на смартфонах, ноутбуках и других устройствах, но при этом нужно учитывать, что отпечатки пальцев могут быть менее надёжны, чем применение длинного пароля или PIN-кода. Система аутентификации или блокировки будет более надежной при использовании отпечатков пальцев в качестве дополнительного фактора аутентификации. Например, для того, чтобы повысить безопасность системы биометрической аутентификации по отпечаткам пальцев рекомендуется:

Использовать несколько биометрических образцов (зарегистрировать несколько различных отпечатков пальцев и использовать их в случайном порядке);

Использование систем многофакторной аутентификации (например, отпечатки пальцев + пароль или отпечатки пальцев + SD-карта);

Использование мультимодальных биометрических данных (например, отпечатки пальцев + сканирование радужной оболочки глаза или отпечатки пальцев + распознавание лица)

Применять технологию обнаружения живого пальца. Датчики в режиме реального времени способны определить, являются ли биометрические характеристики, предоставленные в считыватель отпечатков пальцев, являются подлинными и не поддельными.

Предоставленные результаты являются началом исследований в области биометрической аутентификации по отпечаткам пальцев. Дальнейшим развитием темы исследования может служить расширение списка устройств, для которых будет проведено тестирование применения искусственного отпечатка пальца, а также исследование других способов создания искусственного отпечатка, например, с применением 3D-печати и печати с проводящими чернилами.

Литература:

1. White Paper “*Protecting Against Fingerprint Spoofing in Mobile Devices*”, Synaptics Incorporated, 2016.

2. Y. W. Ju B. H. Lee “*The implementation of secure mobile biometric system*”, International Journal of Bio-Science and Bio-Technology , vol. 5 no. 4 pp. 53-60 2013.

3. Sanaa Ghouzali, Maryam Lafkih, Wadood Abdul, Mounia Mikram, Mohammed El Haziti, and Driss Aboutajdine “*Trace Attack against Biometric Mobile Applications*”, Mobile Information Systems, vol. 2016.

4. Kai Cao and Anil K. Jain "*Hacking Mobile Phones Using 2D Printed Fingerprints*", MSU Technical Report MSU-CSE-16-2, 2016.

5. S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter "*Design and fabrication of 3d fingerprint targets*", IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2284–2297, Oct. 2016.

6. S. S. Arora, A. K. Jain, and N. G. Paulter "*3d whole hand targets: Evaluating slap and contactless fingerprint readers*", 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8, Sept 2016.

7. S. S. Arora, A. K. Jain, and N. G. Paulter "*Gold fingers: 3d targets for evaluating capacitive readers*", IEEE Transactions on Information Forensics and Security, pp. 1–1, Apr. 2017.

8. Joshua J. Engelsma, Sunpreet S. Arora, Anil K. Jain, Nicholas G. Paulter Jr. "*Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations*", IEEE Transactions on Information Forensics and Security, 2017.

9. Yulong Zhang, Zhaofeng Chen, Hui Xue, and Tao Wei "*Fingerprints On Mobile Devices: Abusing and Leaking*", Black Hat Conference, August 7, 2015.

10. Antonio Bianchi, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Simon Pak Ho Chung, Wenke Lee "*Broken Fingers:On the Usage of the Fingerprint API in Android*", Network and Distributed System Security Symposium (NDSS), February 19th, 2018.

11. Yulong Zhang, Tao Wei "*To Swipe or Not to Swipe: A Challenge for Your Fingers*", RSA conference, San Francisco, USA, 2015.

Михайленко Е.В., Уразгильдеев Б.Г.
Краснодарский университет МВД России

О РАЗРАБОТКЕ ПРОГРАММНЫХ МОДУЛЕЙ ДЛЯ ОБРАБОТКИ И ПЕРЕДАЧИ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ «РАСПИСАНИЕ»

Учебные заведения, планируют и осуществляют образовательную деятельность, используя в учебном процессе различные виды организационно-распорядительных документов [3, 7, 8]. Особое место среди таких документов занимают расписание занятий и журнал успеваемости [1, 5].

В целях повышения эффективности образовательной деятельности в Краснодарском университете МВД России уже на протяжении ряда лет заполнение расписания занятий, его верификация, выписка расписаний для кафедр и факультетов, расчет запланированной и выполненной аудиторной нагрузки преподавателями осуществляется в автоматическом режиме с использованием разработанной в университете автоматизированной системы «Расписание» [4].

В настоящее время в университете в связи с отказом от бумажного документооборота и переходом на электронный внедрен модуль «Журналы успеваемости» системы управления учебным процессом «Магеллан». Доступ к данной системе находится на сайте библиотеки университета. Использование системы «Магеллан» предоставляет профессорско-преподавательскому составу университета оперативно заполнять журнал успеваемости, сотрудникам учебного управления анализировать качество учебного процесса, а обучаемым и их родителями в удаленном доступе просматривать оценки, полученные на занятиях, зачетах и экзаменах [2].

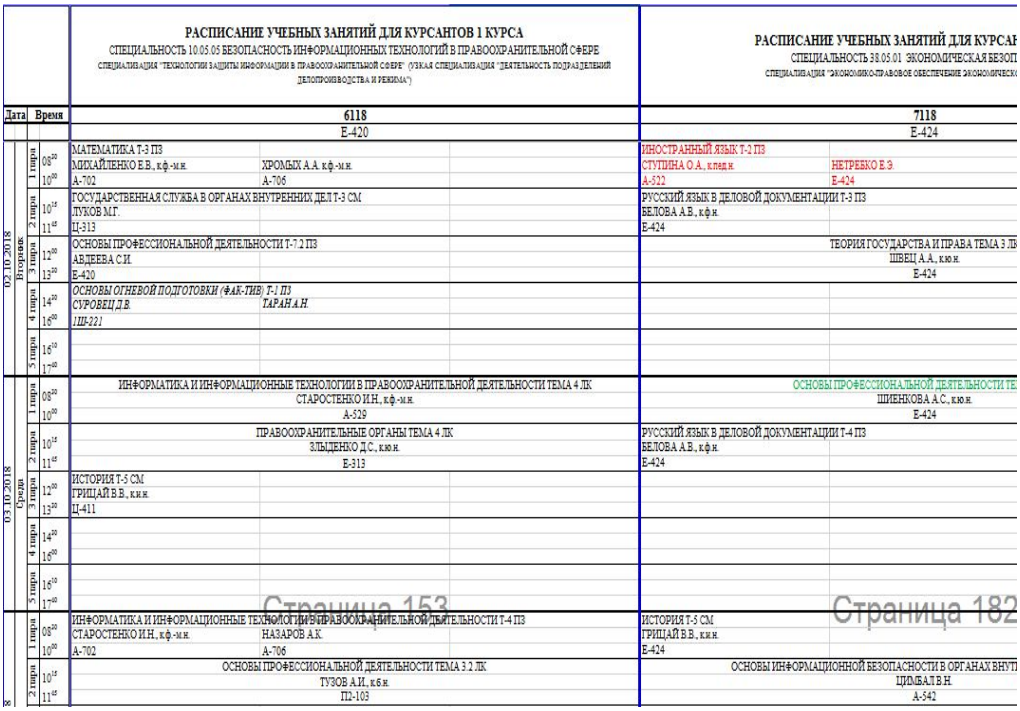
Однако переход на ведение электронного журнала в системе «Магеллан» сопряжен с дополнительными трудозатратами по введению преподавателями информации по каждому занятию. Вручную приходится вводить дату занятия, порядковый номер пары,

форму проведения, количество часов, тему занятия, фамилии ведущих преподавателей. При этом подобная процедура занимает немалое количество времени: преподаватель должен зайти на сайт электронного журнала, авторизоваться, выбрать нужную группу, внести требуемые данные. Часты случаи длительного ответа системы на действия пользователя из-за большого количества используемых в ней компонентов и плохого качества связи. Кроме того, на корректность введенных данных нередко сказывается человеческий фактор.

В рамках реализации эффективного электронного документооборота на кафедре информатики и математики принято решение об автоматизации процесса ввода вышеописанной информации с использованием данных из системы «Расписание». Выходные формы электронного расписания реализованы в формате MS Excel (рис. 1). Это позволило легко провести анализ необходимой информации по выбранной дисциплине для переноса ее в систему «Магеллан».

Для анализа способа взаимодействия с системой «Магеллан» использовались различные анализаторы трафика, в результате чего было выявлено, что при загрузке данных в систему используются ajax-запросы, а возвращаются ответы в JSON-формате [9, 10]. При отслеживании параметров HTTP-запросов, была исследована исходная структура экосистемы программного интерфейса (API) электронного журнала, вследствие чего стала возможна программная реализация методов переноса информации из электронного учебного расписания в модули электронного журнала системы «Магеллан» [6]. На рисунке 2 представлен фрагмент VBA программы взаимодействия с внутренней структурой электронного журнала.

Программа автоматического переноса данных в СУУП «Магеллан» реализована в качестве дополнительных модулей к электронному расписанию занятий. Она запускается с информационного листа с помощью помещенной на листы расписания кнопки «Магеллан». После нажатия пользователем кнопки «Магеллан» происходит автоматический запуск электронного журнала и на экране отображается окно входа в систему (рис. 3).



РАСПИСАНИЕ УЧЕБНЫХ ЗАНЯТИЙ ДЛЯ КУРСАНТОВ 1 КУРСА

СПЕЦИАЛЬНОСТЬ 10.05.05 БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

СПЕЦИАЛИЗАЦИЯ "ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ" (УЗКАЯ СПЕЦИАЛИЗАЦИЯ "ДЕЯТЕЛЬНОСТЬ ПОДРАЗДЕЛЕНИЙ ДЕЛОПРОИЗВОДСТВА И РЕЖИМА")

Дата	Время		6118 Е-420	7118 Е-424
02.10.2018 Вторник	1 пара	08⁰⁰–10⁰⁰	МАТЕМАТИКА Т-3 ПЗ МИХАЙЛЕНКО Е.В., к.ф.-м.н. А-702 / ХРОМЫХ А.А. к.ф.-м.н. А-706	ИНОСТРАННЫЙ ЯЗЫК Т-2 ПЗ СТУПИНА О.А., к.пед.н. А-522 / НЕТРЕБКО Е.Э. Е-424
	2 пара	10¹⁵–11⁴⁵	ГОСУДАРСТВЕННАЯ СЛУЖБА В ОРГАНАХ ВНУТРЕННИХ ДЕЛ Т-3 СМ ЛУКОВ М.Г. Ц-313	РУССКИЙ ЯЗЫК В ДЕЛОВОЙ ДОКУМЕНТАЦИИ Т-3 ПЗ БЕЛОВА А.В., к.ф.н. Е-424
	3 пара	12⁰⁰–13⁵⁰	ОСНОВЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ Т-7 2 ПЗ АВДЕЕВА С.И. Е-420	ТЕОРИЯ ГОСУДАРСТВА И ПРАВА ТЕМА 3 ЛК ШВЕЦ А.А., к.ю.н. Е-424
	4 пара	14⁰⁰–16⁰⁰	*ОСНОВЫ ОГНЕВОЙ ПОДГОТОВКИ (ФАК-ТИВ) Т-1 ПЗ* *СУРОВЕЦ Л.В. / ТАРАН А.Н.* *1Ш-221*	
	5 пара	16¹⁰–17⁰⁰		
03.10.2018 Среда	1 пара	08⁰⁰–10⁰⁰	ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ТЕМА 4 ЛК СТАРОСТЕНКО И.Н., к.ф.-м.н. А-529	ОСНОВЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ТЕ ШИЕНКОВА А.С., к.ю.н. Е-424
	2 пара	10¹⁵–11⁴⁵	ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ ТЕМА 4 ЛК ЗЛЫДЕНКО Д.С., к.ю.н. Е-313	РУССКИЙ ЯЗЫК В ДЕЛОВОЙ ДОКУМЕНТАЦИИ Т-4 ПЗ БЕЛОВА А.В., к.ф.н. Е-424
	3 пара	12⁰⁰–13⁵⁰	ИСТОРИЯ Т-5 СМ ГРИЦАЙ В.В., к.и.н. Ц-411	
	4 пара	14⁰⁰–16⁰⁰		
	5 пара	16¹⁰–17⁰⁰		
8	1 пара	08⁰⁰–10⁰⁰	ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ Т-4 ПЗ СТАРОСТЕНКО И.Н., к.ф.-м.н. А-702 / НАЗАРОВ А.К. А-706	ИСТОРИЯ Т-5 СМ ГРИЦАЙ В.В., к.и.н. Е-424
	2 пара	10¹⁵–11⁴⁵	ОСНОВЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ТЕМА 3 2 ЛК ТУЗОВ А.И., к.б.н. П2-103	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТ ЦИМБАЛ В.Н. А-542

Страница 153 Страница 182

Рис. 1. Фрагмент выходной формы учебного расписания.

```
Function teacher_insert(lid, tid, rid)
    params = "data={""LESSON_ID"":" & lid & ","TEACHER_ID"":" & tid & _
    ","ROLE_ID"":" & rid & ","ID"":null}"
    Set pp = j(p("http://libkrumvd.ru/magellan/modules/system/" + _
    "journal/lessonTeachers.php?operation=i&_dc=1518019993823", "POST", params)
    teacher_insert = pp.success
End Function
```

Рис. 2. Взаимодействие с API: функция добавления к занятию преподавателя.

Рис. 3. Окно ввода логина и пароля

По окончании авторизации в отдельном окне пользователю предлагается выбрать нужную группу и дисциплину, а также семестр, для которого следует заполнить или проверить журнал (рис. 4).

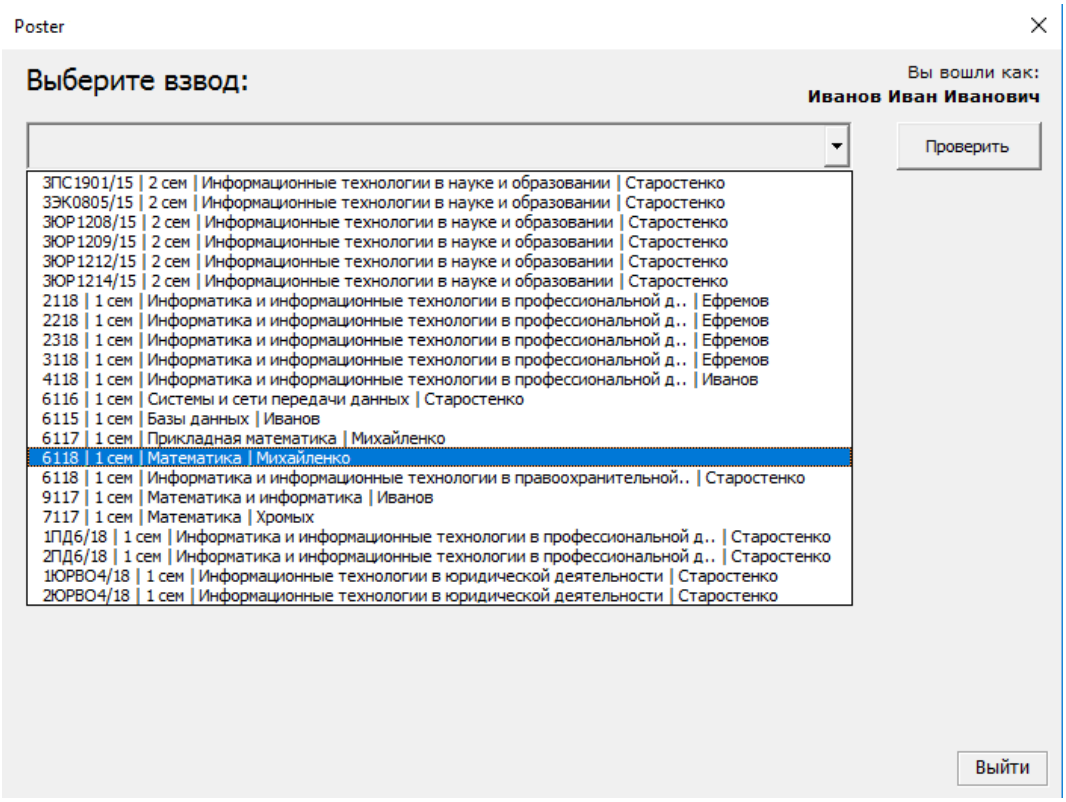
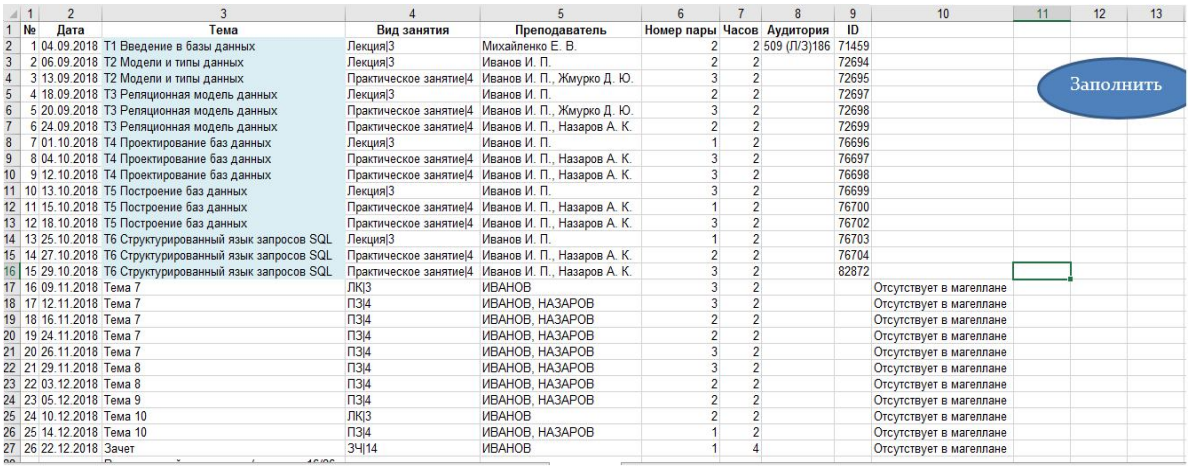


Рис. 4. Окно выбора журнала

В результате выбора программа на отдельном листе открытой рабочей книги «Расписание» в компактной форме выведет результат анализа двух одновременно обрабатываемых документов: расписания занятий и электронного журнала успеваемости за весь обрабатываемый семестр (рис. 5). Если электронный журнал еще не заполнен, то все данные будут взяты из расписания, наименования тем пользователь может скопировать на выводимый лист из тематических планов, а затем нажатием на кнопку «Заполнить» перенести все данные в электронное расписание. Если же электронный журнал уже заполнен преподавателем вручную, то происходит верификация внесенных в электронный журнал данных и в случае неверного заполнения журнала пользователю будет предложено автоматическая исправить ошибки.



№	Дата	Тема	Вид занятия	Преподаватель	Номер пары	Часов	Аудитория	ID	
1	04.09.2018	Т1 Введение в базы данных	Лекция|3	Михайленко Е. В.	2	2	509 (Л/З)186	71459	
2	06.09.2018	Т2 Модели и типы данных	Лекция|3	Иванов И. П.	2	2		72694	
3	13.09.2018	Т2 Модели и типы данных	Практическое занятие|4	Иванов И. П., Жмурко Д. Ю.	3	2		72695	
4	18.09.2018	Т3 Реляционная модель данных	Лекция|3	Иванов И. П.	2	2		72697	
5	20.09.2018	Т3 Реляционная модель данных	Практическое занятие|4	Иванов И. П., Жмурко Д. Ю.	3	2		72698	
6	24.09.2018	Т3 Реляционная модель данных	Практическое занятие|4	Иванов И. П., Назаров А. К.	2	2		72699	
7	01.10.2018	Т4 Проектирование баз данных	Лекция|3	Иванов И. П.	1	2		76696	
8	04.10.2018	Т4 Проектирование баз данных	Практическое занятие|4	Иванов И. П., Назаров А. К.	3	2		76697	
9	12.10.2018	Т4 Проектирование баз данных	Практическое занятие|4	Иванов И. П., Назаров А. К.	3	2		76698	
10	13.10.2018	Т5 Построение баз данных	Лекция|3	Иванов И. П.	3	2		76699	
11	15.10.2018	Т5 Построение баз данных	Практическое занятие|4	Иванов И. П., Назаров А. К.	1	2		76700	
12	18.10.2018	Т5 Построение баз данных	Практическое занятие|4	Иванов И. П., Назаров А. К.	3	2		76702	
13	25.10.2018	Т6 Структурированный язык запросов SQL	Лекция|3	Иванов И. П.	1	2		76703	
14	27.10.2018	Т6 Структурированный язык запросов SQL	Практическое занятие|4	Иванов И. П., Назаров А. К.	2	2		76704	
15	29.10.2018	Т6 Структурированный язык запросов SQL	Практическое занятие|4	Иванов И. П., Назаров А. К.	3	2		82872	
16	09.11.2018	Тема 7	ЛК|3	ИВАНОВ	3	2			Отсутствует в магеллане
17	12.11.2018	Тема 7	ПЗ|4	ИВАНОВ, НАЗАРОВ	3	2			Отсутствует в магеллане
18	16.11.2018	Тема 7	ПЗ|4	ИВАНОВ, НАЗАРОВ	2	2			Отсутствует в магеллане
19	24.11.2018	Тема 7	ПЗ|4	ИВАНОВ, НАЗАРОВ	2	2			Отсутствует в магеллане
20	26.11.2018	Тема 7	ПЗ|4	ИВАНОВ, НАЗАРОВ	3	2			Отсутствует в магеллане
21	29.11.2018	Тема 8	ПЗ|4	ИВАНОВ, НАЗАРОВ	3	2			Отсутствует в магеллане
22	03.12.2018	Тема 8	ПЗ|4	ИВАНОВ, НАЗАРОВ	2	2			Отсутствует в магеллане
23	05.12.2018	Тема 9	ПЗ|4	ИВАНОВ, НАЗАРОВ	2	2			Отсутствует в магеллане
24	10.12.2018	Тема 10	ЛК|3	ИВАНОВ	2	2			Отсутствует в магеллане
25	14.12.2018	Тема 10	ПЗ|4	ИВАНОВ, НАЗАРОВ	1	2			Отсутствует в магеллане
26	22.12.2018	Зачет	ЗЧ|14	ИВАНОВ	1	4			Отсутствует в магеллане

Рис. 5. Результат анализа журналов

Разработанный модуль прошел апробацию на кафедре информатики и математики при проверке и заполнении журналов по изучаемым на кафедре дисциплинам. Внедрение данного модуля в образовательную деятельность университета позволит значительно сократить время на заполнение электронного журнала и займет достойное место на пути эффективного развития автоматизации учебного процесса.

Литература:

1. Лаптев, В.Н. Некоторые аспекты применения среды Visual Basic for Application для создания учебных приложений по математическим дисциплинам / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №09(103). – С. 222 – 233. – IDA [article ID]: 1031409014. – Режим доступа: http://ej.kubagro.ru/2014/09/pdf/14.pdf, 0,75 у.п.л.

2. Лаптев, В.Н. Организация тестирования в автоматизированной контролирующей системе «Контроль» / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2016. – №10(124). – С. 461 – 471. – IDA [article ID]: 1241610026. – Режим доступа: http://ej.kubagro.ru/2016/10/pdf/26.pdf, 0,688 у.п.л.

3. Михайленко, Е.В. О создании Автоматизированной системы «Мониторинг» / Е.В. Михайленко // Математические методы и информационно-технические средства: Труды V Всерос. Науч.-практ. конф., 19 июня 2009 г. / редкол.: Ф.Г. Хисамов, Е.В. Михайленко, И.Н. Старостенко. – Краснодар: Краснодар. ун-т МВД России, 2009. – С. 99 – 101.

4. Михайленко, Е.В. Об автоматизации подготовки расписания учебных занятий / Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XII Всерос. науч.-практ. конф. 17 июня 2016 г. / редкол.: И.Н. Старостенко,

Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодарский университет МВД России, 2016. – С. 175 – 179.

5. Михайленко, Е.В. Организация ветвления и циклов: лекция / Е.В. Михайленко. – Краснодар: Краснодарский университет МВД России, 2015. – 44 с.

6. Михайленко, Е.В. Автоматизация подготовки заданий и проверки выполненных работ по математическим и естественнонаучным дисциплинам / Е.В. Михайленко // Проблемы информационного обеспечения деятельности правоохранительных органов: материалы международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России, 2015. – С.107 – 114.

7. Михайленко, Е.В. Особенности разработки в VBA программных приложений для генерирования практических заданий и анализа их выполнения / Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XI Всерос. науч.-практ. Конф. 19 июня 2015 г. / редкол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, Ю.Н. Сопильняк, А.В. Еськов, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2015. – С. 159 – 162.

8. Михайленко, Е.В. Технологии разработки программных приложений для генерации и проверки выполнения практических заданий по математическим дисциплинам / Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 192 – 199.

9. Михайленко, Е.В. О создании программных приложений реализации методов матричных игр для решения задач оптимизации / Е.В. Михайленко, А.Ю. Макуха // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 199 – 203.

10. Уразгильдеев, Б.Г. Специфика решения транспортной задачи с использованием компьютерных технологий / Б.Г. Уразгильдеев, Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 309 – 314.

11. Старостенко, И.Н. Место и роль электронного обучения в обраховательном процессе / И.Н. Старостенко // Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности: сборник начных статей. – Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2016. – С.17 – 23.

Навоев В.В.
Управление ГФС России по ЦФО

ВЫЧИСЛИТЕЛЬНЫЙ ПРИМЕР ПОИСКА ОПТИМАЛЬНОГО МАРШРУТА ДОСТАВКИ КОРРЕСПОНДЕНЦИИ

Органы государственной власти, выполняя свои функции, постоянно осуществляют пересылку важных документов, распоряжений и иной корреспонденции между центральными и местными органами управления. Телеграф, телефон, радио, факс, электронная почта, предлагая самые совершенные, быстрые и удобные методы доставки корреспонденции, тем не менее, не могут заменить самый древний курьерский способ доставки – «из рук в руки». В настоящее время доставка корреспонденции органам

государственной власти реализуется Государственной фельдъегерской службой Российской Федерации (ГФС России).

Успешность доставки корреспонденции, или, говоря другими словами, обеспечение высокого качества осуществления курьерской деятельности определяется рядом концептуальных принципов работы всей службы. К таким принципам организации ГФС России относятся гарантированность сохранности и оперативность доставки корреспонденции [1], которые могут выступать в качестве показателей маршрутов доставки корреспонденции. Однако расплывчатость представления и неопределенность значений данных показателей требуют использования положений и подходов нечеткой логики. Нечёткая логика позволяет дать строгое математическое описание расплывчатых утверждений, реализуя таким образом попытку преодолеть лингвистический барьер между человеком, суждения и оценки которого являются приближенными и нечеткими, и ЭВМ, которые могут выполнять только четкие инструкции [2].

В [3] предложена модель доставки корреспонденции фельдъегерской связью, включающая:

а) $V = \{v_0, v_1, \ ..., v_{N_1}\}$ — множество из пунктов отправки v_0 и доставки $v_1, v_2, \ ..., v_{N_1}$ корреспонденции. Пункты доставки представлены вершинами v_i графа G_v, а дороги между пунктами – дугами (см. рис. 1).

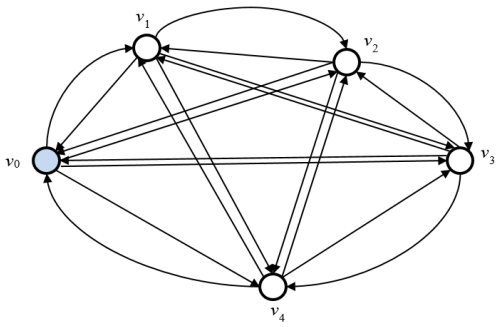


Рис. 1. Граф G_v

б) Отношение «сохранность корреспонденции при доставке из пункта v_i в пункт v_j», заданное с помощью матрицы $Q = (q_{ij})$ экспертных оценок, характеризующих сохранность корреспонденции при доставке из пункта v_i в пункт v_j. При этом сохранность корреспонденции при доставке из пункта v_i в пункт v_j через пункт v_k как определяется как

$$q_{i \to k \to j} = \min\{q_{ik}, q_{kj}\}. \quad (1)$$

в) Три лингвистических переменных, для краткости перечислим только их имена и соответствующие терм-множества:

1) x_1 – гарантированность сохранности корреспонденции;

T_1 = {«без повреждений», «с незначительными повреждениями», «с значительными повреждениями»};

2) x_2 – оперативность доставки;

T_2 = {«высокая», «средняя», «низкая»};

3) y – качество работы фельдъегерской службы;

T_3 = {«удовлетворительное», «неудовлетворительное»};

г) Функции принадлежности:

- для термов переменной x_1:

$$\mu_{СЗП}(z)=\begin{cases}0 \ \ при \ \ z<0,\\ e^{-\frac{z^2}{2\cdot 2^2}} \ \ при \ \ z\geq 0,\end{cases} \qquad \mu_{БП}(z)=\begin{cases}e^{-\frac{(z-10)^2}{2\cdot 2^2}} \ \ при \ \ z\leq 10,\\ 0 \ \ при \ \ z\geq 10.\end{cases}$$

где *СЗП* – с значительными повреждениями, *СНП* – с незначительными повреждениями, *БП* – без повреждений.

д) Правила вида (2), представленные в таблице 3:

$$П_i : ЕСЛИ \ x_1 \ есть \ \widetilde{a}_{i1} \ И \ x_2 \ есть \ \widetilde{a}_{i2} \ ТО \ y \ есть \ \widetilde{b}_i, i=\overline{1,N_2}, \qquad (2)$$

где N_2 – количество правил, $\widetilde{a}_{ij}$ и $\widetilde{b}_i$ – нечеткие термы, которыми в *i*-м правиле оцениваются переменные x_j и y соответственно.

Таблица 3

Правило	ЕСЛИ		ТО
	гарантированность сохранности	оперативность	успешность
$П_1$	без повреждений	высокая	высокая
$П_2$	с незначительными повреждениями	средняя	средняя
$П_3$	с значительными повреждениями	низкая	низкая
$П_4$	с значительными повреждениями	высокая	средняя
$П_5$	без повреждений	низкая	низкая

е) Формулу определения степени выполнения посылки *i*-го правила для текущего входного вектора $\left(x_1^*, x_2^*\right)$:

$$\mu_i\left(x_1^*, x_2^*\right)=\mu_i\left(x_1^*\right)\wedge \mu_i\left(x_2^*\right),$$

где $\mu_i(x_1)$ и $\mu_i(x_2)$ – функции принадлежности x_1 и x_2 термам $\widetilde{a}_{i1}$ и $\widetilde{a}_{i2}$ соответственно, $\wedge$ – *t*-норма, которую в нечетком выводе Мамдани обычно реализуют операцией минимума. Импликация реализуется операцией минимума, а для получения четкого значения выхода $y*$ используется метод центра тяжести [2].

е) Комплексный показатель качества вида:

$$R=\sum_{i=1}^{N_0} c_i \cdot y_i^*, \qquad (3)$$

где c_i – количество предметов корреспонденции, которое необходимо доставить на v_i -й пункт;

y_i^* – значение качества работы фельдъегерской службы при доставке одного предмета корреспонденции на i -й пункт.

Рассмотрим процедуру построения маршрута доставки корреспонденции на примере использования жадного алгоритма, позволяющего получить близкий к оптимальному маршрут.

Пример. Пусть заданы пункт отправки v_0 и пункты доставки v_1, v_2, v_3 корреспонденции и получены в ходе экспертного опроса значения сохранности и времени доставки корреспонденции для маршрутов между ними (см. табл. 1-2). Положим, что в каждый из пунктов v_1, v_2, v_3 необходимо доставить разное количество предметов. Посмотрим, как будет меняться оптимальный маршрут доставки корреспонденции в зависимости от значений c_i. (см. табл. 3).

Таблица 1.

Сохранность корреспонденции

v_i	0	1	2	3
0	0	7	6	1
1	5	0	7	2
2	3	8	0	6
3	3	3	2	0

Таблица 2.

Время доставки (в часах)

v_i	0	1	2	3
0	0	1/4	3/4	1
1	1/4	0	1/2	3/4
2	1/2	3/4	0	3/4
3	1	1/2	1/2	0

Таблица 3.

Состав корреспонденции

Вариант / c_i	A	B	C	D	E	F	G	H
1	1	2	1	1	2	2	3	1
2	1	1	2	1	2	2	1	3
3	1	1	1	2	1	2	1	1

Для построения маршрута доставки корреспонденции воспользуемся жадным алгоритмом. На первом этапе на основе экспертных оценок с использованием системы нечеткого вывода Мамдани определим значения y_i^* для трех маршрутов $v_0 \to v_1$, $v_0 \to v_2$, $v_0 \to v_3$ (см. рис. 2).

Поскольку значение $c_i \cdot y_i^*$ для маршрута $v_0 \to v_1$ максимально, то первым выбранным пунктом доставки будет v_1.

Далее для оставшейся части корреспонденции определим значения y_i^* по маршрутам $v_0 \to v_1 \to v_2$ и $v_0 \to v_1 \to v_3$. В соответствии с (1) $q_{0\to1\to2} = \min\{7, 7\} = 7$, $q_{0\to1\to3} = \min\{7, 2\} = 2$, а значения y_i^* с учетом полного времени доставки корреспонденции в пункты v_2 и v_3 будут принимать значения 5,38 и 5 соответственно.

Поскольку значение $c_i \cdot y_i^*$ для маршрута $v_0 \to v_1 \to v_2$ максимально, то следующим пунктом доставки будет v_2.

Конечным пунктом доставки будет v_3, при этом y_i^* будет равно 5,05.

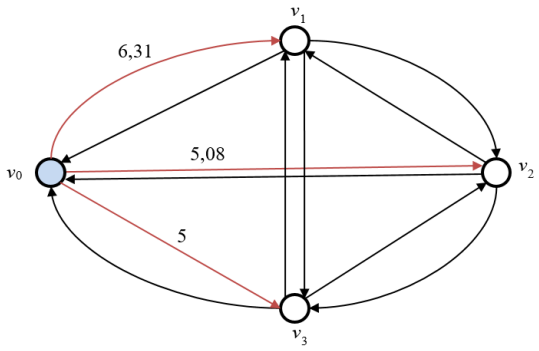


Рис. 2. Первый этап поиска маршрута доставки корреспонденции

В соответствии с формулой (3) комплексный показатель качества будет принимать значение $R = 6{,}31 + 5{,}38 + 5{,}05 = 16{,}74$.

Аналогичным образом определены оптимальные маршруты доставки корреспонденции для остальных вариантов набора корреспонденции, результаты приведены в табл. 4.

Таблица 4.

Оптимальные маршруты для различных наборов корреспонденции

Вариант	Оптимальный маршрут	Комплексный показатель качества R
A	$v_0 \to v_1 \to v_2 \to v_3$	6,31+5,38+5,05=16,74
B	$v_0 \to v_1 \to v_2 \to v_3$	12,62+5,38+5,05=23,05
C	$v_0 \to v_2 \to v_3 \to v_1$	10,16+5,06+5=20,22
D	$v_0 \to v_3 \to v_2 \to v_1$ $v_0 \to v_3 \to v_1 \to v_2$	10+5+5=20
E	$v_0 \to v_1 \to v_2 \to v_3$	12,62+10,76+5,05=28,43
F	$v_0 \to v_1 \to v_2 \to v_3$	18,93+5,38+5,05=29,36
G	$v_0 \to v_2 \to v_3 \to v_1$ $v_0 \to v_2 \to v_1 \to v_3$	15,24+5+5=25,24
H	$v_0 \to v_3 \to v_2 \to v_1$ $v_0 \to v_3 \to v_1 \to v_2$	15+5+5=25

Как видно по результатам расчёта, используемый комплексный показатель качества R, значительно изменяет порядок следования пунктов доставки, если учитывается количество предметов в наборе корреспонденции. Поэтому возможен выбор первым такого участка следования, при котором будет выбираться не наилучший отрезок в смысле сохранности и оперативности доставки только одного предмета, а такой при котором его оптимальность будет определяться только числом доставляемых предметов корреспонденции. В связи с этим возможным является введение в комплексный показатель качества (3) дополнительного коэффициента, учитывающего важность доставляемого предмета.

Возможность применения нечеткой логики для поиска оптимального маршрута доставки позволяет, используя экспертные оценки, повышать комплексный показатель качества работы фельдъегерской службы по доставке корреспонденции. Необходимо также отметить, что возможность введения дополнительных условий по категоризации доставляемых предметов корреспонденции может значительно повлиять на построение и выбор маршрута доставки. Учитывая современный уровень развития вычислительных средств проведение расчетов по определению оптимального маршрута доставки в подразделениях ГФС России может быть автоматизировано и осуществляться с учётом актуализации исходных данных.

Литература:

1. Навоев В.В. Апробация алгоритма выбора маршрута доставки корреспонденции фельдъегерской связью // Вестник Воронежского института МВД Росси – 2017 – № 2 – С. 182-191.

2. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 736 с.

3. Навоев В.В. Применение нечеткой логики для поиска оптимального маршрута доставки корреспонденции фельдъегерской службой / В.В. Навоев, А.Н. Копылов, О.В. Пьянков // Актуальные проблемы прикладной математики, информатики и механики: сборник трудов Международной научно-технической конференции, Воронеж, 18–20 декабря 2017 г. – Воронеж : Издательство ≪Научно-исследовательские публикации≫, 2017. – С. 740-746.

Назаров А.К.
Краснодарский университет МВД России

АСИМПТОТИЧЕСКИЙ АНАЛИЗ ГИПЕРБОЛИЧЕСКИХ СИСТЕМ С БЫСТРО ОСЦИЛЛИРУЮЩИМИ СЛАГАЕМЫМИ

В данной работе рассматриваются гиперболические системы дифференциальных уравнений с частными производными первого порядка, содержащих осциллирующие по времени с частотой ω>>1 слагаемые. Для указанных типов систем применен и обоснован метод усреднения Крылова-Боголюбова и построены полные асимптотики решений.

В параллелепипеде $\Pi_0 = D_0 \times [0,T]$ (D_0 – параллелепипед в $\mathbb{R}^n$) рассматривается возмущенная задача вида

$$\frac{\partial u_i}{\partial t} + \sum_{j=1}^{n} \left[\lambda_{ij}(x,t,\omega t) + \sqrt{\omega}\mu_{ij}(x,t,\omega t)\right] \frac{\partial u_i}{\partial x_j} =$$

$$= f_i(x,t,\omega t,u) + \sqrt{\omega}\varphi_i(x,t,\omega t,u), \quad 1 \leqslant i \leqslant m, \qquad (1)$$

$$u(x,0) = g(x), \qquad (2)$$

где m>0, n>0, ω>>1, $\lambda_{ij}(x,t,\tau), \mu_{ij}(x,t,\tau), f_i(x,t,\tau,u), \varphi_i(x,t,\tau,u)$ – известные действительные функции (1 ≤ j ≤ n, 1 ≤ i ≤ m), g(x) – известная вектор-функция со значениями в $\mathbb{R}^m$, $u = \begin{pmatrix} u_1 \\ u_2 \\ \cdots \\ u_m \end{pmatrix}$ – искомая вектор-функция с значениями в $\mathbb{R}^m$, компоненты которой зависят от переменных *x* и *t*.

Наряду с исходной возмущенной задачей (1)-(2) в параллелепипеде Π_0 рассмотрим в слое Π=$\mathbb{R}^n \times [0,T]$ усредненную задачу

$$\frac{\partial v_i}{\partial t} + \sum_{j=1}^{n} \Lambda_{ij}(x,t)\frac{\partial v_i}{\partial x_j} = F_i(x,t,v), \quad 1 \leqslant i \leqslant m,$$

$$v(x,t)\big|_{t=0} = g(x),$$

где функции $\Lambda_{ij}(x,t)$, $F_i(x,t,v)$ и вектор-функция *g(x)* однозначно определяются через данные исходной задачи (1)-(2). Относительно усредненной задачи будем предполагать, что у нее существует ограниченное решение $v(x,t)$.

При выполнении указанных и некоторых дополнительных условиях справедлива следующая теорема.

Теорема 1. Для любого открытого ограниченного параллелепипеда D_0 в $\mathbb{R}^n$ и любого $\varepsilon > 0$ найдется такое $\omega_0 > 0$, что при $\omega > \omega_0$ существует единственное решение $u_\omega(x,t)$ задачи (1)-(2) в Π_0, и для любых (x,t) из Π_0 выполняется неравенство

$$\|u_\omega(x,t) - v(x,t)\| < \varepsilon.$$

Дополнительно к условиям теоремы 1 будем предполагать выполнение следующих условий:

1) $\mu_{ij}(x,t,\tau) \equiv \mu_{kj}(x,t,\tau) \equiv \eta_j(x,t,\tau)$ $(1 \leq \text{j} \leq \text{n}, 1 \leq \text{i}, k \leq \text{m})$;

2) функции $\lambda_{ij}(x,t,\tau)$, $\eta_j(x,t,\tau)$ $(1 \leq \text{j} \leq \text{n}, 1 \leq \text{i} \leq \text{m})$ вместе с их частными производными по (x,t) любого порядка определены и непрерывны в области определения, а также $l(>0)$ периодичны по τ;

3) функции $f_i(x,t,\tau,u), \varphi_i(x,t,\tau,u)$ $(1 \leq \text{i} \leq \text{m})$ вместе с их частными производными по (x,t,u) любого порядка определены и непрерывны в области определения, а также $l(>0)$ периодичны по τ;

4) средние функций $\eta_j(x,t,\tau)$ и $\varphi_i(x,t,\tau,u)$ $(1 \leq \text{j} \leq \text{n}, 1 \leq \text{i} \leq \text{m})$ по τ равны 0:

$$< \eta_j(x,t,\tau) > \equiv \frac{1}{l}\int_0^l \eta_j(x,t,\tau)\ d\tau = 0,$$

$$< \varphi_i(x,t,\tau,u) > \equiv \frac{1}{l}\int_0^l \varphi_i(x,t,\tau,u)\ d\tau = 0.$$

Асимптотику решения в Π будем искать в виде ряда

$$u(x,t) = u^0(x,t) + \sum_{k=1}^{\infty} \omega^{-k/2}(u^k(x,t) + v^k(x,t,\omega t)),$$

где вектор-функции $v^k(x,t,\tau)$ по переменной τ являются l - периодическими с нулевыми средними.

Рассмотрим также два вида задач.

Задачей вида «А» будем называть задачу о l - периодическом с нулевым средним решением системы уравнений вида

$$\frac{\partial v}{\partial \tau} = f(\tau),$$

где $f(\tau)$ – известная l - периодическая с нулевым средним вектор-функция со значениями в $\mathbb{R}^m$.

Задача вида «В» - это задача Коши для системы m линейных уравнений вида

$$\frac{\partial u_i}{\partial t} + \sum_{j=1}^{n} a_{ij}(x,t)\frac{\partial u_i}{\partial x_j} = \sum_{r=1}^{m} b_{ir}(x,t)u_r + c_i(x,t), (x,t) \in \Pi,$$

$$u_i(x,0) = d_i(x), \quad x \in \mathbb{R}^n,\ 1 \leqslant i \leqslant m.$$

Здесь $a_{ij}(x,t), b_{ir}(x,t), c_i(x,t), d_i(x)$ известные функции, которые однозначно определяются через данные исходной возмущенной задачи.

В сделанных предположениях справедливо следующее утверждение.

Теорема 2. 1. Построение любой p-ой частичной суммы $u^p(x,t)$ формальной асимптотики решения исходной возмущенной задачи в слое Π сводится к решению конечного числа линейных задач видов (А) и (В).

2. Для любого $p = 0,1,2$ ... и любого ограниченного параллелепипеда Π_0 найдутся такие положительные постоянные c_p и ω_p, что при $\omega > \omega_p$ для решения $u_\omega(x,t)$ возмущенной задачи равномерно в Π_0 выполняется оценка

$$\|u_\omega(x,t) - u^p(x,t)\| < c_p\omega^{-(p+1)/2}.$$

Рассмотрим иллюстративный пример, а именно, задачу Коши для системы дифференциальных уравнений следующего вида

$$\begin{aligned}
&\frac{\partial u_1}{\partial t} + (\cos x + \sqrt{\omega}\sin\omega t)\frac{\partial u_1}{\partial x} = \sqrt{\omega}u_2\cos\omega t,\\
&\frac{\partial u_2}{\partial t} + \sqrt{\omega}\sin\omega t\frac{\partial u_2}{\partial x} = \sqrt{\omega}u_1\cos\omega t + u_1\sin\omega t + \sin t,\\
&u_1(x,0) = 0,\\
&u_2(x,0) = 0.
\end{aligned} \tag{3}$$

Асимптотику решения данной задачи будем искать в виде ряда:

$$u_1(x,t) = u_{10}(x,t) + \frac{1}{\sqrt{\omega}}\Big(u_{11}(x,t) + v_{11}(x,t,\omega t)\Big) +$$
$$+ \frac{1}{\omega}\Big(u_{12}(x,t) + v_{12}(x,t,\omega t)\Big) + ...,$$
$$u_2(x,t) = u_{20}(x,t) + \frac{1}{\sqrt{\omega}}\Big(u_{21}(x,t) + v_{21}(x,t,\omega t)\Big) + ... \tag{4}$$

Подставляя ряд (4) в исходную систему (3), получим задачу с начальными условиями. Приравнивая в ней коэффициенты при старшей степени $\omega^{1/2}$, получим

$$\frac{\partial v_{11}}{\partial \tau} + \sin\tau \frac{\partial u_{10}}{\partial x} = u_{20}\cos\tau,$$
$$\frac{\partial v_{21}}{\partial \tau} + \sin\tau \frac{\partial u_{20}}{\partial x} = u_{10}\cos\tau. \tag{5}$$

Откуда находим

$$v_{11} = u_{20}\sin\tau + \cos\tau \frac{\partial u_{10}}{\partial x},$$
$$v_{21} = u_{10}\sin\tau + \cos\tau \frac{\partial u_{20}}{\partial x}. \tag{6}$$

Приравнивая коэффициенты при более младших степенях ω, можно найти любое количество начальных членов асимптотики задачи (3)

$$u_1(x,t) = \frac{1}{\sqrt{\omega}}(\sin\tau - \sin\tau\cos t) + \frac{1}{2\omega}(t - \sin t)\sin\tau + ...,$$
$$u_2(x,t) = 1 - \cos t + \frac{1}{2\sqrt{\omega}}(t - \sin t) + \frac{1}{2\omega}(\cos t - 1)\cos^2\tau + ... \tag{7}$$

При этом согласно теореме 2, в частности, для $p=1$ получим, что для любого ограниченного параллелепипеда $\Pi_0 = [a,b]\times[0,T]$ в $\mathbb{R}^2$ найдутся такие положительные постоянные c_1 и ω_1, что при $\omega > \omega_1$ для решения $u(x,t)=\binom{u_1(x,t)}{u_2(x,t)}$ задачи Коши (3) равномерно в Π_0 выполняются оценки

$$|u_1(x,t) - \frac{1}{\sqrt{\omega}}(\sin\omega t - \sin\omega t\cos t)| \leqslant \frac{c_1}{\omega},$$
$$|u_2(x,t) - 1 + \cos t - \frac{1}{2\sqrt{\omega}}(t - \sin t)| \leqslant \frac{c_1}{\omega}.$$

Литература:

1. Боголюбов Н.Н. О некоторых статистических методах в математической физике. Львов: Изд. АН УССР, 1945. 139 с.

2. Хома Г.П. Теорема об усреднении для гиперболических систем первого порядка // Укр. мат. журн. 1970. Т.22, №5. С.699–704.

3. Симоненко И.Б. Метод усреднения в теории нелинейных уравнений параболического типа с приложением к задачам гидродинамической устойчивости. Ростов-на-Дону: Изд. РГУ, 1989. 111 с.

4. Левенштам В.Б. Обоснование метода усреднения для параболических уравнений, содержащих быстроосциллирующие слагаемые с большими амплитудами // Изв. РАН сер. мат. 2006. Т. 70, № 2. С. 25-56.

5. Назаров А.К. Усреднение уравнений в частных производных первого порядка // Эколог. вестник науч. центров ЧЭС. 2015, №4. С. 62-68.

Никеев С.С., Филипенко И.В.
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

МОДЕЛИРОВАНИЕ ВТОРЖЕНИЙ ДЛЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Аннотация. Для определения требований системы обнаружения вторжений предлагается моделировать вторжение. При этом каждое вторжение разбивается на семь этапов, и каждый из этапов рассматривается более подробно.

Ключевые слова: система обнаружения вторжений, вторжения, система, моделирование вторжений, обнаружение вторжений.

Чтобы помочь в определении и проверке требований к системе обнаружения вторжений (СОВ), будем моделировать вторжение, которое будет являться нарушением политики безопасности системы. Вторжения приводят к компрометации (несанкционированное раскрытие данных или использование услуг), целостности (несанкционированное изменение данных) или доступности (отказ в обслуживании).

Вторжения могут осуществляться разными способами. Такие вопросы, как какие вторжения могут быть эффективно обнаружены СОВ на какой стадии вторжения программное обеспечение (ПО) СОВ должно обнаруживать каждую атаку, и какие гарантии можно дать, чтобы программное обеспечение СОВ обнаружило вторжения, должно решаться анализом требований. Подход к моделированию, начинается с тщательного анализа вторжений и поддерживает разработку теоретической модели обнаружения вторжений, будет отвечать на вопросы, как вторжения можно обнаружить, какие данные из разных датчиков могут быть скооперированы, и количественную оценку того, что это событие является вторжением. Вторжения приводят к несанкционированному раскрытию данных или использованию услуг, несанкционированному изменению данных или отказу в обслуживании.

Моделирование вторжений представляет собой обратный поиск. Он начинается с вторжения и отслеживается через возможные параллельные и последовательные комбинации событий, которые вызвали такое вторжение. Моделировать вторжение можно в дальнейшем, например, используя логический граф И-ИЛИ. В данной работе рассматривается только общий обзор, отвечающий на вопрос: «Как происходит вторжение?».

Моделирование основывается на различных источниках. Стандарты, используемые в текущих сетях TCP, IP, являются общедоступными. Предложения и стандарты для IP-сетей публикуются в интернете. Реализации большинства сетевых протоколов свободно доступны в программном обеспечении, таком как Linux FreeBSD и Apache, что позволяет публиковать обзор проблем безопасности. Многочисленные исследователи и хакеры активно обнаруживают и публикуют уязвимости в публичных форумах, такие как bugtraq и веб-сайтах, такие как www.securityfocus.com.

Ошибки, которые, как правило, ориентированы на UNIX, рассматриваются в деревьях отказов, хотя многие проблемы (например, переполнение буфера) существуют в программном обеспечении других систем. Вместо того чтобы смотреть прямо на исходный код для этих систем, огромное количество публично обсуждаемой информации об уязвимости используется в качестве входных данных для моделирования вторжений.

Подход, к моделированию предлагаемый в статье, основывается в разделении вторжения на этапы, которые достигает злоумышленник при осуществлении вторжения.

Анализ Рю вторжений [1] разделил вторжения на семь этапов:

– разведка – поиск целей;
– идентификация уязвимостей – нахождение уязвимостей в целях;

– проникновение – получение несанкционированного доступа к цели с помощью уязвимости;

– контроль - получить привилегии над целью;

– встраивание – скрытие активности в цели и обеспечение будущего доступа к цели;

– извлечение и изменение данных – получение или изменение конфиденциальной информации;

– ретрансляция атак – атаковать другие цели.

Далее рассмотрим подробнее каждый из предложенных этапов.

Разведка. Фаза разведки идентифицирует потенциальные цели в сетях организации. Сетевые цели включают не только многопользовательские хосты (например, UNIX или Windows NT), но также маршрутизаторы, интеллектуальные хабы и, возможно, даже модемы. Услуги, предлагаемые системами и именами пользователей в системах, также являются полезными битами информации для злоумышленника, но для достижения успешной атаки может потребоваться только часть этой информации.

Идентификация уязвимостей. Идентификация уязвимости тесно связана с разведкой. На этом этапе злоумышленник ищет уязвимости, которые могут привести к проникновению. Злоумышленник последовательно сканирует многие порты, уязвимые для атаки. Сканирование портов – это активная атака, и ее обычно легко обнаружить, если она выполняется очень медленно.

Проникновение. Проникновение происходит, когда злоумышленник получает несанкционированный доступ к системе. Способы проникновения включают в себя использование различных уязвимостей сетевого сервера (плохая аутентификация и переполнение буфера), аутентификация с использованием незаконно полученных паролей и захват сеанса TCP.

Контроль. Злоумышленник должен получить достаточные привилегии в системе, чтобы продолжить последующие этапы вторжения. Зачастую злоумышленник должен получить привилегии, эквивалентные привилегиям системного администратора, чтобы получить достаточный контроль над системой. Если проникновение было особенно эффективным и достаточным привилегии уже были получены, этот шаг может и не понадобиться.

Механизмы, используемые злоумышленником, включают в себя использование переполнения буфера в привилегированных локальных программах, использование временных файлов или сигналах, использование слабых разрешений на критические файлы и устройства, взлома пароля для учетной записи администратора.

Встраивание. Встраивание подразумевает установку или модификацию системы так, что даже если злоумышленник обнаружен и будут предприняты шаги для восстановления системы, он все равно сможет войти в систему. Например, код системы начальной загрузки может быть изменен для повторной установки бэкдор, если исполняемые программы системы будут восстановлены из резервных копий или установочного носителя. Типичные методы включают в себя установку троянских коней, бэкдоров и других руткит-программ, удаление следов вторжения из системных журналов и отключение систем обнаружения.

Руткит – это набор программ для встраивания в систему, которые позволяют злоумышленнику скрыть свои действия и могут включать в себя программы для использования на следующем этапе, извлечение и изменение данных. Рассматриваются две версии руткита – это руткит Linux с 1994 года и версия 4 руткита Linux.

Руткит Linux очень прост. Он состоит из четырех программ:

– fix – программа для установки других программ-руткитов вместо оригинальных системных программ копирующая разрешения, время. дату и контрольную сумму оригинальной программы для программы руткита;

– login – модифицированная версия программы аутентификации пользователя для входа, которая позволяет всем войти в систему с паролем whOOt!;

– netstat – модифицированная версия программы отчетности сетевой активности, которая скрывает сетевую активность отдельных пользователей или подключений к конкретным хостам или портам;

– ps – модифицированная версия программы отчетов о состоянии процесса ps, которая скрывает процессы, принадлежащие конкретным пользователем, процессы, выполняемые на определенных терминалах, и процессы, выполняющие определенные программы.

Версия 4 руткита Linux устанавливает гораздо больший набор программ для встраивания, чем руткит 1994 года, включая chfn, chsh, crontab, find, inetd, passwd, rshd, sysklogd, tcp и сниффер паролей.

Извлечение и изменение данных. На этапе извлечения и модификации данных злоумышленник собирает информацию о конфигурации и работе системы. Скрытые соединения могут использоваться для перемещения обнаруженных данных из собранной системы на базу злоумышленника. Примером полезных извлеченных данных могут быть взломанные пароли учетных записей.

Ретрансляция атак. После того, как система полностью скомпрометирована, ее можно использовать для ретрансляции атак. Атаки могут быть запущены против доверенных хостов для расширения количества хостов под контролем злоумышленника. Системы также могут быть просто использованы для участия в распределенных атаках типа «отказ в обслуживании». Tribe Flood Network и Trinoo являются распределенными атаками отказа в обслуживании. Например, распределенная атака отказа в обслуживании Stacheldraht зависит от агентов [2] ретрансляции, которые установлены злоумышленником на взломанных компьютерах. Ретранслятор Stacheldraht принимает команды от обработчика, который управляет группой агентов ретрансляции. Обработчик, в свою очередь, контролируется клиентом Stacheldraht, который предоставляет пользовательский интерфейс для злоумышленника. Ретранслятор Stacheldraht реализует ICMP переполнение, SYN переполнение, UDP переполнение и атаки Smurf. С помощью агентов [5] Stacheldraht, распределенных логически в Интернете, злоумышленник может монтировать атаку, которая может полностью отключить доступ к Интернету даже большой организации.

Существует множество других форм ретрансляции атак, включая автоматические и ручные средства. Stacheldraht, Tribe Flood Network и Trinoo являются образцом существующих хорошо известных, хорошо проанализированных распределенных систем ретрансляции атак.

В заключение рассмотрим два примера использования предложенного разделения вторжения на этапы.

Пример 1: вторжение FTP SITE EXEC. Атака SITE EXEC против wuftpd является интересным эксплойтом переполнения буфера. Когда кто-то входит в wuftpd как пользователь анонимный или ftp просит ввести адрес электронной почты в качестве пароля. Однако злоумышленник может отправить вредоносный код оболочки в ответ на запрос пароля. Затем, если команда SITE EXEC включена, злоумышленник может отправить команду SITE EXEC с символами % – форматирования, которые вызывают переполнение буфера с данными, ранее полученными в качестве пароля [3]. Примером команды FTP SITE EXEC для злоумышленника может быть строка «SITE EXEC … (код объекта для выполнения) %n (код объекта) %n (код объекта)%n\n». Последовательность форма-

тирования %n интерпретируется функцией printf как запрос на запись количества выводимых до сих пор символов в целочисленное местоположение. Злоумышленник может разработать эксплойт, который использует последовательность форматирования %n для процедуры возвращения адреса в стэке. Когда функция printf возвращает, и если эксплоит будет успешным, выполняется код, предоставленный злоумышленником. В случае FTP-сервера wuftpd строка, предоставленная в качестве аргумента команде SITE EXEC, передается в функцию syslog, которая интерпретирует символы % – форматирования с использованием семейства подпрограмм printf.

– Разведка. Злоумышленник обнаруживает хост FTP-сервера, и обнаруживает его доступность.

– Идентификация уязвимостей. Злоумышленник соединяется с FTP-сервером и убеждается, что номер версии ПО, сообщаемый сервером, уязвим для атаки FTP SITE EXEC.

– Проникновение. Злоумышленник подключается к FTP-серверу, дает «анонимный» или «ftp» в качестве имени пользователя и вводит вредоносный код оболочки в качестве пароля. Затем злоумышленник выдает команду SITE EXEC, содержащую последовательности символов форматирования в стиле printf, которые переполняют буфер символов в стеке процесса, чтобы выполнить код, предоставленный в качестве ранее введенного «пароля». Если переполнение выполнено успешно, код, предоставленный злоумышленником, выполняется с привилегиями root. Успешная атака FTP SITE EXEC также дает контроль, поэтому злоумышленник может перейти на более поздние этапы вторжения.

– Контроль. Предполагается, что успешное проникновение приводит к привилегированному доступу, поэтому контрольная фаза вторжения может быть обойдена.

– Внедрение. Злоумышленник запускает версию Linux Rootkit версии 4, которая заменяет ряд программ с помощью троянских реализаций, которые скрывают его действия. Таким образом, происходят изменения в файловой системе.

– Извлечение данных. Злоумышленник устанавливает и запускает сниффер паролей, который запоминает имена пользователей и пароли.

– Ретрансляция атак. Злоумышленник устанавливает и запускает распределенный агент отказа в обслуживании, такой как Trinoo, TFN или Stacheldraht. Затем злоумышленник может использовать систему для совершения атак на другие сетевые сайты.

Моделирование вторжения помогло определить требования для программного обеспечения мобильных агентов, которым поручено выявлять вторжение FTP SITE EXEC. Система обнаружения вторжений должна контролировать команды PASS в сеансе FTP для данных, которые не представляют действительную последовательность печатаемых символов. Недопустимая последовательность печатных символов – это событие минимального сокращения. В анализе ничего не говорится о том, как следует осуществлять или выполнять мониторинг: это просто приводит к требованиям к системе обнаружения вторжений.

Пример 2: вторжение FTP-отказов. Атака FTP-отказов может использоваться для передачи данных на сетевой порт, к которому злоумышленник обычно не имеет доступа [4]. Один из способов использования этой уязвимости – отправить данные на удаленный сервер оболочки, который доверяет FTP-хосту через FTP-сервер. После того, как злоумышленник обнаруживает FTP-сервер и хост, используя rsh который доверяет FTP-серверу, злоумышленник пытается использовать этот эксплойт:

– загружает специально отформатированный файл на FTP-сервер;

– выдает команду FTP PORT, которая направляет FTP-сервер для отправки следующей загрузки на порт 514 на целевом хосте;

– выдает команду FTP GET для «загрузки» содержимого предварительно загруженного файла в порт 514 на цель: команда GET открывает соединение с FTP-сервером на порту 20 к демону rsh на цели;

– если целевой сервер доверяет FTP-серверу, rsh будет принимать содержимое файла так, как если бы он был введен пользователем и выполнял данную команду.

Рассмотрим данное вторжение поэтапно.

– Разведка. Злоумышленник обнаруживает хост FTP-сервера и целевой хост, и обнаруживает их доступность FTP-сервера и сервера RSH [6].

– Идентификация уязвимостей. Злоумышленник соединяется с FTP-сервером и убеждается, что номер версии ПО, сообщаемый сервером, уязвим для атаки с отказом FTP. Для злоумышленника также нужен каталог на FTP-сервере, на который он может загрузить файл: если злоумышленник не имеет доступа к FTP-серверу, отличному от «анонимного», злоумышленнику придется искать такой каталог. Также, вероятно, придется предположить, что целевой хост доверяет хосту FTP-сервера, если только злоумышленник уже не имеет доступа к целевому хосту и может читать файлы etc, hosts.equiv или «root, rhosts».

– Проникновение. Злоумышленник загружает командный файл оболочки на FTP-сервер и выдает соответствующие команды FTP, чтобы заставить FTP-сервер «загрузить» файл в службу RSH-адреса. Успешная атака отказа FTP, установленная против привилегированной учетной записи на целевой стороне, также дает контроль, поэтому злоумышленник может перейти на более поздние этапы вторжения.

– Контроль. Предполагается, что успешное проникновение приводит к привилегированному доступу, поэтому контрольная фаза вторжения может быть обойдена.

– Внедрение. Злоумышленник устанавливает версию руткита Linux версии 4, которая заменяет ряд программ с помощью троянских реализаций, которые скрывают действия злоумышленника. Замененные программы включают ps, login, netstat, chfn, chsh, crontab, find, inetd, passwd, rshd, sysklogd и tcp. Программа обновления флэш-памяти также устанавливается как часть руткита Linux версии 4, которая ведет к фазе извлечения данных.

– Извлечение данных. Злоумышленник устанавливает и запускает сниффер паролей, который запоминает имена пользователей и пароли.

– Ретрансляция атак. Злоумышленник устанавливает и запускает распределенный агент отказа в обслуживании, такой как Trinoo, TFN или Stacheldraht. Затем злоумышленник может использовать систему для совершения атак на другие сетевые сайты.

Моделирование вторжения помогло определить требования для программного обеспечения мобильного агента, которому было поручено обнаружить атаку отказов FTP. Программные требования к СОВ состоят в том, чтобы контролировать команды и ответы в сеансе FTP, отслеживать соединения rsh и сопоставлять выходы с двух мониторов, чтобы определить, была ли предпринята попытка отката FTP и была ли атака успешной.

Каждый из шагов, описанных выше, представляет собой сценарий, для определения лучшего момента, когда могут применяться контрмеры. Контрмеры в системах обнаружения вторжений обычно включают оповещения диспетчера системы (через электронную почту, пейджинг или просто сообщения журнала), прекращение сетевых подключений или логинов и отключение учетных записей пользователей.

Моделирование вторжений исследуют необходимые и достаточные комбинации событий, которые приводят к использованию уязвимости. Разработка таких моделей для вторжений позволяет проводить их обнаружение и проверку. Кроме того, анализ модели выявляет условия, при которых контрмеры могут быть успешно применены системой обнаружения вторжений, чтобы вмешаться до того, как вторжение будет успешным. Определение того, какие характеристики вторжений можно контролиро-

вать, является важной частью анализа требований для СОВ. Каждое событие должно быть проанализировано, чтобы определить, какая часть контролируемой системы является свидетельством возникновения вторжения. Если нет возможности получить доказательства этого вторжения, его невозможно обнаружить.

Анализируя эти события можно определить, какие вторжения будет особенно трудно обнаружить, и может давать подсказки относительно способов предотвращения таких вторжений. Например, существуют определенные события вторжений, которые не имеют заметного эффекта в распределенной системе сайта. Например, в случае взлома пароля способы предотвращения вторжения включают использование одноразовых паролей или сеансов терминалов, чтобы избежать переноса паролей в чистом виде.

Таким образом, использование моделирования вторжений было представлено с помощью вспомогательных примеров. Обследовано разделение вторжений на различные этапы. Были описаны этапы вторжения, и были исследованы два вторжения. Был описан пример использования моделирования для анализа контрмер.

Анализ моделей вторжения к ряду преимуществ. Они позволяют проводить структурированный анализ вторжений, включая анализ степени тяжести и вероятности, определение контрмер, определение приоритетов для разработки и определяют требования к СОВ, также могут, в дальнейшем, помочь в процессе проверки СОВ.

Литература:

1. Ruiu D., Cautionary tales: Stealth coordinated attack howto // Digital Mogul 2. – 1999. –76 p.

2. Кошелев Д.А., Частиков А.П., Дейкун Д.Г., Шевцова К.Г., Полусмак В.И., Бородовицина Т.К., Арутюнян Т.В., Программно–аппаратное обеспечение обучающихся и самообучающихся нейросетей / Международный научно-исследовательский журнал «Успехи современной науки». – 2016. –№8.– С. 21-23.

3. Jennings N. R., Wooldridge M. J. Applications of Intelligent Agents. –London: Queen Mary & Westfield College, University of London. – 2000. – 27 p.

4. Кошелев Д.А., Частиков А.П. Искусственный интеллект в информационных технологиях // Инновационные технологии в образовательном процессе. Материалы XVII Всероссийской научно-практической конференции. 2016. С. 259-261.

5. Арутюнян Т.В., Онищук С.А. Волновая природа сердечной деятельности / Всероссийская заочная научно-практическая конференция «Современные проблемы физики, биофизики и инфокоммутационных технологий». Коллективная монография. Краснодар: Краснодарский ЦНТИ, 2014. – С. 77-86.

6. Лыков Н.Ю., Максимов Р.В., Шарифуллин С.Р. Маскирование структуры и алгоритмов функционирования интегрированных инфокоммуникационных систем / VIII международная научная конференция «ТТС-16». Краснодар: КубГТУ, КВВАУЛ им. А.К. Серова; под общ. ред. Б.Х. Гайтова. 2016. – С. 203-206.

Осипян В.О., Литвинов К.И.

Кубанский государственный университет

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КРИПТОСИСТЕМЫ НА ОСНОВЕ ДИОФАНТОВА УРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

На основе теоретических истоков построения математических моделей эффективных криптосистем мы исходим о необходимости использования сложных математических задач, решение которых потребует от нелегального пользователя большого объема вычислительной работы. К таким задачам, следуя К. Шеннону [1], относятся задачи, содержащие «диофантовы трудности», использование которых препятствует возможности сократить множество перебираемых ключей.

Предварительно приведём некоторые факты, используемые нами в дальнейшем при построении математической модели систем защиты информации (СЗИ).

Как известно [2, 3], под диофантовым уравнением понимают полиномиальное уравнение

$$f(x_1, x_2, \ldots, x_n) = 0 \quad (1)$$

коэффициенты которого суть целые числа, и решения требуется найти тоже в целых или целых неотрицательных числах. Задача решения диофантово уравнения (1), как правило, заключается в поиске целочисленных решений заданного уравнения или доказательства того, что таких решений нет.

В 1900 году была сформулирована Десятая проблема Гильберта, состоящая в нахождении алгоритма решения произвольного алгебраического диофантова уравнения. В 1970 году Ю.В. Матиясевич доказал алгоритмическую неразрешимость данной проблемы [2]. Следствием из этого является то, что гарантированно отсутствует общий алгоритм решения некоторого диофантова уравнения (что значительно затрудняет решение некоторого уравнения без какой-либо дополнительной информации о корнях).

Сегодня, использование диофантовых уравнений для разработки систем защиты информации становится все интенсивнее [4, 5, 6, 9, 10, 11]. Цель данной работы – продемонстрировать возможность использования даже простейших диофантовых уравнений для разработки достаточно устойчивых ко взлому систем защиты информации.

Рассмотрим возможность применения диофантовых уравнений некоторого класса для математического моделирования систем защиты информации.

2 Метод решения линейного неоднородного диофантова уравнения

Рассмотрим линейное диофантово уравнение

$$\sum_{i=1}^{m} a_i \cdot x_i = c, \quad (2)$$

где $A = (a_1, \ldots a_m), c, m$ – целые числа, $m \geq 2$.

Для данного уравнения справедливы следующие утверждения:

1) Если наибольший общий делитель $a_i, i = 1,2, \ldots, m$ не делит c, то уравнение (4) неразрешимо в целых числах.

2) Справедливо обратное, если наибольший общий делитель $a_i, i = 1,2, \ldots, m$ делит c, то уравнение (4) разрешимо в целых числах и имеет бесконечное множество решений.

Следовательно, если наибольший общий делитель $a_i, i = 1,2, \ldots, m$ равен 1 , т.е. $a_i, i = 1,2, \ldots, m$ взаимно простые числа, то уравнение (4) всегда разрешимо в целых числах. Это открывает возможности для применения данного уравнения (4) при разработке математической модели простейшей системы защиты информации в случае, когда все его коэффициенты взаимно простые, что означает ….

Предварительно определим вектор модулей $N = (n_1, \ldots, n_m), m \geq 2$, удовлетворяющий следующим условиям:

1) $\forall j,\ j \in [1, m]\ n_j < \sum_{i=1}^{m} a_i$;

2) $\forall i, j,\ i \neq j\ , (n_i, n_j) = 1.$

Также определим вектор переменных $B = (b_1, \ldots, b_m)$, удовлетворяющих следующему условию:

1) $\forall i, j, i, j \in [1, m], a_i \cdot b_j > n_j.$

Подробное описание подбора параметров представлено в разделе 3.

Используя переменные n_j и b_j, рассчитаем коэффициенты k_{ji}:

$$k_{ji} = a_i \cdot b_j \, mod \, n_j.$$

Тогда уравнение (4) можно представить в виде системы:

$$\begin{cases} \sum_{i=1}^{m} a_i \cdot x_i \cdot b_1 \bmod n_1 = c * b_1 \bmod n_1 \\ \dots \\ \sum_{i=1}^{m} a_i \cdot x_i \cdot b_m \bmod n_m = c * b_m \bmod n_m \end{cases} \Rightarrow \begin{cases} \sum_{i=1}^{m} k_{1i} \cdot x_i = c_1 (\bmod n_1) \\ \dots \\ \sum_{i=1}^{m} k_{mi} \cdot x_i = c_m (\bmod n_m) \end{cases} \quad (4)$$

Для того чтобы система (6) решалась однозначно, необходимо избавиться от неопределенности, порождаемой операцией $\bmod n_j$ в правых частях уравнений системы. Это приведет нас к системе

$$\begin{cases} \sum_{i=1}^{m} k_{1i} \cdot x_i = c_1, \\ \dots \\ \sum_{i=1}^{m} k_{mi} \cdot x_i = c_m. \end{cases} \quad (5)$$

Для этого необходимо, чтобы выполнялись условия:

$$\begin{cases} \sum_{i=1}^{m} k_{i1} \cdot x_i < n_1, \\ \dots \\ \sum_{i=1}^{m} k_{im} \cdot x_i < n_m. \end{cases} \quad (6)$$

Так как $k_{i,j}$ – фиксированные значения, то выполнение указанных условий (8) позволит определить допустимые граничные значения переменных x_i, при которых система (6) будет решаться однозначно.

Ограничим сверху правые части системы неравенств (8):

$$\begin{cases} \sum_{i=1}^{m} k_{i1} \cdot x_i \le \max(k_{i1}) * \sum_{i=1}^{m} x_i, \\ \sum_{i=1}^{m} k_{im} \cdot x_i \le \max(k_{im}) * \sum_{i=1}^{m} x_i. \end{cases} \quad (7)$$

Таким образом, если данные ограничения (9) будут меньше n_j, то и исходные неравенства будут меньше соответствующих n_j.

$$\begin{cases} \max(k_{i1}) * \sum_{i=1}^{m} x_i < n_1 \\ \dots \\ \max(k_{im}) * \sum_{i=1}^{m} x_i < n_m \end{cases} \Rightarrow \begin{cases} \sum_{i=1}^{m} x_i < \frac{n_1}{\max(k_{i1})} \\ \dots \\ \sum_{i=1}^{m} x_i < \frac{n_m}{\max(k_{im})} \end{cases} \Rightarrow \sum_{i=1}^{m} x_i < \min\left(\frac{n_j}{\max(k_{1j}, \dots, k_{mj})}\right). \quad (8)$$

Система уравнений (6) при соблюдении условий (10) имеет единственное решение, если ранг матрицы K, составленной из значений k_{ij} равен m.

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{pmatrix}; \ \operatorname{rang}(K) = m.$$

Иными словами, если векторы $(k_{11}, \dots, k_{m1}), \dots, (k_{m1}, \dots, k_{mm})$ линейно независимы. Если же эта система линейно зависима, то система не будет разрешаться однозначно.

3 Подбор векторов, обеспечивающих корректное решение линейного неоднородного диофантова уравнения

Для прикладного приложения разработанного метода решения линейного неоднородного диофантова уравнения (4) к моделированию системы защиты информации необходимо, чтобы подобранные переменные b_j и модули n_j обеспечивали достаточно большое значение выражения (10). Иными словами, чтобы была возможность шифровать исходные сообщения заранее фиксированной длины; например, 256 – для шифрования отдельных байтов). А также, чтобы ранг полученной матрицы был равен m.

Рассмотрим возможность построения векторов A, B, N, на основе определенной изначально матрицы K.

Пусть существует квадратная матрица K с рангом m (в общем случае это может быть единичная матрица).

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mm} \end{pmatrix};\ rang(K) = m.$$

Подберем такие различные взаимно простые модули n_j, чтобы значение выражения (10) было больше или равно некоторого t. Также подберем переменные b_j, так, чтобы $\forall j, j \in [1, m]\ (b_j, n_j) = 1$.

Таким образом, мы получаем систему уравнений относительно a_i:

$$\begin{cases} b_1 * a_1 = k_{11} (\mathrm{mod}\ n_1), \\ \dots \\ b_1 * a_m = k_{1m} (\mathrm{mod}\ n_1), \\ b_2 * a_1 = k_{21} (\mathrm{mod}\ n_2), \\ \dots \\ b_2 * a_m = k_{2m} (\mathrm{mod}\ n_2), \\ \dots \\ b_m * a_1 = k_{m1} (\mathrm{mod}\ n_m), \\ \dots \\ b_m * a_m = k_{mm} (\mathrm{mod}\ n_m). \end{cases} \quad (9$$

Как видно из системы (11), каждый $a_i, i = 1,2, \dots, m$ вычисляется независимо от других. Рассмотрим вычисление на примере одного из них. Пусть для общности это будет a_1.

Рассмотрим систему, состоящую из m уравнений.

$$\begin{cases} b_1 * a_1 = k_{11} (mod\ n_1) \\ \dots \\ b_m * a_1 = k_{m1} (mod\ n_m) \end{cases} \quad (10)$$

Сведем систему (12) к системе вида:

$$\begin{cases} a_1 = k'_{11} (mod\ n_1) \\ \dots \\ a_1 = k'_{m1} (mod\ n_m) \end{cases} \quad (11)$$

Так как $\forall j,\ j \in [1, m]\ (b_j, n_j) = 1$, это возможно.

Система (13) однозначно разрешима, с использованием Китайской теоремы об остатках [8]. Таким образом, мы находим искомый a_1. Аналогичным образом, находятся прочие $a_i, i = 1,2, \dots, m$.

4 Моделирование СЗИ на основе заданного линейного неоднородного диофантова уравнения

Рассмотрим использование описанного преобразования линейного неоднородного диофантова уравнения (1) для моделирования систем защиты информации как симметричной, так и асимметричной.

Этап генерации ключа совпадает для обоих случаев: определяется матрица K ранга m и вектор $N = (n_1, \dots, n_m)$ так, чтобы значение системы (10) было больше либо равно некоторого t – размерность пространства исходных текстов. Множество исходных текстов – целые числа из полуинтервала $[0, .., t)$. Также определяется вектор $B = (b_1, \dots, b_m)$, так чтобы $\forall j, j \in [1, m]\ (b_j, n_j) = 1$. Вектор $\mathrm{A} = (\mathrm{a}_1, \dots, \mathrm{a}_\mathrm{m})$ является решением системы (12). Далее, в зависимости от типа системы защиты информации, найденные векторы A, B, N и матрица K относятся к симметричным или асимметричным ключам.

В симметричных системах защиты информации для шифрования и расшифровывания применяется один и тот же ключ. Этим ключом будут число t, векторы A, B, N и матрица K [9].

Схема реализации симметричной системы защиты информации:

1) Генерация ключа.

Пользователь Алиса определяет ключ шифрования $\mathrm{d} = \{\mathrm{t}, \mathrm{A}, \mathrm{B}, \mathrm{N}, \mathrm{K}\}$ и затем посылает эту информацию пользователю Бобу по безопасному каналу (или с использованием различных протоколов обмена симметричными ключами).

2) Шифрование и передача сообщения.

Алиса выбирает исходное сообщение $\mathrm{M} = \sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{M_i}, \mathrm{M} \in [1, \mathrm{t})$. Далее он вычисляет шифртекст C с использованием ключа d:

$$\mathrm{C} = \mathrm{E}(\mathrm{M}, \mathrm{d}) = \sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{M_i} * \mathrm{a_i}.$$

и передает Бобу полученный шифртекст C.

3) Дешифрование сообщения.

Боб вычисляет исходный текст M с использованием ключа d. По сути, действия Боба состоят в построении системы (7) на основе диофантова уравнения $\sum_{i=1}^{m} x_i * a_i = C$ с использованием векторов B, N, K. Сумма решений системы совпадет с исходным сообщением M.

В системах асимметричного шифрования используются 2 ключа – открытый и закрытый, связанные друг с другом. Открытый ключ передается по открытому (небезопасному каналу) и используется для шифрования сообщения. Для дешифрования сообщения используется секретный ключ [9].

Из описания схемы реализации системы асимметричного шифрования легко заметить, что для шифрования используется только вектор A и число t. А векторы B, N и матрица K лишь в дешифровании. Таким образом, вектор A может выступать в роли открытого ключа, а векторы B, N и матрица K – в качестве закрытого.

Схема реализации асимметричной системы защиты информации:

1) Генерация ключевой пары.

Алиса определяет открытый ключ шифрования $e = \{t, A\}$ и закрытый ключ $\mathrm{d} = \{B, N, K\}$, а затем посылает открытый ключ Бобу по открытому каналу.

2) Шифрование и передача сообщения.

Боб выбирает исходное сообщение $\mathrm{M} = \sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{M_i}, \mathrm{M} \in [1, \mathrm{t})$. Далее он вычисляет шифртекст C с использованием открытого ключа

$$\mathrm{C} = \mathrm{E}(\mathrm{M}, \mathrm{e}) = \sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{M_i} * \mathrm{a_i},$$

и передает Алисе полученный шифртекст C.

3) Дешифрование сообщения.

Алиса вычисляет исходный текст M с использованием ключа d. По сути, действия Алисы состоят в построении системы (7) на основе диофантова уравнения $\sum_{i=1}^{m} x_i *$

$a_i = C$ с использованием векторов B, N, K. Сумма решений системы совпадет с исходным сообщением M.

5 Пример асимметричной системы защиты информации на основе линейного неоднородного диофантова уравнения с тремя переменными

Рассмотрим простой пример СЗИ, в основе которого лежит линейное неоднородного диофантово уравнения из трех переменных.

Генерация ключа.

Определим t = 256 – мощность алфавита. В качестве матрицы K возьмем единичную матрицу ранга *3*. В качестве вектора модулей $N = (n_1, \dots, n_m)$, $m = 3$ возьмем 3 последовательных простых числа, больших 256 – $N = (257, 263, 269)$. В качестве вектора переменных $B = (n_1, \dots, n_m), m = 3$ возьмем следующий вектор $B = (2,3,5)$.
Тогда система (11) будет иметь вид

$$\begin{cases} 2 * a_1 = 1 (\mathrm{mod}\ 257), \\ 2 * a_2 = 0 (\mathrm{mod}\ 257) \\ 2 * a_3 = 0 (\mathrm{mod}\ 257), \\ 3 * a_1 = 0 (\mathrm{mod}\ 263), \\ 3 * a_2 = 1 (\mathrm{mod}\ 263), \\ 3 * a_3 = 0 (\mathrm{mod}\ 263), \\ 5 * a_1 = 0 (\mathrm{mod}\ 269), \\ 5 * a_2 = 0 (\mathrm{mod}\ 269), \\ 5 * a_3 = 1 (\mathrm{mod}\ 269). \end{cases} \Rightarrow \begin{cases} a_1 = 129 (\mathrm{mod}\ 257), \\ a_2 = 0 (\mathrm{mod}\ 257) \\ a_3 = 0 (\mathrm{mod}\ 257), \\ a_1 = 0 (\mathrm{mod}\ 263), \\ a_2 = 88 (\mathrm{mod}\ 263), \\ a_3 = 0 (\mathrm{mod}\ 263), \\ a_1 = 0 (\mathrm{mod}\ 269), \\ a_2 = 0 (\mathrm{mod}\ 269), \\ a_3 = 54 (\mathrm{mod}\ 269). \end{cases}$$

Используя Китайскую теорему об остатках [8] получаем:

$$a_1 = 228159075,$$
$$a_2 = 1022062272,$$
$$a_3 = 259143894.$$

Таким образом, имеем следующий открытый ключ – вектор $A = (228159075, 1022062272, 259143894)$ и мощность алфавита t.

Рассмотрим процесс шифрования. Пользователь Боб знает открытый ключ пользователя Алисы $A = (228159075, 1022062272, 259143894)$ и t=256. Он выбирает исходное сообщение m из чисел на отрезке $[1, 256]$ и разбивает его на 3 слагаемых произвольным образом (слагаемые – неотрицательные, включая равные 0, но это упростит взлом для криптоаналитика). Пусть $m = 239 = 123 + 71 + 45$. Тогда шифр c сообщения m равно:

$$c = 228159075 * 123 + 1022062272 * 71 + 259143894 * 45 = 112291462767$$

Рассмотрим процесс дешифрования. Алиса получает шифртекст $c = 112291462767$ и, используя вектор переменных $B = (2,3,5)$ и вектор модулей $N = (257, 263, 269)$, рассчитывает $c_i, i \in [1..3]$:

$$\begin{cases} c_1 = b_1 * c \bmod n_1 = 2 * 112291462767 \bmod 257 = 123 \\ c_2 = b_2 * c \bmod n_2 = 3 * 112291462767 \bmod 263 = 71 \\ c_3 = b_3 * c \bmod n_3 = 5 * 112291462767 \bmod 269 = 45 \end{cases}$$

Таким образом, учитывая значения матрицы K, уравнение (4) сводится к следующей системе уравнений:

$$\begin{cases} 1 * x_1 + 0 * x_2 + 0 * x_3 = 123, \\ 0 * x_1 + 1 * x_2 + 0 * x_3 = 71, \\ 0 * x_1 + 0 * x_2 + 1 * x_3 = 45, \end{cases} \quad (12)$$

которая обладает единственным решением. Алиса находит решение этой системы (14):

$$x_1 = 123, \quad x_2 = 71, \quad x_3 = 45.$$

Как видно, найденные слагаемые совпадают со слагаемыми, выбранными отправителем, а их сумма совпадет с исходным сообщением $m = 239$.

6 Криптоанализ разработанной системы защиты информации

Рассмотрим криптоанализ вышеуказанного метода. Криптоаналитику, осуществляющему попытку взлома криптосистемы, доступны открытый ключ – вектор $A = (a_1, \dots a_m)$ и мощность алфавита t, а также шифртекст c. Таким образом, криптоаналитику требуется найти необходимое решение диофантово уравнения (4). Диофантово уравнение (4), имеет счетно-бесконечное множество целочисленных решений, среди которых натуральных решений может быть ограниченное число, что сократит множество возможных вариантов для криптоаналитика и, соответственно, упростит для него процедуру взлома.

Рассмотрим данную проблему на следующем простом примере. Пусть в распоряжении криптоаналитика имеются вектор A с компонентами $a_1 = 20, a_2 = 15, a_3 = 24$ и шифртекст c, которые образуют следующее диофантово уравнение:

$$20\mathrm{x}_1 + 15\mathrm{x}_2 + 24\mathrm{x}_3 = 59 \quad (13)$$

Указанное диофантово уравнение (15) имеет следующее параметрическое решение:

$$\begin{cases} \mathrm{x}_1 = 1 - 3\mathrm{t} - 9\mathrm{s}, \\ \mathrm{x}_2 = 1 + 4\mathrm{t} + 4\mathrm{s}, \\ \mathrm{x}_3 = 1 + 0\mathrm{t} + 5\mathrm{s}, \end{cases} \quad (14)$$

Легко заметить, что единственное решение (16) в натуральных числах это $\mathrm{x}_1 = 1; \mathrm{x}_2 = 1; \mathrm{x}_3 = 1$, которое и будет искомым решением уравнения (15), и, соответственно, их сумма – искомое исходное сообщение $m = 3$. Таким образом, одно из необходимых условий надежности шифра – это наличие нескольких равновероятных решений в натуральных числах, суммы элементов которых различаются. Тем самым для криптоаналитика создастся неопределенность, связанная с диофантовыми трудностями.

7 Заключение

В работе разработана математическая модель системы защиты информации, основанная на линейном неоднородном диофантовом уравнении:

$$\sum_{\mathrm{i}=1}^{\mathrm{m}} \mathrm{a}_\mathrm{i} \cdot \mathrm{x}_\mathrm{i} = \mathrm{c},$$

Исходным сообщением служит некоторое решение данного диофантова уравнения, а шифртекстом – правая часть c. Представлен также метод нахождения этого решения, основанный на построении с использованием некоторой секретной информации системы уравнений, решение которой совпадает с требуемым решением исходного диофантова уравнения.

Разработанная математическая модель, несмотря на имеющиеся уязвимости, демонстрирует потенциал применения диофантовых уравнений для разработки систем защиты информации. В частности, они позволяют строить криптосистемы, допускающие существования множества равновероятных ключей, среди которых лишь один будет «истинным» ключом, а прочие будут «ложными».

В перспективе, данную модель можно обобщить на произвольную степень диофантова уравнения, что значительно усложнит проблему решения уравнения для аналитика.

Литература:

1. Shannon C. Communication theory of secrecy systems, Bell System Techn. J. 28, № 4 – 1949. P. 656-715.

2. Матиясевич Ю. В. Диофантовы множества // Успехи мат. наук. 1972. Т. 27, вып. 5. С. 185–222.

3. L.E.Dickson. History of the Theory of Numbers. vol.2. Diophantine Analysis. N.Y.1971.

4. Osipyan V.O. Mathematical modelling of cryptosystems based on Diophantine problem with gamma superposition method // SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks ACM, 2015. pp 338-341.

5. Osipyan V.O. Buiding of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems // ACM, 2012, pp.124-129.

6. Осипян, В.О. Моделирование ранцевых криптосистем, содержащих диофантовую трудность [Текст] / А.С. Арутюнян, С.Г. Спирина // Чебышевский сборник. 2010.Т. XI, вып. 1. с. 209–217.

7. Koblitz N. A Course in Number Theory and Cryptography. Springer-Verlag New York. 1987.

8. Саломаа А. Криптография с открытым ключом. М., 1995.

9. Shuhong Gao, Raymond Heindl. Multivariate public key cryptosystems from diophantine equations. Designs Codes and Cryptography 67(1):1-18 · April 2011

10. Harry Yosh. The key exchange cryptosystem used with higher order diophantine equations. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

11. C.H. Lin, C.C. Chang, R.C.T. Lee. A new public-key cipher system based upon the diophantine equations. IEEE Transactions on Computers (Volume: 44, Issue: 1, Jan 1995).

12. Старостенко И.Н., Сопильняк Ю.Н. Информационная безопасность / И.Н. Старостенко, Ю.Н. Сопильняк. – Краснодар: Краснодарский ун-т МВД России, 2012.

Остапенко В.С.
Центральный филиал
Российского государственного университета правосудия
Панферкина И.С., Мещерякова Е.И.
Воронежский институт МВД России
Кузнецова А.В.
Воронежский государственный университет

К ВОПРОСУ О СТАНОВЛЕНИИ ФРАКТАЛЬНО-ВИЗУАЛЬНОГО МЕТОДА В ПЕДАГОГИЧЕСКИХ ИССЛЕДОВАНИЯХ

В «Национальной доктрине образования Российской Федерации», определившей развитие системы образования до 2025 года, отмечается, что необходимо обеспечить ее приоритеты в государственной политике «с учетом современных достижений науки, систематического обновления всех аспектов образования, отражающих изменения в сфере культуры, экономики, науки, техники и технологий» [6]. Для реализации этой цели применяются инновационные подходы в педагогических исследованиях, основанные, в том числе, и на методах визуализации и фрактальной геометрии, синергетических закономерностях. Именно на междисциплинарном уровне, когда открытия в естественных науках непротиворечиво сопрягаются с новациями в гуманитарном познании, возможны прорывные направления в научно-педагогических исследованиях, ведущих к улучшению качества образования.

Современный мир наполнен визуальными (лат. visualis -- зрительный, англ.visibility - наглядный) образами. Поэтому визуально доступные для восприятия аспекты социального и природного мира являются предметом изучения многих социально-гуманитарных и естественных наук. Так, например, активно развивается визуальная социология, в фокусе которой визуальный образ представляет собой не только самостоятельный объект познания, но и средство познания социума в целом. Так, П.

Штомпка в своей работе «Визуальная социология» приводит перечень визуально доступных объектов и явлений (фотографии, рисунки и т.п.), которые являются предметом для социологического анализа посредством визуального метода [10].

Визуализация – это удобство, доступность и красота восприятия какого-либо объекта. И если этот объект обладает свойствами фрактальности – то это двойная эстетика и удобство зрительного отражения окружающих явлений. И обращение к педагогическим аспектам визуализации во взаимосвязи с фрактальностью возможно в контексте инновационных подходов в образовании, и в частности, с использованием теории фракталов. В педагогических исследованиях построение рисунков, схем по определенным правилам наглядности применяется давно, но каждый автор имеет свое представление о методике визуализации, а иногда опирается лишь на интуицию и здравый смысл. Поэтому есть смысл и необходимость упорядочить взгляды на эту давно знакомую проблему на основе предлагаемого фрактально-визуального метода.

Теорию фракталов (лат. fractus — дроблёный, сломанный, разбитый) в 1960-х годах разработал американский математик Бенуа Б. Мандельброт, который предложил новый взгляд на явления природы и закономерности развития общества на основе принципа самоподобия. Ученый по-новому интерпретировал фрактальные структуры применительно к конкретным познавательным аспектам естественнонаучного и гуманитарного знания. Пользуясь методами аналогии и компьютерной визуализации, Б.Б. Мандельброт описал способы отождествления многообразных математических и природных форм как фрактальных, посредством которых возможна диверсификация этого понятия на различные сферы знания, придание данному понятию междисциплинарного категориального статуса [4].

Геометрические фракталы наиболее зримо обладают свойством самоподобия, когда каждая мельчайшая часть структуры является подобной всей структуре в целом или же какой-либо более ее крупной части. Такие фракталы всегда являются наглядными, визуальными, т.к. сразу видна их самоподобность, не меняющаяся при изменении масштаба. Линейные фракталы обладают самоподобием в чистом виде – любая часть есть точная копия целого. Нелинейные фракталы обладают неточным самоподобием – в них часть есть не точная, а деформированная копия целого, что более приемлемо для социально-гуманитарного познания. Фрактальная геометрия не может быть не визуальной и в этом смысле фрактально-визуальный метод может быть применим во многих отраслях знания – от объяснения построения снежинки до развития экономических и образовательных систем и вселенной в целом. Таким образом, с помощью фрактально-визуального метода можно наглядно изобразить форму облака и модель формирования качеств личности. Например, самоподобие можно наблюдать в ветках деревьев и кустарников, снежинок, при исследовании экономических кризисов (волны Кондратьева), построении схематической модели образовательной системы и т.п. Все перечисленные объекты и другие, подобные им по своей структуре, можно визуализировать на основе фрактальности [7]. Для иллюстрации сказанного приведем примеры построения фракталов «Дерево», «Лист», «Снежинка» (рис. 1).

Рис. 1. Примеры построения фракталов «Дерево», «Лист», «Снежинка»

Принцип построения геометрических фракталов не сложен. Необходимо задать «основу» или «фрагмент», повторяющийся при каждом изменении масштаба. Затем разделять более крупную геометрическую фигуру на мелкие элементы, а те, в свою очередь, делить на аналогичные фигуры меньшего размера. Продемонстрируем это на примере фрактала «Гора» (рис. 2). Используя более крупные треугольники, дробим их на четыре мелких и затем повторяем эту процедуру снова и снова, пока не получится реалистичный горный ландшафт.

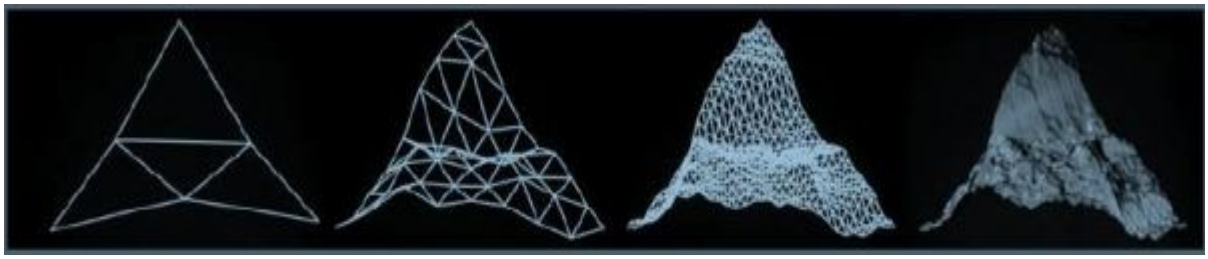


Рис. 2. Пример построения фрактала «Гора»

Таким образом, мы создаем фрактальный алгоритм для построения изображений, что можно применять при построении рисунков, схем в гуманитарных науках, изобразительном искусстве. Так, в работах кубистов можно найти фрактальные начала, а «Черный квадрат» Казимира Малевича – это геометрический фрактал как символ субъективного миропонимания. Можно предположить, что применение методологии фрактальных алгоритмов в различным отраслях знания поможет повысить не только наглядность и привлекательность предлагаемых разработок и идей, но и повысить их эффективность, активизировать внедрение на прорывных направлениях естественных и гуманитарных наук, искусства.

Основу фрактально-визуального метода, применяемого в социально-гуманитарном познании, на наш взгляд, может составить, например, «ковер» Вацлава Серпинского, предложенном польским ученым еще в 1915 году [9]. Фрактал «ковер Серпинского», представляет собой квадрат, который делится двумя горизонтальными и двумя вертикальными линиями на девять равных частей-квадратов, подобных исходному. Затем центральный квадрат выбрасывается, а к остальным восьми применяется та же процедура, и т.д. (рис. 3). Этот фрактал наглядно демонстрирует возможности фрактально-визуального метода для его реализации в социально-гуманитарных исследованиях в целом, и в педагогике, в частности, при построении, например, схем, рисунков, графиков, таблиц и т.п., усиливающих наглядную выразительность и требующих содержательного наполнения классических геометрических форм – квадратов,

прямоугольников, которые наиболее часто применяются в наглядных педагогических моделях.

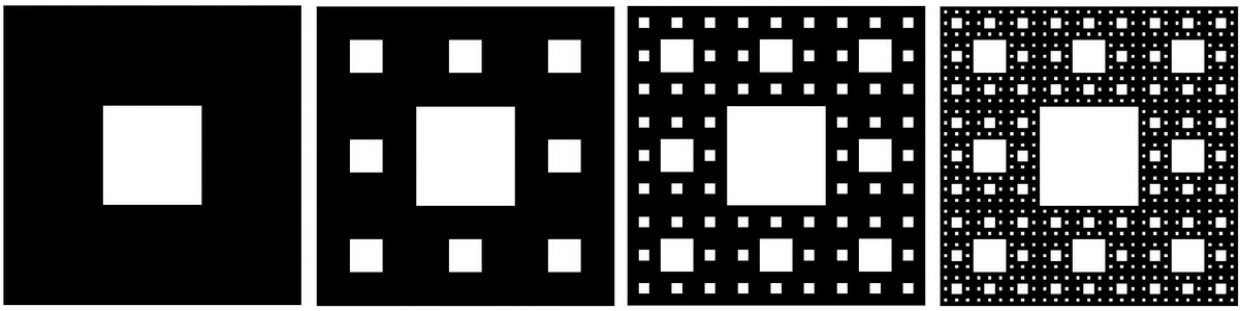


Рис. 3. Пример последовательного построения геометрического фрактала «Ковер Серпинского»

В современной науке фракталам уделяется большое внимание, так как множество природных и социальных феноменов обнаруживают фрактальные свойства. Безусловно, и в педагогике, применение фрактального принципа вполне реально. Сказанное позволяет обозначить контур смежной междисциплинарной проблемы: если теория фрактала широко используется в различных областях знания, то вполне обосновано и ее применение в социально-гуманитарном познании, и в частности, в педагогических исследованиях, для объяснения сущности понятий (образовательный процесс, система знаний, формы, методы обучения т.п.), которые наглядно позиционируются рисуночным, графическим и т.п. наглядными способами. Такое обращение к теории фракталов вполне оправданно, поскольку, разрабатывая предметную область применения фрактально-визуального метода в педагогических исследованиях, необходимо иметь в виду, что многие положения этой теории уже используются в педагогике и имеют практическое применение [2, 3, 5, 7, 8]. Так, авторы труда «Фрактальная педагогика: онтологические смыслы и методологические возможности» А.Г. Маджуга и И.А. Синицина, считают, что возможно применение фрактально-резонансного подхода, в рамках которого фрактальная педагогика дает возможность систематизировать и обобщить взгляды на теорию фракталов в различные исторические эпохи, объединить единичное, общее и всеобщее и обеспечить формирование фрактальной педагогики как научного концепта культуры и образования. Раскрывая сущность концептуально-теоретических основ фрактальной педагогики, авторы определяют ее как «парадигму современной педагогической науки, предметная область которой задана ее категориальной матрицей, где обучение, образование, самообразование, воспитание, самовоспитание, развитие и саморазвитие выступают в качестве самоподобных структур, имеющих нелинейный характер и функционирующих в соответствии с принципом резонанса, благодаря которому в атмосфере совместного бытия возникает мир отношений в диалоге с «Другим» и формируется конструктивно-творческая доминанта, преобразующая ресурсный потенциал личности в аспекте ее созидательной активности» [3]. В нашем случае, фрактально-визуальный метод соотносится с фрактальной педагогикой как частное с общим и дополняет, конкретизирует, расширяет ее понимание.

Таким образом, в педагогических исследованиях, по нашему мнению, фрактальные структуры с ярко выраженной визуализацией проявляют следующие свойства.

Во-первых, обладают нетривиальной структурой на всех масштабах, так как изменение масштаба не означает упрощение структуры, – она на всех шкалах сохраняет одинаково сложную картину исследуемого педагогического объекта.

Во-вторых, являются самоподобными или приближённо самоподобными, то есть, любая часть фрактального объекта похожа на весь объект в целом: часть снежинки – всей фигуре; отдельный квадрат в рисунке – всему рисунку и т.п.

В-третьих, имеют дробную метрическую размерность (иначе называемой фрактальным измерением), превосходящую топологическую и характеризующую уровень визуализации – слишком мелкий масштаб просто не воспринимается (он не виден), а слишком большой не имеет смысла в виду ограниченности носителя изображения (книга, альбом, слайд и т.п.).

В-четвертых, уменьшают энтропию, так как создают некоторый порядок в формах, до того считавшихся хаотическими, неупорядоченными. Мера хаоса (энтропия) существенно уменьшается в процессе построения фрактально-визуального объекта. В форме облака, в строении дерева или организации образовательного процесса можно найти измеряемые параметры – фрагменты, упорядочивающие хаос и ведущие к уменьшению энтропии.

Исходя из выщеуказанных достаточно жестких схем построения фрактальной наглядности может возникнуть вопрос: а не «загоняем» ли мы творческий процесс формирования, например, научного мировоззрения студентов, в «прокрусторово ложе» жесткой схемы, мало подверженной новациям? В данном контексте необходима разработка и теоретическое обоснование принципиально нового концепта «фрактально-визуальный метод исследования». В этом аспекте определённый интерес представляет точка зрения французских философов Ж. Делеза и Ф. Гваттари о том, что «фрактал являет собой первооснову коммуникации и выступает инновационной парадигмой, позволяющей в полной мере раскрыть абрис осмысления динамической рекурсии, координации эмоционально-эмфатической, когнитивной и знаковой модификации организма в языке ментальных репрезентаций как системе концептов и эмоциональной составляющей, представленной невербальными знаками» [1]. Если несколько упростить данный авторами научный конструкт, но использовать прямо их мысль о фрактале как «первооснове коммуникации», то фрактально-визуальный метод в педагогических исследованиях можно определить как поиск изначального фрагмента, элемента, на основе которого строятся подобные структуры разного масштаба, сохраняя общее сходство для большей наглядности и выразительности содержания, заключенного в рисунки, схемы, графики и т.п. Примерами такой фрактальной наглядности могут служить рисунки педагогических моделей, рассматриваемых в диссертационных исследованиях.

Построение модели формирования научного мировоззрения студентов начинается с выявления исходного фрактала – простого прямоугольника (квадрата), но далее возможно, а иногда и необходимо, отойти от жесткой схемы построения фрактала по типу «ковра Серпинского». Какие-то прямоугольники могут «выпадать», или наоборот «вписываться» в общую схему, исходя из необходимости содержательного насыщения фрактальной формы и поэтому это уже нелинейный фрактал, так как он построен не по жестким геометрическим правилам, а в соответствии со смыслом рисунка, схемы. Но соблюдение общих правил построения рисунка, в соответствии с фрактально-визуальным методом, предполагает создавать его на основе самоподобия, симметричности, наглядности, трансформируемости, внешней привлекательности, внутренней содержательности каждого фрагмента и всего объекта в целом, диалектичности формы и содержания. И что важно – наглядный педагогический фрактал – это всегда диалектика формы и содержания.

Следует отметить, что такие рисунки, включающие фрактальные структуры, в научных педагогических исследованиях используются довольно часто, но иногда без соблюдения элементарных правил их построения. Существенное нарушение, например, правила самоподобия, приводит к наглядному «дискомфорту», к потере приемлемой наглядности и частичной потере смысловой нагрузки рисунка.

Таким образом, применение фрактально-визуального метода в педагогических исследованиях представляет возможности:

- усилить привлекательную наглядность рисунков, схем, графиков и т.п., построенных по «законам фрактальной красоты» по аналогии с природными фракталами;

- показать относительную простоту изображения и доступность для любого пользователя (возможность строить самостоятельно, или вносить свои коррективы);

- выразить сжатое и логически обоснованное изложение смысла, заключенного в фигуры фрактальной геометрии;

- продемонстрировать относительную симметричность изображения, позволяющую оценить весь рисунок в целом через его логическую стройность и непротиворечивость;

- гармонизировать фрактальную форму и педагогическое содержание, что ведет к их единству, тесной взаимосвязи и способствует более глубокому усвоению представленного наглядного материала;

- реализовать возможность цветового решения фрактальных структур для их выразительности и привлекательности в визуальном аспекте;

- использовать философские категории, адаптированные к педагогическому конструктивному осмыслению: содержание и форма, единичное и общее, часть и целое, которые выражают логику и траекторию построения рисунка, схемы, графика;

- внедрить эстетику педагогических фракталов в сферу интересов научного сообщества, изучающего проблемы активизации исследований на «стыке» наук, позволяющих повысить эвристический потенциал гуманитарных дисциплин, и педагогики, в частности.

Переход образования к междисциплинарным взаимосвязям позволит решить проблему взаимного обогащения естественнонаучных и гуманитарных наук, обеспечить переход от классических схем одной науки к многообразию и переплетению полидисциплинарных методов исследования, том числе и на основе теорий фракталов и визуализации, что будет способствовать повышению эффективности и качества научных разработок, обучения и воспитания в образовательных организациях в целом. Резюмируя сказанное, можно констатировать, что интеграция методологии естественных и гуманитарных наук концептуализирует идеи фрактально-визуального метода, имеющего своими целями подготовку в образовательном процессе вузов специалистов высокой квалификации, востребованных в современных условиях.

Литература:

1. Делез Ж., Гваттари Ф. Что такое философия? / Ж.Делез, Ф. Гваттари. Серия: Философские технологии. Пер. С. Зенкин. – Москва, Изд-во: Академический Проект, 2009. – 261 с.

2. Маджуга А. Г. Концептуально-теоретические основы фрактальной педагогики как новой области социально-гуманитарного знания / А.Г. Маджуга, И.А. Синицина, Е.В. Филипенко // Научный диалог. – 2015. – № 12 (48). – С. 450–159.

3. Маджуга А. Г. Фрактальная педагогика: онтологические смыслы и методологические возможности: монография / А.Г. Маджуга, И.А. Синицина. – Стерлитамак: Изд-во СФБашГУ, 2015. – 365 с.

4. Мандельброт Б.Б. Фракталы и хаос: множество Мандельброта и другие чудеса / Б.Б. Мандельброт. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2009. – 392 с.

5. Михайленко, Е.В. Дискретная математика: учеб. пособие / Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2016. – 104 с.

6. О национальной доктрине образования в Российской Федерации: Постановление Правительства РФ от 04.10.2000 №751 [Электронный ресурс]. – URL: http://www.karavella.nios.ru/DswMedia/nacional-nayadoktrinaobrazovaniyavrf.pdf (дата обращения: 5.06.2018).

7. Перерва Л.М., Юдин В.В. Фрактальное моделирование: учебное пособие / под общ. ред. В.Н. Гряника. – Владивосток: Изд-во ВГУ ЭС, 2007.– 186 с.

8. Самкова М. А. Фрактальная модель учебно-педагогического дискурса / М.А. Самкова // В мире науки и искусства: вопросы филологии, искусствоведения и культурологии: материалы XXIX междунар. науч.-практ. конф. – Новосибирск : НП «СибАК», 2013. – № 9 (28). – С. 86–91.

9. Серпинский В. Пифагоровы треугольники./ В. Серпинский – Москва: Учпедгиз, 1959. – 111 с.

10. Штомпка П. Визуальная социология. Фотография как метод исследования: учебник. – Москва: Логос, 2010. – 213 с.

11. Старостенко И.Н. О некоторых аспектах оптимизации образовательного процесса с использованием информационных технологий // Математические методы и информационно-технические средства: Труды всероссийской научно-практической конференции, 23 июня 2006 г. – Краснодар: Краснодарский университет МВД России, 2006. – С. 183-189.

Петрищева Е.Н., Карпика А.Г.
Ростовский юридический институт МВД России

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ И БЕЗОПАСНОСТИ РОССИЙСКОГО СЕГМЕНТА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Человеческая цивилизация активно переходит к новому этапу своего развития – информационному обществу, которое характеризуется увеличением роли информации, знаний, информационных технологий в жизни общества, а также высокой скоростью коммуникационных процессов. Изменения, происходящие во всех сферах общественной жизни, приводят к появлению экономики, ориентированной на высокие технологии, электронной демократии и электронного государства, социальных сетей, сообществ и других явлений, присущих данному этапу развития общества.

Развитие информационных технологий и глобальной сети «Интернет» предоставили новые возможности пользователям, которые получили возможность свободно обмениваться информацией, качать с торрентов любую информацию: программное обеспечение, видеоигры, кино, музыкальные и литературные произведения, размещать в сети любую информацию, общаться в социальных сетях.

В мире существует три модели государственного регулирования Интернета [13]:

1. Европейская (континентальная) модель – отраслевые регуляторы имеют высокую долю самостоятельности, однако при этом работают в связке с государством для того чтобы обеспечить соблюдение интересов всех заинтересованных сторон, личная инициатива имеет жесткую регламентацию со стороны законодательства, а на первое место выдвигается развитие услуг по функциональному и практическому информированию граждан (например: в Швейцарии стимулируются социальные программы; во Франции – техническое обеспечение).

2. Англоамериканская – где контроль государства минимальный, приоритет частной инициативы, полная либерализация рынка информационных технологий, очень гибкое законодательство или его отсутствие, информационные технологии ориентированы в основном на развлечения.

3. Азиатская – абсолютный контроль государства, которое принимает участие в обеспечении крупных вложений в развитие информационных технологий.

Отсюда и возникают проблемы правового регулирования глобальной сети «Интернет», а именно [13]:

1. Отсутствие единого нормативного правового регулирования;

2. Отсутствие правовой основы разноуровневой интеграции информационного пространства: мировой, региональной и пространной;

3. Необходимо создание центра формирования единого информационного пространства;

4. Необходим полноценный мониторинг единого информационного пространства;

5. Необходима сертификация информационных продуктов и деятельности субъектов;

6. Необходимо установление ответственности за формирование единого информационного пространства;

7. Необходимо законодательное ограничение информационной экспансии.

В связи с этим стоит отметить, что попытки государственного регулирования Интернета – общемировой тренд. Российское законодательство то же претерпело некоторые изменения, поскольку на протяжении нескольких последних лет Россия занимает первое место в Европе по количеству пользователей интернета. По оценке специалистов в 2017 год аудитория пользователей интернета в России составила 87 млн. человек (71 %). За год российская интернет-аудитория по данным Mediascope увеличилась на 2%. При этом 66 млн. человек, или 54 % от населения РФ, пользуются интернетом хотя бы 1 раз в месяц через мобильные устройства, а 20 млн. человек – 16% от населения страны – только с мобильных устройств.

Быстрее всего растет аудитория на смартфонах: по состоянию на 2017 год 46% населения страны заходят в интернет со смартфонов – прирост составил 15% за год.

Согласно прогнозу экспертов, в 2020 году беспроводной доступ в Интернет покроет 85% планеты, количество подключенных к нему устройств, превысит 50 миллиардов. К 2041 году пропускная способность сетей увеличится в 500 раз.

Поэтому в 2016-2017 годах Государственная дума приняла целый ряд неоднозначных законов, которые могут серьезно осложнить жизнь российского сегмента информационно-телекоммуникационной сети «Интернет» (Рунета).

Наибольший резонанс в области регулирования конфиденциальности информации в сети «Интернет» вызвал Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [14], так называемый «пакет Яровой», который фактически отменил приватность по умолчанию в сетевом пространстве.

Данный Федеральный закон был принят большинством депутатов и подписан президентом, несмотря на достаточно громкий протест общественности и предупреждения о серьезных противоречиях положений законопроекта Конституции РФ, запрещающей без судебного решения прослушивать и сбирать информации о частной жизни гражданина.

Внедрение положений данного закона будет поэтапным, т.е. может происходить по региональному принципу, по типам операторов связи, по составу хранения данных или другим принципам. Вице-премьер РФ Аркадий Дворкович отмечал, что «есть общее согласованное мнение правительства, что нужно поэтапно с 1 июля 2018 года вводить определенные требования данного закона.

Федеральный закон от 23 июня 2016 г. № 208-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Кодекс Российской Федерации об административных правонарушениях». Федеральный закон вступил в силу с 1 января 2017 г. [1], в котором прописаны особенности

распространения информации новостными агрегаторами. До размещения общественно значимых сведений, владелец новостного агрегатора, обязан проверить их достоверность.

Роскомнадзору поручено вести реестр новостных агрегаторов. Согласно поправкам владельцем новостного агрегатора может быть только российское юридическое лицо или гражданин нашей страны [2].

Федеральный закон от 3 июля 2016 г. № 244-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации» (так называемый «Налог на Google») вступил в силу с 1 января 2017 года. Западные компании должны будут зарегистрироваться в системе Федеральной налоговой службы (ФНС) и платить налоги (в размере 18%) наравне с российскими операторами.

Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации» (вступил в силу с 1 ноября 2017 года) [9].

Новым законом устанавливается запрет на использование информационных систем и программ для получения доступа к интернет-ресурсам, заблокированным в России. Под действие закона попадают не только прокси- и VPN-сервисы, но и анонимные сети, такие как Tor и I2P. Кроме того, документ запрещает поисковым системам вроде Google и «Яндекс» выдавать ссылки на заблокированные ресурсы.

Федеральный закон от 01.07.2017 № 156-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" (т.н. закон о блокировке копий сайтов «зеркал», вступил в силу с 1 октября 2017 года) [10]. Законом определяется порядок ограничения доступа к «зеркалам» пиратских сайтов.

Федеральный закон от 29.07.2017 № 241-ФЗ "О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» (так называемый закон о Интернет-мессенджерах) должен вступить в силу с 1 января 2018 года [8].

Закон вводит понятие организатора обмена мгновенными сообщениями (мессенджера) и возлагает на него обязанность обеспечивать передачу сообщений только тех пользователей, кто идентифицирован в установленном правительством порядке.

Закон предлагает осуществлять идентификацию пользователей с использованием абонентского номера на основании договора об идентификации, заключаемого мессенджерами с оператором связи. При этом устанавливается, что мессенджеры, которые являются российскими юридическими лицами или гражданами РФ, вправе осуществлять идентификацию пользователей самостоятельно путем определения абонентского номера, без заключения договора.

Также отмечается, что «наряду с обязанностями по идентификации на мессенджеры возложены обязательства по обеспечению технической возможности отказа пользователей от получения электронных сообщений от других пользователей, обеспечению возможности рассылки электронных сообщений по инициативе органов государственной власти, а также ограничению рассылки и передачи сообщений, содержащих информацию, распространяемую с нарушением требований законодательства РФ».

В случае неисполнения мессенджерами требований об ограничении рассылки сообщений, содержащих информацию, распространяемую с нарушением требований законодательства РФ, предусматривается возможность ограничения доступа к мессенджеру.

В конце июня 2017 года Telegram оказался на грани блокировки в России после отказа предоставить Роскомнадзору сведения для внесения в «реестр организаторов распространения информации». Однако после публичной дискуссии Telegram все же

дал необходимую информацию – регистрационные данные компании (о доступе к переписке пользователей речь не шла).

В октябре мировой суд оштрафовал Telegram на 800 тысяч рублей за отказ предоставить ФСБ информацию для декодирования сообщений, Мещанский суд Москвы, как апелляционная инстанция, признал это решение законным. По заявлению адвоката, штраф назначен за отказ Telegram представить спецслужбам информацию для декодирования переписки обвиняемых в теракте в Санкт-Петербурге. Адвокаты пояснили в суде, что на запрос ФСБ Telegram не отреагировал, посчитав его незаконным и технически неисполнимым, кроме того были основания сомневаться в законности запроса ФСБ потому что компания находится на территории иностранной юрисдикции.

В апреле 2018 года Роскомнадзор обратился в Таганский суд города Москвы с требованием заблокировать мессенджер Telegram на всей территории России из-за нежелания создателя Telegram Павла Дурова сотрудничать с российскими властями и предоставить ФСБ ключи шифрования. Суд принял решение о блокировке мессенджера. После чего операторам связи была направлена информация об ограничении доступа к Telegram. В течение нескольких дней под блокировку попали миллионы IP-адресов Amazon, Google и других компаний, что привело к сбоям в работе целого ряда сайтов и сервисов и лишь незначительно повлияло на работоспособность и посещаемость Telegram. Позднее часть IP-адресов была разблокирована. За месяц с небольшим, прошедший с момента блокировки Telegram, Роскомнадзор ограничил доступ к 80 прокси и VPN-сервисам [11].

По словам представителей Роскомнадзора, все попавшие под блокировку сервисы были специально созданы для обеспечения доступа к Telegram. При этом 10 VPN- и прокси-сервисов были разблокированы после того, как перестали давать возможность обойти блокировку Telegram.

Между тем блокировка Telegram в России привела к значительному росту популярности зарубежных VPN-сервисов.

Следующий Законопроект о регулировании критической инфраструктуры Рунета Министерством связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [6]. Законопроект предусматривает внесение изменений в закон «О связи» и призван обеспечить «целостность, непрерывность, стабильность, устойчивость и защищенность функционирования российского национального сегмента» интернета, говорится в пояснительной записке. В документе вводится понятие «критической инфраструктуры интернета», к которой ведомство отнесло национальные домены зоны.ru и .рф, точки обмена трафиком, все автономные системы, которыми владеют как юридические, так и физические лица.

Министерством связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) предложило также создать государственную информационную систему (ГИС) обеспечения целостности, устойчивости и безопасности функционирования российского сегмента интернета. Новая система будет работать на основе «программных, технических средств и информационных технологий, обеспечивающих сбор, обработку, хранение, предоставление, размещение и использование информации о критических элементах» рунета, а также информации о его интеграции «с международными сетями связи, а также маршрутно-адресной информации в сетях передачи данных и российской части сети «Интернет». Законопроект выполняет поручения президента Владимира Путина по итогам заседания Совета безопасности двухлетней давности, который поручил принять меры, которые бы обеспечили устойчивость рунета, в случае отключения российского сегмента интернета от внешнего мира. Документ является рамочным и практически не содержит деталей регулирования элементов критиче-

ской инфраструктуры, эта часть будет прописываться на уровне подзаконных актов правительства.

В ноябре 2017 года Министерство экономического развития РФ подготовило отрицательное заключение на разработанные Министерством связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) поправки в федеральный закон «О связи», которые вводят дополнительное регулирование инфраструктуры российского сегмента интернета. «С учетом изложенного на основе проведенной оценки регулирующего воздействия проекта акта Минэкономразвития России сделан вывод об отсутствии достаточного обоснования решения проблемы предложенным способом регулирования» [17].

В мае 2017 года Президент Владимир Путин подписал указ, утверждающий «Стратегию развития информационного общества в РФ на 2017–2030 годы» [16]. Стратегия сводится к стремлению властей как можно больше использовать российские технологии и расширить государственный контроль в интернете.

Кроме того, в тексте документа предлагается принять меры, исключающие анонимность пользователей сети и их «безответственность и безнаказанность». Также планируется создание специальной системы, гарантирующей «личную безопасность пользователей, конфиденциальность их информации» [16].

Безопасным следует считать только те программы и сервисы, которые получат сертификат ФСБ. Надо осторожнее относиться к программам и сервисам, которые управляются из-за рубежа, зависят от принудительных обновлений и собирают информацию о пользователях. И лучше вообще заменить все российскими аналогами. Особенно это касается программ и алгоритмов шифрования данных. Телефоны тоже лучше делать российские.

Нужно добиться, чтобы в российском информационном пространстве распространялась «достоверная и качественная информация российского производства».

Рунет обезопасят от выключения иными государствами. Для этого в 2018 году в российском законодательстве будет зафиксирован статус и описана схема работы российского сегмента информационно-телекоммуникационной сети (Рунета). Технически устранить возможность отключения России от интернета планируется к 2021 году. Об этом говорится в проекте программы «Цифровая экономика» [15]. Это документ, подготовленный межведомственной рабочей группой при Минкомсвязи, направлен весной 2017 года в правительство и утвержден распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р.

Для защиты рунета запланирован ряд организационных мероприятий. В 2018 году будет законодательно закреплен правовой статус российского сегмента сети интернет, его инфраструктуры (реестр адресов, маршрутно-адресной информации, корневых серверов), а также порядок финансирования и функционирования Рунета.

По мнению российских чиновников, ограничение интернета в России, как в Китае, позволит обеспечить информационную безопасность страны, и что китайский вариант – правильный путь развития для данного направления. Система, созданная властями Китая, позволяет блокировать как отдельные сайты, так и определенные поисковые запросы. «Китай менее щепетилен к мнению общества, они оценили угрозу и ограничили интернет. Теперь у них таких проблем нет», – сказал Герман Клименко, советник президента РФ по вопросам развития интернета [7].

По данным Всероссийского центра изучения общественного мнения (ВЦИОМ), идею отдельного интернета для России поддерживает 81% населения России. При этом 58% одобряют создать альтернативную сеть со странами БРИКС (Бразилия, Россия, Индия, Китай, Южно-Африканская Республика). Еще 23% считают, что оптимальным

вариантом был бы полностью изолированный от внешнего мира интернет, существующий лишь в границах самой России [12].

Каждый четвертый из поддержавших эту идею «затруднился ответить» о причинах своего решения. Среди тех, у кого объяснения есть, большинство (49%) сослались на то, что отдельный интернет «повысит уровень безопасности» в стране и станет «лучшей защитой от международных хакеров» [12].

Объекты критической информационной инфраструктуры России в 2017 году подвергались атакам около 70 миллионов раз, большинство компьютерных атак были из-за рубежа. Представитель центра безопасности связи ФСБ Николай Мурашов отметил, что «в настоящий момент, с точки зрения развития средств защиты информации, РФ обладает достаточным потенциалом».

Сегодня интернет сильно изменился, изменилось и отношение к нему государства, в том числе и отношение к регулированию национального домена. Государство принимает гораздо более активное участие в управлении национальными доменами .RU и .РФ. Интернет не может быть местом «расхристанной квазисвободы», где бесконтрольно распространяется любая информация, сказал президент России Владимир Путин, выступая на медиафоруме Общероссийского народного фронта [5]. Российский сегмент интернета должен быть устойчивым к разного рода атакам. Для этого власти должны контролировать инфраструктуру и следить за ее безопасностью. Хорошо это или плохо покажет время, а пока тенденция введения очень жесткого регулирования отрасли наблюдается во многих странах мира.

Литература:

1. Новостным агрегаторам смягчили условия существования / http://www.comnews.ru/node/102353.

2. Федеральный закон от 23 июня 2016 г. № 208-ФЗ "О внесении изменений в Федеральный закон «"Об информации, информационных технологиях и о защите информации" и Кодекс Российской Федерации об административных правонарушениях» / http://www.garant.ru

3. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2017) / http://www.consultant.ru

4. Интернет меняется, меняется и отношение государства к нему / http://www.tadviser.ru/index.php

5. Конец «расхристанной квазисвободы» в интернете / http://www.bbc.com/russian/news-39480727.

6. Минкомсвязи представило законопроект о регулировании Рунета / http://www.forbes.ru/news/332621

7. Советник Путина предложил ограничить интернет, как в Китае / http://www.trud.ru/article/26-01-2017/1346319

8. Госдума приняла закон о регулировании мессенджеров / https://ria.ru/society/20170721/1498890579.html

9. Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации» / http://www.consultant.ru

10. Федеральный закон от 01.07.2017 № 156-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"» / http://www.consultant.ru

11. Роскомнадзор заблокировал 80 VPN-сервисов в борьбе с Telegram / https://hitech.newsru.com/article/21may2018/rkn_vpn

12. Путина заявили о готовности России к отключению от Интернета / https://inforesist.org/otklyucheniyu-ot-interneta/

13. Государственное регулирование Интернета за рубежом / http://oplib.ru/random/view/222704

14. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» / http://www.consultant.ru

15. Петрищева Е.Н., Лемайкина С.В. Правовые аспекты государственного регулирования «Рунета» // Юристъ-Правоведъ, 2017, № 3 (82). С. 177-183.

16. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» / http://www.garant.ru

17. Министерство экономического развития РФ выдало отрицательное заключение на законопроект Минкомсвязи о дополнительном регулировании рунета / http://orv.gov.ru/Content/Item?n=27356

Петров С.А., Васин О.И., Щербаков В.А.
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

ОСОБЕННОСТИ ПЕРЕДАЧИ ДАННЫХ В МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ ПРИ «СТАТИСТИЧЕСКОМ» И «ЛАВИННОМ» МЕТОДАХ МАРШРУТИЗАЦИИ

На сегодняшний день широко применяются два метода маршрутизации: статистический, представленный в работе технологией многопротокольной коммутации с помощью меток MPLS (MultiProtocol Label Switching) [1], и лавинный, представленный протоколом OSPF (Open Shortest Path First – выбор кратчайшего пути первым) [2].

Оба метода реализуют два принципиально разных подхода к формированию маршрута передачи данных: «статистический» метод полагается на накопленную статистику соединений, а «лавинный» – задействует рассылку данных от «соседа» к «соседу» в поисках оптимального маршрута без накопления статистики. В связи с этим, можно предположить, что в условиях выхода элементов сети из строя (внешних деструктивных воздействий), когда статистика соединений отсутствует, «статистический» метод будет показывать худший результат по сравнению с «лавинным».

Полученные в статье «Анализ влияния методов маршрутизации на объем доступных сетевых ресурсов» [3] теоретические результаты подтверждают это предположение. Выводы статьи [3] утверждают, что в условиях внешних деструктивных воздействий, при которых примерно 30% сетевых ресурсов МСС выходит из строя, целесообразнее применять «лавинный» метод формирования ПРИ по сравнению со «статистическим» методом.

С целью подтверждения (либо опровержения) актуальности приведенных теоретических выводов представляется интерес провести опыт моделирования МСС в свободно распространяемой программной среде имитационного моделирования Graphical Network Simulator 3 v 1.4 (GNS3) [4].

Сопоставительный анализ «статистического» и «лавинного» методов маршрутизации проводится на примере работы протоколов MPLS и OSPF в условиях внешних деструктивных воздействий на элементы МСС имеющей структуру «ячеистого» типа, состоящей из одного сервера (Server), десяти маршрутизаторов (Router1 ÷ Router10), пяти локальных сетей (LAN 1 ÷ LAN 5).

При этом каждая локальная сеть организована на базе технологии Fast Ethernet, на транспортном уровне поддерживается протоколами TCP и UDP, в своей структуре содержит 10 компьютеров, подключаемых к коммутаторам по принципу топологии «звезда» и генерирует трафик видеоконференции (Video Conferencing, VC). Трафик видеоконференции будет генерироваться со следующими произвольно выбранными параметрами: скорость 1350 Кбит/сек., размер кадра 128*120 пикселей, частота 10 кадров/сек., разрешение 9 бит на пиксель.

В программе GNS3 в качестве сервера будет выступать виртуальный сервер, созданный в программном продукте виртуализации Virtual Box от компании Oracle на базе операционной системы Windows Server 2012 R2.

Исходная структура анализируемой мультисервисной сети связи, построенная в программе GNS3, представлена на рис. 1.

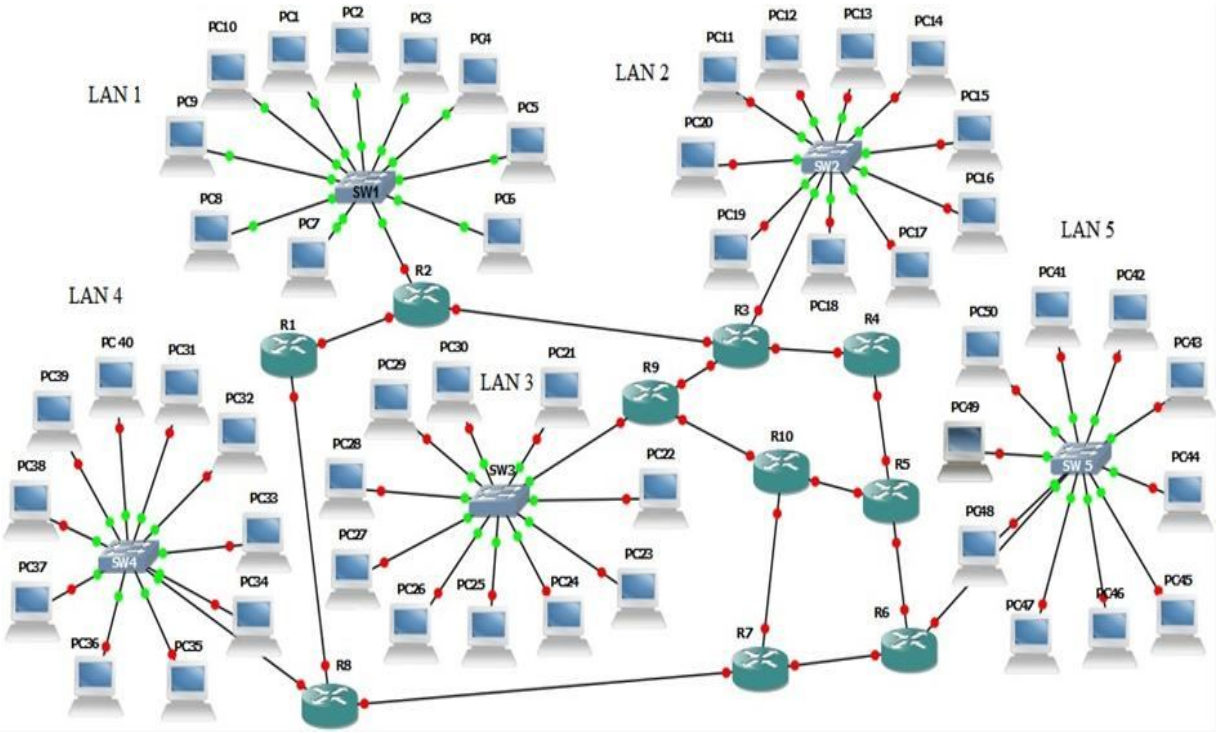


Рис. 1. Исходная структура анализируемой мультисервисной сети в программе GNS3

Процесс исследования влияния внешних деструктивных воздействий на элементы МСС подразумевает под собой череду испытаний имитационного моделирования. В одном испытании сеть функционирует в течение получаса. Первые 5 минут сеть работает в штатном режиме, т.е. в отсутствии внешних деструктивных условий, когда все маршрутизаторы сети находятся в рабочем состоянии. На 5-ой, 10-ой и 15-ой минутах опыта моделирования последовательно выводятся из строя, соответственно, 9-ый (Router9), 5-ый (Router5) и 6-ой (Router6) маршрутизаторы (см. рис.1). Маршрутизаторы соединены сетевым кабелем с одинаковой, заранее определенной в каждом испытании пропускной способностью r = 1 Гбит/с, r = 100 Мбит/с и r = 10 Мбит/с. Таким образом, последовательный вывод из строя маршрутизаторов и постепенное снижение пропускной способности сетевого кабеля имитирует процесс внешнего деструктивного воздействия.

В каждом испытании маршрутизаторы поддерживают только один из двух протоколов: OSPF либо MPLS. Сценарий 30-ти минутного испытания одинаков для обоих протоколов.

Внешние деструктивные воздействия уменьшают общий сетевой ресурс R_0. В данном случае под сетевым ресурсом понимается совокупность всех пропускных способностей кабелей r, соединяющих маршрутизаторы между собой. Таких кабельных соединений в анализируемой структуре сети на момент начала проведения испытания 12. По итогу проведения опыта имитационного моделирования общий сетевой ресурс сократится вдвое, а анализируемая структура сети поменяет свой тип с “ячеистой” на “линейную”.

Результатом одного испытания имитационного моделирования является $N_{\text{потерь}}$ – количество потерянных пакетов VC за единицу времени.

На рис. 2 – 4 представлены результаты описанного выше опыта имитационного моделирования анализируемой МСС с поддержкой протоколов MPLS и OSPF (в отдельных испытаниях) в программном продукте GNS3 при пропускных способностях сетевого кабеля
r = 1 Гбит/с, r = 100 Мбит/с
и r = 10 Мбит/с.

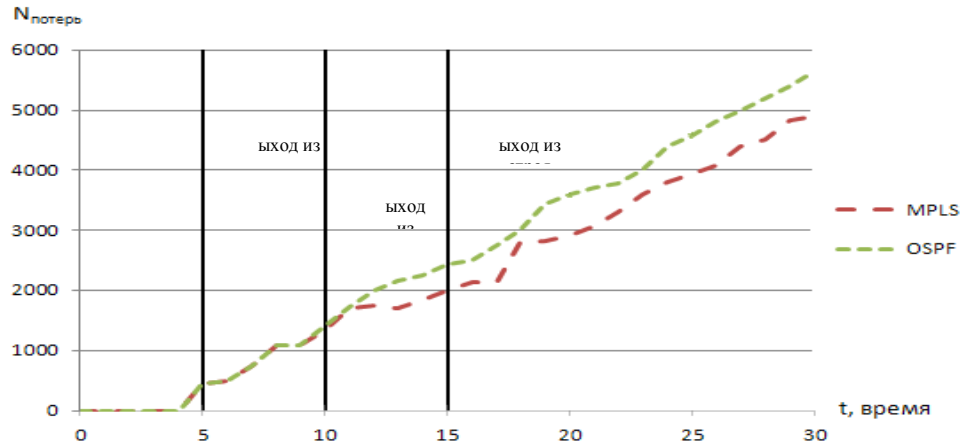


Рис. 2. Пропускная способность r = 1 Гбит/с

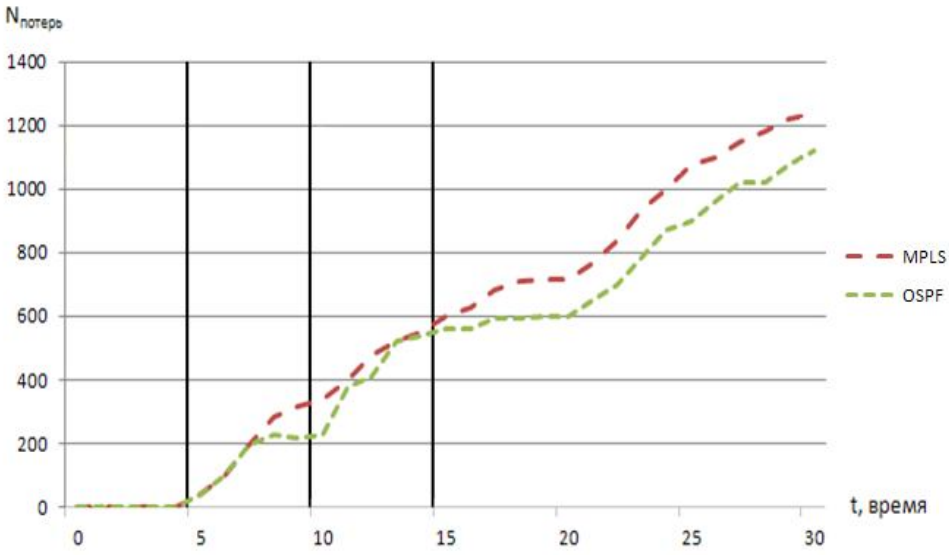


Рис. 3. Пропускная способность r = 100 Мбит/с

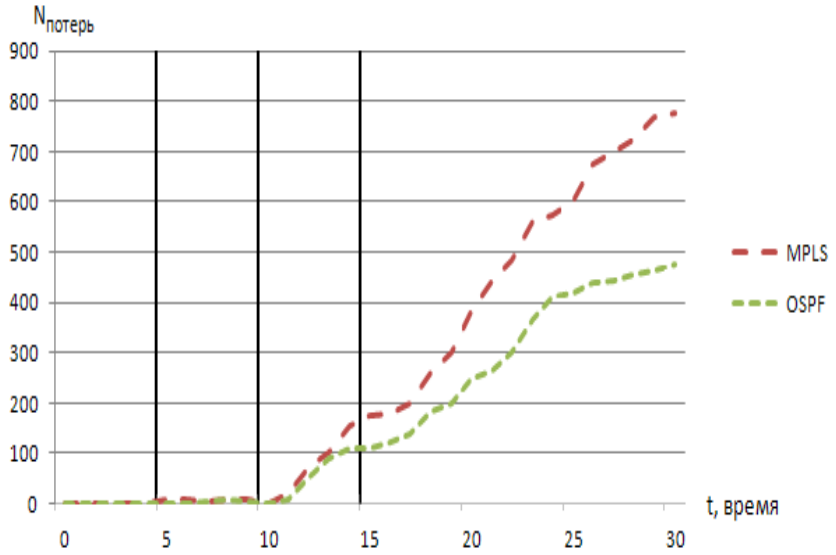


Рис. 4. Пропускная способность r = 10 Мбит/с

Рассчитаем значение коэффициента неопределенности состояния сетевых ресурсов *x* (степень недоступности общих сетевых ресурсов анализируемой сети) по следующему правилу:

$$x_i = \frac{R_0 - R_0^{(i)}}{R_0}; i = \overline{1,4}.$$

Опустим индекс *i* при x_i и проведем нормирование результатов моделирования:

$$\overline{N} = 1 - \frac{N_{\text{потерь}}}{N_{\text{потерь (max)}}^{(j)}}; j = \overline{1,3}$$

где $N_{\text{потерь (max)}}^{(j)}; j = \overline{1,3}$ – максимальное значение $N_{\text{потерь}}$ в каждом из трех испытаний имитационного моделирования.

Полученные результаты расчетов представлены на рисунках 5–7.

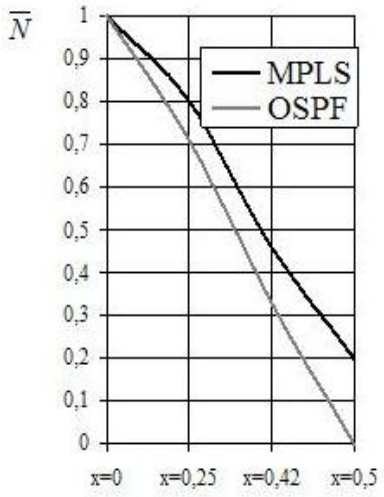


Рис. 5. Нормированные результаты моделирования в GNS3 v 1.4 при *r* = 1 Гбит/с

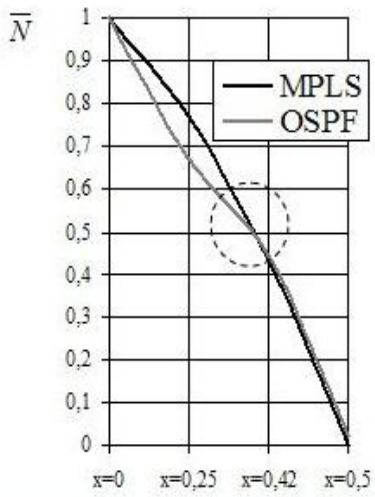


Рис. 6. Нормированные результаты моделирования в GNS3 v 1.4 при *r* = 100 Мбит/с

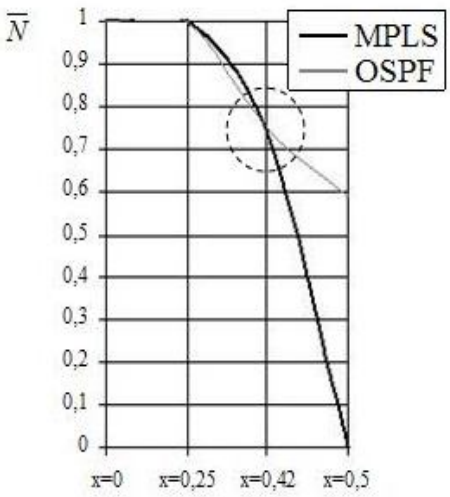


Рис. 7. Нормированные результаты моделирования в GNS3 v 1.4 при *r* = 10 Мбит/с

Результаты испытаний показали, что в условиях внешних деструктивных воздействий, при которых примерно 40% сетевых ресурсов МСС выходит из строя, целесообразно применять «лавинный» метод формирования ПРИ по сравнению со «статистическим», что фактически подтверждает теоретический вывод, полученный в источнике [3].

Литература:

1. RFC 3031. Multiprotocol Label Switching Architecture, January 2001.
2. RFC 5340. OSPF for IPv6, July 2008.
3. Новиков, С.Н. Анализ влияния методов маршрутизации на объем доступных сетевых ресурсов / С.Н. Новиков, А.А. Буров // Науч.-техн. ведомости СПбГПУ. – 2009. – С. 41-47.
4. GNS3. The software that empowers network professionals. Внутренний ресурс официального сайта компании GNS3 Technologies. [Электронный ресурс]. URL: https://community.gns3.com/software (дата обращения: 3.02.2017).

Пидшморг Ю.В., Кучерук Д.А.
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

ИНФОРМАЦИОННЫЕ ОТНОШЕНИЯ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Информационное пространство – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию [2].

Современное информационное общество представляет собой социальную общность, в которой основным предметом труда выступают информация и знания, а в качестве орудия труда используются информационные технологии. Отличительной особенностью информационного общества выступает повсеместная информатизация – процесс создания, накопления и использования информационных ресурсов, который, в свою очередь, предполагает формирование оптимальных социально-экономических и организационно-технических условий, способствующих удовлетворению информационных потребностей членов общества, органов государственной власти и местного самоуправления, организация, общественных объединений. Взаимоотношения индивидов в подобном обществе определяются как информационные, так как именно информация в нем выступает главным условием стратегической устойчивости, стабильности, развития и процветания.

Информационные отношения – непрерывный процесс и результат обращения членов общества к разнообразным источникам информации, а так же их взаимодействие в процессе информационного обмена, который затрагивает практически все сферы жизнедеятельности современного человека: экономическую, политическую, духовную, культурную. Индивиды «окованы» множеством информационных связей, что, с одной стороны, выступает объективной необходимостью, позволяя экономить время и оперативно действовать в режиме многозадачности, а с другой – делает человека информационно-зависимым на уровне биологической потребности.

На основе анализа тенденций развития информационных отношений в современном обществе, авторами были выделены их проблемные характеристики, а так же предложена концепция благоприятных перспектив развития информационных отношений с учетом долгосрочных интересов общества в целом.

Первой проблемной особенностью информационных отношений в современном информационном пространстве авторы отмечают то обстоятельство, что сознание человека перегружено объемами информации, выходящими за рамки физических возможностей восприятия. Информационные связи такого человека неуклонно растут, так как он находится в постоянном поиске актуальной для себя информации. При этом, немаловажное значение с точки зрения исследовательского интереса имеет именно ролевая характеристика индивида в коммуникативном процессе: на первый взгляд индивид выступает активной стороной данного процесса, так как добровольно инициирует обращение к источникам информации. То есть, индивид выполняет роль активного субъекта коммуникативного взаимодействия. В свою очередь, источники информации, в частности, средства массовой коммуникации, давно и прочно заняли активную позицию по реализации в современном обществе учебно-воспитательно-поучительных функций, отодвинув на второй план в этом процессе семью, религию, ближайшее окружение. Таким образом, информационно-зависимый человек выступает уже не субъектом коммуникативного процесса, а, напротив, объектом воздействия субъективных интересов стороны, формирующей и транслирующей множественные информационные потоки.

Второй проблемной характеристикой информационных отношений авторы отмечают высокий уровень зависимости современного человека от мнения окружающих и отсутствие объективного понимания последствий этой зависимости. Люди бояться быть непринятыми обществом и себе подобными, поэтому всеми возможными способами человек старается «закрепиться» в социуме, утвердить в нем свои позиции и не быть отчужденным «своими». Роль средств массовой коммуникации в этом процессе заключается в том, что они порционно выдают необходимые для человека подсказки: что говорить, смотреть, слушать, носить, где учиться, работать, отдыхать, чтобы не отличаться от принятых в данном конкретном обществе норм. Если индивид соответствует заданным жизненным «стандартам», то он «свой», если же нет, то «чужой». В свою очередь, человек старается соответствовать введённым критериям актуальности и сопричастности своим социальным сообществам.

Миллионы людей добровольно включаются в виртуальные сообщества, «живут» в иллюзорных мирах, не имеющих ничего общего с реальностью, но в которых гораздо легче самореализоваться, самовыразиться и достичь псевдопризнания и псевдоуважения нереальной общественности. Эти псевдомиры подавляют потребность реального, живого общения, человек становится частью виртуального мира, построенного по принципу информационного порабощения, управляемого вполне реальными людьми [5].

Таким образом, авторы подошли к формулировке третьей проблемной особенности современных информационных отношений: через средства массовой коммуникации транслируются и латентно насаждаются интересы субъектов, формирующих и транслирующих информационные потоки. К ним можно отнести любые общественные структуры, группировки, личности, воздействующие на сознание широких слоев населения в целях достижения собственных корыстных интересов – от идеологического доминирования (субъекты информационного воздействия – духовные лидеры, общественные и политические деятели, олигархи, представители бизнес-элиты) до пропаганды (явной или скрытой) социально-опасных явлений, разрушающих общество [5]:

- насаждение западных приоритетов (жажда наживы, гедонизм, тотальное потребительство, приоритет материальных ценностей над духовными);
- разрушение системы традиционно российских ценностей (приоритет семьи, уважение к старшим, сохранение традиций и генетической памяти);
- раскол православной церкви, разрушение идеологии (духовное уничтожение личности);

- моральное растление молодежи (низкий уровень воспитания и образованности);
- насаждения идеи никчемности широких масс населения (пропаганда идеи «места под солнцем для сверхлюдей»).

Субъектами такого информационного воздействия могут выступать недружественные государства, иностранные организации, незаконные вооруженные формирования, экстримистские организации, секты, манипулятивные воздействия которых на сознание информационно-зависимых – опаснейшее явление современного общества – информационный терроризм [5].

Информационный терроризм как объективное явление информационных отношений в современном информационном обществе – четвертая, обозначенная авторами проблема, анализу которой в работе уделено особое внимание в силу того, что само явление имеет глобальный характер, а его последствия несут угрозу всему человечеству.

Как уже отмечалось ранее, отличительной особенностью современных информационных отношений выступает информатизация всех сфер жизни современного человека, в основе которой – развития информационная инфраструктура – главное и неотъемлемое условие процветания информационного терроризма. Под информационной инфраструктурой понимается совокупность информационных, вычислительных и коммуникационных ресурсов, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в интересах различных пользователей [3].

Атаки информационных террористов развиваются по следующим направлениям:

1) Умышленное нарушение нормального функционирования информационных процессов и вывод из строя объектов информационной инфраструктуры (нарушения сеансов информационного обмена или проведения каких-либо электронных финансовых операций, срыв проведения электронных конференций и переговоров, провоцирование сбоев в работе различных объектов национальной информационной инфраструктуры, в том числе обеспечивающих управление сложными техническими системами, отнесенными к категории критически важных).

2) Незаконное получение и использование информации и данных (разноплановая криминальная деятельность, начиная от незаконного получения паролей доступа до проникновения в федеральные информационные сети и системы. При этом основная сложность в расследовании преступлений такого рода связана с идентификацией источника враждебного информационного воздействия, в качестве которого может выступать как отдельный хаккер, так и хорошо организованная команда профессионалов, работающая в интересах государства – вероятного противника).

3) Разрушение или уничтожение объектов критически важной инфраструктуры государства и его вооруженных сил путем воздействия на них через информационно-управляющие сети. Реализация угроз этой группы может иметь значительные негативные последствия как для экономики страны, так и для ее безопасности.

4) Манипуляция информацией с целью достижения политических, экономических, военных преимуществ или удовлетворения собственных амбиций правонарушителей. Такого рода информационные атаки могут проводиться комбинированно, совместно с атаками, отнесенными к первой и (или) второй группе. Особенность угроз данного типа заключается в том, что нельзя однозначно оценить ущерб от их реализации. Если в некоторых случаях это может быть основанием для какого-либо официального заявления и негативные последствия оперативно устраняются, то иногда ущерб бывает гораздо более значительным, особенно когда такого рода атаки остаются не обнаруженными и связаны с манипулированием финансовой, экономической или военной информацией. [4]. Методами атак информационных террористов в рамках данного направления могут выступать следующие:

- фальсификация истории – целенаправленное искажение (частичное нарушение) целостной картины исторического развития человеческого общества (или выбранной его части) в определенный временной промежуток;

- ложное основание – способ, когда совокупность аргументов оказывается неполной, скрыты или искажены неугодные факты;

- эклектика – разновидность предметной фальсификации, когда в качестве аргументов приведены такие, которые никак не связаны с доказываемым тезисом;

- ложный тезис – разновидность предметной фальсификации, когда искажен (сужен или расширен) или подменен сам доказываемый тезис;

- уход от предмета – способ, при котором среди многочисленных уловок в споре может применяться уход или отклонение от темы или попытка запутать основную мысль в деталях и частностях. Главное при этом навязать оппоненту выгодную для себя тематику. Однако, следует учитывать, что применение подобного способа может решать задачу доказательства иного тезиса, является составной частью информационной борьбы в другой области;

- демагогия (апелляция к аудитории) – способ, при котором преследуется цель увеличения количества сторонников своей позиции в споре за счет использования группового эгоизма, национальных или расовых предрассудков слушателей и др.;

- переход на личность оппонента – способ фальсификации, который преследует те же цели, что и способы предыдущей группы, но объект воздействия при этом иной. Примером может служить ссылка на порочащую действия оппонента мотивацию (трусость, жажда наживы и т.д.) или на какие-либо его (или его сторонников) проступки или неэтичные действия [1].

Безграничный технический и методический потенциал средств массовой коммуникации (телевидения, интернет) делает их действенными инструментами в руках информационных террористов, нацеленных на превращение свободно мыслящих людей в оглупленную толпу, для которой повсеместно транслируются бескомпромиссные споры и баталии, горячие и жесткие дискуссии, активность и беспристрастность медийных персон – построенный по определенному сценарию общественно-политический «спектакль».

Популярность каналов массовой коммуникации – телевидения и интернет – у массовой аудитории объективно обусловлена рядом причин:

1. Обладают высоким суггестивным потенциалом, используя методы нейролингвистического программирования, гипноза, закладки поведенческих команд, дезинформации, информационных подлогов, искусственного замалчивания важнейших фактов, расстановки неверных акцентов и проч.

2. Воспринимаются информационно-зависимыми людьми легко и некритично, так как усилия для коммуникативного контакта – минимальны, а эффект причастности к транслируемым событиям – ощутимый.

3. Удовлетворяют потребность масс в эксклюзивной, уникальной, никому ранее не известной сенсации, притом, чем больше шокирующих подробностей ее сопровождают, тем привлекательнее с коммуникативной точки зрения сообщение, выходящее за рамки обыденного.

4. Обеспечивают потребность масс «подглядывать в замочную скважину», транслируя бездоказательные, зачастую сфабрикованные подробности личной жизни политиков, общественных деятелей, звезд шоу-бизнеса, медийных персон на уровне сплетен и слухов; при том, между сторонниками той или иной позиции искусственно провоцируются конфликты и столкновения.

5. Распространяют статус и уровень общественного признания канала передачи информации на содержание транслируемого события: чем большим доверием и попу-

лярностью пользуется канал у аудитории, тем живее общественный отклик на представляемое событие.

6. Формируют эффект беспристрастности и объективности транслируемых событий через выстроенные по определенному сценарию социально-политические шоу: поиск истины и ответов на «вечные» вопросы (противостояние богатых и бедных, неизлечимые болезни, экологические катастрофы, приближение конца света), иллюзия свободы слова и гласности (СМИ исполнены социальными провокациями, сквернословием, вульгарностью, не имеющими ничего общего с объективностью и «чистотой» содержания транслируемой информации), минимизация цензуры.

7. Оказывают воспитательно-поучительное воздействие на многомиллионную аудиторию: телекоммуникационные каналы передачи информации характеризуются широким охватом, высокой частотой первичных и последующих контактов, а так же глубокой суггестивной эффективностью.

Таким образом, телевидение и интернет характеризуются весьма привлекательным потенциалом для их использования информационными террористами. Авторы подчеркивают, что интернет-пространство отличается от телевидения рядом специфических характеристик, позволяющим повысить поражающий эффект атак информационных террористов.

Во-первых, интернет-пространство – это достаточно обезличенная, обширная по масштабам среда, где любой желающий от любого имени может создать аккаунт или сообщество с целью пропаганды любой идеи, в том числе, и асоциальной, аморальной, террористической. Подобные сообщества могут объединять сотни и тысячи единомышленников по всему миру, вербовать новых идейных последователей, формируя сеть пользователей с определёнными психографичекими характеристиками (в том числе, и радикальными, ориентированными на акты физического уничтожения населения).

Во-вторых, интернет-пространство в силу своей массовости и обезличенности выступает благодатной средой для виртуального разжигания межрасовых конфликтов, унижения человеческого и общенационального достоинства, попрания духовных ценностей, искажения исторических фактов, которые, в свою очередь, выступают провокаторами реальных актов физического уничтожения «врага», объявленного таковым в виртуальном пространстве.

В-третьих, интернет-пространство позволяет информационным террористам осуществлять масштабные технические атаки (скрытые и открытые) на популярные у пользователей сайты с целью поражения программного обеспечения через компьютерные вирусы, черви, «логические бомбы», троянские программы и проч., которые приводят к:

- извлечению персональных данных пользователей или иной информации личного характера;
- запуску необратимых изменений операционной системы;
- внешнему управлению системой.

В-четвертых, интернет-пространство служит источником материального обеспечения террористических группировок посредством запуска сфабрикованных «социальных» проектов и программ, ориентированных на участие в поддержке тяжело больных детей, одиноких стариков, приютов для бездомных животных и проч.

В-пятых, интернет-аудитория, характеризуется высокой степенью социальной дифференциации, что позволяет информационным террористам манипулировать различными общественными слоями. Коммуникативная эффективность любого информационного потока зависит от того, насколько его содержание вписывается в картину мира и совпадает с представлениями получателей информации. Другими словами, чем актуальнее и понятнее тема обращения и чем правильнее подобраны методы ее подачи,

тем «живее» социальный отклик на информационный повод. Информационно-атакующей стороне достаточно выделить социальную общность с определенными психографическими параметрами, определить уязвимость этой общности и нанести по ней целенаправленный удар. Так, например, для детей и молодежи актуальны вопросы самоутверждения, самовыражения, уверенности в себе, принятие сверстниками. С манипулятивной точки зрения данные аудитории привлекательны отсутствием четко сформированных жизненных установок и ориентиров, которые через средства массовой коммуникации подаются им в виде готовых моделей поведения (часто аморальных) с целью закладки поведенческих команд (суицид, асоциальные модели поведения, агрессия против родителей, вредные привычки и проч.). Для взрослого трудоспособного населения актуальными являются вопросы финансовой стабильности, социальной защищенности, безопасности и уверенности в будущем. Таким образом, темы борьбы богатых и бедных, слабых и сильных, вреда отдельных видов продуктов, неизлечимых болезней и эпидемий, экологических катастроф, приближения конца света, повсеместно транслируемые средствами массовой коммуникации, волнуют, запугивают, и тем самым, дестабилизируют массы. Физическая безопасность общества, военные перевороты, террористические атаки, стихийные бедствия, права и свободы человека и гражданина – темы, беспокоившие общество на уровне инстинктов самосохранения и генетической памяти. Следствие атак информационных террористов в данном направлении – общественная паника, отчаяние, физический страх, нерациональные потребительские решения, недоверие государству, – почва для командного призыва к действию масс в масштабах страны: переворот, массовые восстания, убийства, войны [6].

Информационная безопасность страны – одна из важных составляющих ее национальной безопасности, оказывающая существенное влияние на защиту национальных интересов страны в различных сферах жизнедеятельности общества и государства [7].

Система информационной безопасности – система, обеспечивающая стабильное состояние защищенности информационных ресурсов от воздействия информационного оружия. При этом все необходимые силы и средства поддерживаются в постоянной готовности к отражению возможной агрессии как в самом информационном пространстве, так и с его широкомасштабным использованием, а также принимаются все возможные меры по раннему выявлению и нейтрализации потенциальных конфликтов и угроз в информационном пространстве [2].

Обеспечение информационной безопасности общества в целом, и каждого отдельно взятого его члена – это вопрос национальной безопасности государства, решать который необходимо на международном, федеральном, региональном уровнях правоохранительными усилиями государственных органов, комитетов, комиссий, которые во взаимодействии с различными общественными организациями и гражданами способны создать единое безопасное информационное пространство с отлаженным механизмом противодействия информационному терроризму, в основе которого:

1. Международное сотрудничество в вопросах информационной безопасности общедоступных информационных ресурсов на основе выработки единой методической и понятийно-категориальной базы с целью унификации подходов к содержанию и оценке последствий атак информационных террористов.

2. Оптимизация системы законодательного регулирования прав, свобод, обязанностей и ответственности владельцев и пользователей средств массовой коммуникации с целью обеспечения технической и психологической безопасности транслируемых информационных потоков.

3. Общедоступность и прозрачность системы оповещения владельцев и пользователей средств массовой коммуникации об информационных атаках, а так же формиро-

вание эффективного механизма обратной связи с надзорными органами для информирования о фактах таких атак.

4. Непрерывное обучение и повышение уровня компетентности специалистов, занятых вопросами обеспечения информационной безопасности.

5. Повышение информационной грамотности пользователей средств массовой коммуникации усилиями семьи (ближайшего окружения, психологов) на стадии первичной социализации, а на стадии вторичной – в школах, СУЗах, ВУЗах, на рабочих местах [5].

В заключение отметим, что информация в руках информационных террористов – эффективный инструмент «социального подстрекательства», доступная альтернатива физическому разрушению и уничтожению общества, помешать которым может лишь комплексное решение проблем «экологичности» транслируемых в обществе информационных потоков на международном, федеральном и региональном уровнях [5].

Литература:

1. Агеев Н.В. Почему и как происходит искажение истории // военная мысль. – 2006. - №9. – С. 59-65.

2. Базылев С.И., Дылевский И.Н., Комов С.А., Петрунин А.Н. Деятельность Вооруженных Сил Российской Федерации в информационном пространстве: принципы, правила, меры доверия // Военная мысль. – 2012. – № 6. – С. 24-28.

3. Голубев Ю.Н., Гринь В.Р., Ширманов А.В. Терминологические заторы на путях военной информатизации // Военная мысль. – 2012. – № 6. – С. 44-53.

4. Молчанов Н.А. Информационный потенциал зарубежных стран как источник угроз военной безопасности РФ // Военная мысль. – 2008. – № 10. – С. 2-9.

5. Пидшморга Ю.В., Кучерук Д.А. Информационный терроризм как объективное явление современного информационного общества: материалы международной научно-практической конференции «Научная исследовательская деятельность в России и за рубежом» (26 апреля 2018 г.) Отв. редактор Зарайский А.А. – Саратов: Издательство ЦМП «Академия бизнеса», 2018. – С.74-77.

6. Пидшморга Ю.В. Информационная безопасность – актуальная проблема современности: материалы международной научно-практической конференции «Современная наука как фактор преобразования современного общества» (4 мая 2018 г., г.Москва) Отв. редактор Зарайский А.А. – Саратов: Издательство ЦМП «Академия бизнеса»,

7. Пузенькин И.В., Михайлов В.В. Роль информационно-психологических средств обеспечении обороноспособности государства // Военная мысль. – 2015. – № 7. – С. 11-15.

Письменский М.В., Басан Е.С.

Институт компьютерных технологий и информационной безопасности

Инженерно-технологическая академия г. Таганрог

АНАЛИЗ ВОЗМОЖНОСТЕЙ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ДЛЯ ГРУППЫ МОБИЛЬНЫХ РОБОТОВ

В современном мире все больше задач подвергается автоматизации, а также появляются новые перспективные отрасли производства и науки. Одна из таких перспективных областей – это автономные беспилотные роботы, которые могут выполнять различные функции, от разведки и сбора данных, до транспортировки различных грузов. Часто для увеличения эффективности работы роботов объединяют в автономные децентрализованные группы. Такая архитектура позволяет им собирать больше информации и быть более надёжным, ведь поломка одного из роботов не приведет к провалу

задания. Децентрализованная архитектура уже используется в системах умных домов, и различных сенсорных сетях. Но распределённая архитектура вносит и свои корректировки в аспекты информационной безопасности. Имея распределённую архитектуру, такие автономные роботы подвержены специфичным атакам, а многие защитные меры в такой распределенной сети не могут быть реализованы.

В данной статье рассматриваются требования федеральной службы по техническому и экспортному контролю Российской Федерации (далее ФСТЭК) для автоматизированных систем управления производственными и технологическими процессами (далее АСУ ТП), описанные в приказе ФСТЭК от 14 марта 2014 года[1]. Данный приказ многое повторяет или заимствует из следующих документов:

1. Семейство отраслевых стандартов NERC Critical Infrastructure Protection (NERC CIP);
2. Семейство стандартов ISA/IEC 62443 Industrial Automation and Control Systems Security;
3. Рекомендации NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security» и NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations»[2]

В документе NIST SP 800-53 так же, как и во ФСТЭК 31 описана модель непрерывного усовершенствования информационной безопасности и схожие требования к мерам защиты. Документы NIST SP 800-53 и ФСТЭК 31 отличаются нескорыми требованиями, например, в NIST отсутствуют такие группы требований к мерам безопасности как «Защита среды виртуализации (ЗСВ)», «Обеспечение безопасной разработки программного обеспечения (ОБР)», «Управление обновлениями программного обеспечения (ОПО)». Так же имеется небольшое различие по самим мерам, входящим в группы требований. Так же в NIST определенный приоритеты мер, с которых стоит начать внедрение

Описание АСУ ТП

Анализируемая АСУ ТП представляет собой многоуровневую структуру, в которой выделяются два уровня: уровень операторского управления и уровень автоматического управления.

На уровне автоматического управления находятся автономные беспроводные летающие роботы, которые используют операционную систему Ubuntu Mate 16.04.2 (Xenial) с установленным фреймворком Robot Operation System и оснащены wi-fi модулями способными работать по стандарту 802.11n, так как в этом стандарте была добавлена функция «ad-hoc 11n». При помощи этой функции роботы связываются в беспроводную децентрализованную сеть. Такая сеть не имеет постоянной структуры, клиентские устройства соединяются друг с другом в реальном времени. В такой сети каждый узле передает данные напрямую узлу назначения, а не через маршрутизаторы как в обычных централизованных сетях. Для маршрутизации в сети данные роботы используют протокол AODV. Данный протокол является проактивным, и является более энергоэффективным[3,4] Как аппаратное обеспечение для этих роботов используется одноплатные компьютеры Raspberry pi. Роботы также имеют различные датчики для анализа обстановки, такие как камеры и дальномер для измерения дальности от различных объектов. и выявления своего месторасположения.

На уровне операторского управления располагается автоматизированное рабочее место оператора, то есть компьютер с сертифицированной операционной системой на основе Lunux, такой как SUSE Linux или Red Hat Enterprise Linux. Оператор следит за информацией, приходящей от роботов и может посылать им команды. Так же для связи роботов с рабочим местом оператора используется маршрутизатор ASUS RT-AC5300.

Формирование требований к АСУ ТП

Для принятия решения о необходимости создания системы защиты информации для исследуемой сети, согласно приказу ФСТЭК № 31, необходимо проанализировать цели создания данной автоматизированной системы и задачи, которые решает данная АСУ ТП. В данном случае АСУ ТП включает в себя группу автономных роботов, выполняющих разведку на территории указанной оператором. Так же данные роботы могут принимать некоторые решения без внимания оператора, на основании полученной датчиками информации о местности и алгоритмов группового управления.

Затем следует определить информацию, нарушение доступности, целостности или конфиденциальности которой может привести к нарушению штатного режима функционирования АСУ ТП. Все это следует делать, основываясь на Приложении 1, приказа ФСТЭК № 31. В данной АСУ ТП выделяется два вида критически важной информации, измерительная и управляющая. Измерительную информацию получают датчики, установленные на автономных роботах. На основании этой информации роботы принимают локальные решения о своей дислокации на местности, препятствиях, и наиболее оптимальных путях выполнения поставленной задачи. Управляющую информацию роботы получают от оператора и друг друга при помощи алгоритмов группового управления, она служит для постановки основной задача и её коррекции.

Нарушение целостности измерительной информации, то есть ее искажение, уничтожение или модификация, может привести к выводу роботов из строя или перехвата этих роботов. Это угроза регионального характера, значит степень возможного ущерба средняя.

Нарушение доступности измерительной информации, то есть неправомерное блокирование, может помещать роботам ориентироваться на местности, что может привести к выводу роботов из строя таким образом, степень ущерба низкая.

Обеспечение конфиденциальности для измерительной информации требуется в случаях, когда выполняется разведка охраняемых территорий, утечка такой информации может раскрыть различную конфиденциальную информацию о топологии предприятия, что может является угрозой локального характера.

Таким образом измерительная информация, обрабатываемая в АСУ ТП имеет низкий уровень значимости, так как для всех свойств безопасности информации определены низкие уровни ущерба.

Далее выполняется разбор последствий нарушений свойств безопасности информации для управляющий информации.

Нарушение целостности измерительной информации, то есть ее искажение, уничтожение или модификация, может привести к выходу робота из строя, а также полным контролем над роботом, что в свою очередь может привести к использованию данных роботов в различных противоправных действиях, таких как нападение на людей или использования в террористических актах. Что будет является чрезвычайной ситуацией регионального или межмуниципального характера, а значит степень возможного ущерба является средней.

Нарушение доступности для управляющей информации, приведет у невыполнения поставленной изначально задачи, или даже потере роботов. Роботы могут быть полностью выведены из строя лишившись команд оператора и функций группового управления. Потеря роботов имеет средний уровень ущерба.

Нарушение конфиденциальности для управляющей информации может привести к неправомерному доступу ко всем полученным роботами командам, а значит миссия роботов станет известна злоумышленнику. Что может привести лишь к угрозе локального характера, а значит и степень ущерба оценивается как низкая.

Управляющей информации присвоен средний уровень критичности информации, так как хотя бы для одного из свойств безопасности определён средний уровень возможного ущерба.

На основании вышеописанной анализа информации, было принято решение о необходимости создания системы защиты автоматизированной системы управления. Так же определенны цели и задачи системы защиты, такие как обеспечение целостности, доступности и конфиденциальности для управляющий и измерительной информации, не ниже необходимых для второго класса защищенности.

Далее были оценены угрозы безопасности информации и построена модель угроз. Для этого пункта будет использован проект «Методика определения угроз безопасности информации в информационных системах. Данный проект необходимо применять совместно с банком данных угроз безопасности ФСТЭК России.

Для исследуемой АСУ ТП такие нарушители как внешние субъекты или преступные организации обладают базовым (низким) потенциалом нападения при реализации угроз безопасности в информационной системе. Но конкурирующие организации обладают средним потенциалом, так как могут знать о данной системы или о защите таких систем, и обладают большими средствами и мотивацией.

Далее были оценены возможные способы реализации угроз безопасности информации. Способы реализации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы. Для данной системы были выбраны следующие возможности для реализации угроз: несанкционированный доступ и (или) воздействие на объекты на прикладном уровне; несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы); несанкционированный физический доступа и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации;

Требования к системе защиты АСУ определяются в зависимости от класса защищенности автоматизированной системы, который как для измерительной информации является средним – К2, так и для для управляющей информации средний - К2. Так как оба типа информации имеют средний класс защищенности то и будем использовать его для формирования требований. Объекты защиты на операторском уровне – управляющая и измерительная информация, передаваемая и получаемая компьютером оператора. На уровне автоматического управления это управляющая и измерительная информация, передавая между автономными роботами, а также передаваемая и получаемая от компьютера оператора, а также сами автономные роботы.

Далее следует выбрать меры по защите информации в АСУ ТП на основании особенностей системы, модели угроз и класса защищенности.

В пункте «Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)»

1. ИАФ.0 Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа (уровень операторского управления).

2. ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора (уровень операторского управления).

3. ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (уровень автоматического управления).

4. ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов (уровень операторского управления).

5. ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (уровень операторского управления).

В пункте «Управление доступом субъектов доступа к объектам доступа (УПД)»

1. УПД.0 Разработка правил и процедур (политик) управления доступом субъектов доступа к объектам доступа (уровень операторского доступа).

2. УПД.3 Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления (уровень операторского управления, уровень автоматического управления)

3. УПД.6 Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе) (уровень операторского управления).

4. УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (уровень операторского управления).

5. УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (уровень операторского управления, уровень автоматического управления).

6. УПД.14 Регламентация и контроль использования в автоматизированной системе управления технологий беспроводного доступа (уровень автоматического управления)

В пункте «Ограничение программной среды (ОПС)»

1. ОПС.0 Разработка правил и процедур (политик) ограничения программной среды (уровень операторского управления).

2. ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов (уровень операторского управления).

В пункте «Регистрация событий безопасности (РСБ)»

1. РСБ.0 Разработка правил и процедур (политик) регистрации событий безопасности (уровень операторского управления).

2. РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения (уровень операторского управления).

3. РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации (уровень операторского управления).

4. РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (уровень операторского управления).

5. РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (уровень операторского управления).

В пункте «Антивирусная защита (АВЗ)»

1. АВЗ.1 Реализация антивирусной защиты (уровень операторского управления).

2. АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) (уровень операторского управления).

В пункте «Обнаружение вторжений (СОВ)»

1. СОВ.0 Разработка правил и процедур (политик) обнаружения вторжений (уровень автоматического управления).

2. СОВ.1 Обнаружение вторжений (уровень автоматического управления).

3. СОВ.2 Обновление базы решающих правил (уровень автоматического управления).

В пункте «Контроль (анализ) защищенности информации (АНЗ)»

1. АНЗ.0 Разработка правил и процедур (политик) контроля (анализа) защищенности (уровень операторского управления, уровень автоматического управления).

2. АНЗ.1 Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей (уровень операторского управления, уровень автоматического управления).

3. АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации (уровень операторского управления, уровень автоматического управления).

4. АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей (уровень операторского управления)

В пункте «Обеспечение целостности (ОЦЛ)»

1. ОЦЛ.0 Разработка правил и процедур (политик) обеспечения целостности (уровень операторского управления, уровень автоматического управления).

2. ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (уровень операторского управления, уровень автоматического управления).

В пункте «Обеспечение доступности (ОДТ)»

1. ОДТ.0 Разработка правил и процедур (политик) обеспечения доступности (уровень операторского управления, уровень автоматического управления).

2. ОДТ.1 Использование отказоустойчивых технических средств (уровень операторского управления, уровень автоматического управления).

В пункте «Защита среды виртуализации (ЗСВ)»

1. ЗСВ.0 Разработка правил и процедур (политик) защиты среды виртуализации (уровень операторского управления, уровень автоматического управления).

2. ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (уровень операторского управления, уровень автоматического управления).

В пункте «Защита автоматизированной системы и ее компонентов (ЗИС)»

1. ЗИС.0 Разработка правил и процедур (политик) защиты автоматизированной системы и ее компонентов (уровень операторского управления, уровень автоматического управления).

2. ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (уровень операторского управления, уровень автоматического управления).

3. ЗИС.4 Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) (уровень операторского управления, уровень автоматического управления).

4. ЗИС.20 Защита беспроводных соединений, применяемых в автоматизированной системе управления (уровень операторского управления, уровень автоматического управления).

5. ЗИС.22 Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании (уровень операторского управления, уровень автоматического управления).

Так же следует добавить, что из-за ограничений автономных роботов, таких как – небольшая память и низкая вычислительная мощность, выбранные средства защиты информации долдоны быть как можно более легковесными, иначе они будут влиять на штатную работу устройств.

Разработка и внедрение системы защиты автоматизированной системы управления

При разработке системы защиты были определенны следующие субъекты доступа: оператор, отправляющий команды группе роботов через компьютер операторов. И следующие объекты доступа, являющиеся объектами защиты: автоматизированное ра-

бочее место оператора, автономные роботы. Роботы связанны беспроводными связями с другими роботами, а выбранный лидер группы роботов подключен к маршрутизатору. К этому же маршрутизатору подключен и компьютер оператора. Роботы передают между собой информацию о задании, принимая решения при помощи алгоритмов группового управления, так же роботы получают управляющую информацию от оператора. Роботы передают собранную измерительную информацию лидеру группы, после чего лидер группы передает ее на компьютер оператора.

Стандартными средствами управления учетными записями Ubuntu создана учетная запись оператора на уровне диспетчерского управления на автоматизированном рабочем месте оператора. Только оператор, который вошел под своей учетной записью может посылать команды роботам, а также принимать их. Заблокирована возможность устанавливать какое-либо дополнительное программное обеспечение. Установлен минимальная длина пароля в 8 символов, а также время жизни пароля 2 месяца, после истечения этого срока пароль должен быть принудительно изменен. С помощью этого реализуются меры ИАФ.0, ИАФ.1, ИАФ.3, ИАФ.4. УПД.11, ОПС.1, ОПС.2, АНЗ.5, ЗСВ.0, ЗСВ.1, ОПС.0, ОПС.1.

В межсетевом экране Netfilter при помощи утилиты iptables настроены белые списки, согласно этим спискам, оператор может отправлять и передавать данные лишь ограниченному количеству устройств внутри сети по ip-адресу и протоколу, в белые списки занесен ip-адрес и порт сервера обновлений антивируса и операционной системы, а так же статические, заранее заданные адреса беспилотных роботов. Также открыт только порт 1194 для openVPN. Все пакеты пришедшие с ip-адресов не включенных в белые списки блокируются. Такие средства позволяют реализовать требования УПД.0, УПД.3, УПД.14

Программа Fail2ban реализует требования УПД.6. После пяти неудачных попыток входа учетная запись будет заблокирована. Данная программа не является сертифицированной.

Для учета разлитых событий безопасное используется встроенная в Ubuntu компонент auditd. Данная программа позволяет вести учет системных событий и событий безопасности. В журнал учета будут заноситься все попытки подключиться к ip-адресам, которых нет в белом списке, установить или запустить неразрешенное программное обеспечение. Так же в журнал будут добавляться сообщения об ошибках. Данная программа не является сертифицированной и реализует требования РСБ.0, РСБ.1, РСБ.2, РСБ.3, РСБ.5.

Настроенный сервер openVPN на автоматизированном рабочем месте оператора, и настроенный клиент openVPN на автономных роботах позволяют иметь надежный зашифрованный канал для передачи информации между оператором и роботами. Данная реализация технологии VPN считается безопасной и обеспечивает защиту на сетевом, транспортном, сеансовом, представительском и прикладном уровнях сетевой модели OSI Данная технология позволяет частично реализовать требования УПД.3, УПД.13. УПД.14, ЗИС.0, ЗИС.3, ЗИС.4, ЗИС.20, ЗИС.22. Данные требования реализованы лишь частично, потому что ВПН используется только для установления связи между выбранным лидером группы и компьютером оператора.

Сканер-ВС – сертифицированный инструмент для анализа защищенности информационных систем. В сканере реализован контроль целостности, аудит беспроводных сетей, аудит информационной системы, контроль эксплойтов. Запуск этого сканера до запуска и после полета беспилотных роботов, является обязательным использования автоматизированных роботов является обязательным. Данное средство реализует следующие требования: АНЗ.0. АНЗ.1, АНЗ.4, АНЗ.5, ОЦЛ.0, ОЦЛ.1.

Сертифицированный антивирус, такой как Kaspersky Endpoint Security 10 для Linux или Dr.Web Enterprise Security Suite 10 версиипозволяют обеспечить реализацию АВЗ.1, АВЗ.2 для уровня операторского управления.

Для защиты беспроводного канала используется программа сертификации WPA2, на данный протокол существуют известные атаки, такие как KRACK, Hole196, так же возможен атака грубой силы, для этого возможно начать процесс деаунтификации, и собрать большое количество данных для авторизации, после чего подбор паролей может проводится удаленно. Данный протокол является лучшим по сравнению с WPA WEP. Данный проткал позволяет реализовать требования ЗИС.22.

Для реализации ИАФ.2 на автоматизированном рабочем месте оператора был настроен RADIUS сервер с открытым исходным кодом FreeRadius. Для каждого из роботов были созданы учетные записи. На маршрутизаторе ASUS RT-AC5300 была настроена функция «Radius with 802.1x» для аутентификации и авторизации через сервер RADIUS. Данный маршрутизатор не является сертифицированным устройством, но сертифицированных аналогов не было найдено.

Требования СОВ.0, СОВ.1 для уровня автоматизированного управления не были выполнены из-за отсутствия подходящих систем обнаружения вторжений. Данные роботы имеет мало памяти и вычислительной мощности, и реализация этого требования может сильно повлиять на штатную работу данных роботов.

Требования ОДТ.0 и ОДТ.1 не были реализованы так как небыли найдено подходящих средств обеспечения доступности. Данные роботы используют беспроводной как нал передачи данных и находятся в неподконтрольной территории, в которой канал передачи данных может быть ненадежным, злоумышленник может создать в нем помехи или же получить физический доступ к роботам.

Большинство требований реализованы лишь частично из-за невозможности использовать сертифицированные средства защиты информации. Для разрабатываемой АСУ ТП использование сертифицированных средств может приводить к нарушению штатной работы системы из-за слабых мощностей беспилотных роботов.

Приказ ФСТЭК №31 предлагает комплексный подход обеспечению защиты информации, а АСУ ТП. В приказе рассмотрены все актуальные подходы к защите информации. Такие как классификация системы, определена угроз, классификация нарушителя, определения требований и разработка системы защиты. Данный приказ даёт большую свободу выбора средств защиты, для построения индивидуального подхода при обеспечении защиты информации, что позволяет учитывать уникальные особенности системы, ее требования и ограничения.

Данный приказ достаточно полно охватывает системы мобильных роботов, но реализация данного приказа все равно недостаточна для защиты роботов. В своей основе такие системы имеют фундаментальные проблемы и ограничения безопасности, такие как беспроводная среда передачи данных и малая память, и вычислительная мощность. Многие требования реализованы частично и часто не смогут защитить от целенаправленной атаки. Данные роботов можно получить, физически разобрав их и получив прямой доступ к памяти или нарушить их работу, сломав их.

Работа выполнена при поддержке Гранта Министерства образования и науки Российской Федерации Инициативный научный проект № 2.6244.2017/8.9.

Литература:

1. Приказ ФСТЭК России от 14 марта 2014 г. N 31 Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [Электронный

ресурс] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 20.06.2018).

2. NIST 800-82 Guide to Industrial Control Systems (ICS) Security [Электронный ресурс] URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09 (дата обращения 20.06.2018).

3. Nadia Qasim, Fatin Said, Hamid Aghvami ," Mobile Ad Hoc Networks Simulations Using Routing Protocols for Performance Comparisons", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

4. M. Lakshmi, P. E. Sankaranarayanan, Performance Analysis of Three routing protocols in wireless Mobile Ad Hoc Network. Information technology Journal 5 (1), 114-120, 2006.

Полупанов А.А., Полупанова Е.Е., Аликумова А.И.
Кубанский государственный университет

ПОДСИСТЕМА МОДЕЛИРОВАНИЯ ДВИЖЕНИЯ ТРАНСПОРТА ПО ДОРОГЕ С ПРЕПЯТСТВИЯМИ

Введение. Автоматическое управление на реальных дорогах – это давнее стремление не только водителей, но и всей автомобильной промышленности в целом. Будущее беспилотного управления неизбежно требует всестороннего и надёжного восприятия дороги и дорожного окружения. Эта задача является достаточно сложной из-за огромного количества вариантов предметов и дорожных условий (дорожное полотно, транспортные средства, различные препятствия, освещение, погода и т.д.), поэтому актуальна разработка новых методов, моделей, алгоритмов компьютерных систем анализа и обработки цифровых изображений дорожного полотна [1-2].

В статье приведена блок-схема работы алгоритма подсистемы моделирования движения транспортного средства по дороге с препятствиями, показанная на рисунке 1.

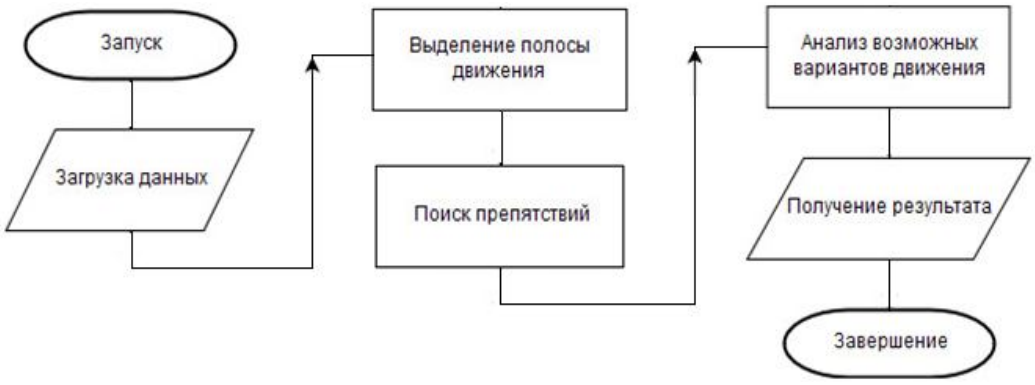


Рис. 1. Блок-схема работы алгоритма подсистемы моделирования движения транспортного средства по дороге с препятствиями

Рассмотрим подробнее основные этапы приведённой выше блок-схемы.

Выделение полосы движения. После загрузки входных данных на полученном изображении алгоритмически выделяется полоса дорожного полотна, по которой движется автомобиль. На первом этапе изображение преобразуется к размеру 960 x 540. После изменения масштаба «картинка» из цветной цветовой палитры переводится в черно-белую и применяется размытие по Гауссу (фильтр) [3], как показано на рисунке 2.

Рис. 2. Применение размытия по Гауссу

Для упрощения процесса обнаружения краев, изображение преобразуется из цветного в оттенки серого, что позволяет отбросить информацию о цвете и заменить ее одним значением интенсивности для каждого пикселя изображения. Подавление шума путём усреднения значения соседних пикселей позволяет облегчить работу алгоритма и достичь более качественных результатов.

Следующим этапом выделяются края и границы присутствующие на изображении. Оператор Кэнни [4] анализирует пиксели в соответствии с их производной по направлению, т.е. градиентом. Резкое изменение в соседних пикселях позволяет выделить линии, находящиеся на изображении. Результат данного этапа представлен на рисунке 3.

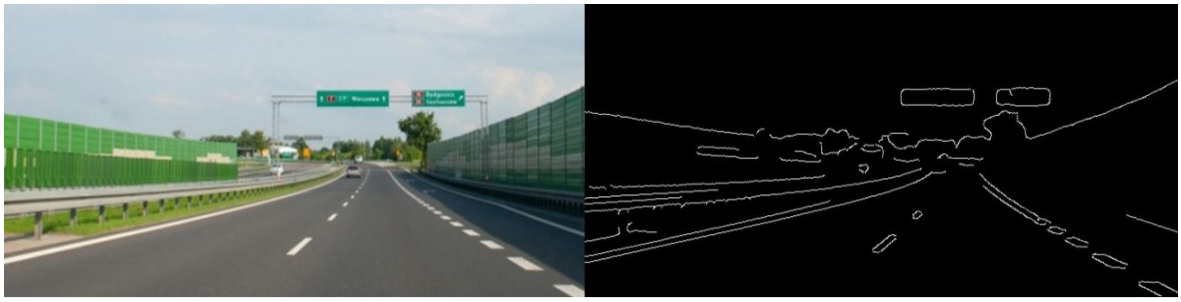


Рис. 3. Результат применения оператора Кэнни на правом изображении

Затем, с учетом положения и ориентации камеры в пространстве выделяется непосредственная полоса движения, расположенная в области, ограниченной трапецией, как показано на рисунке 4.

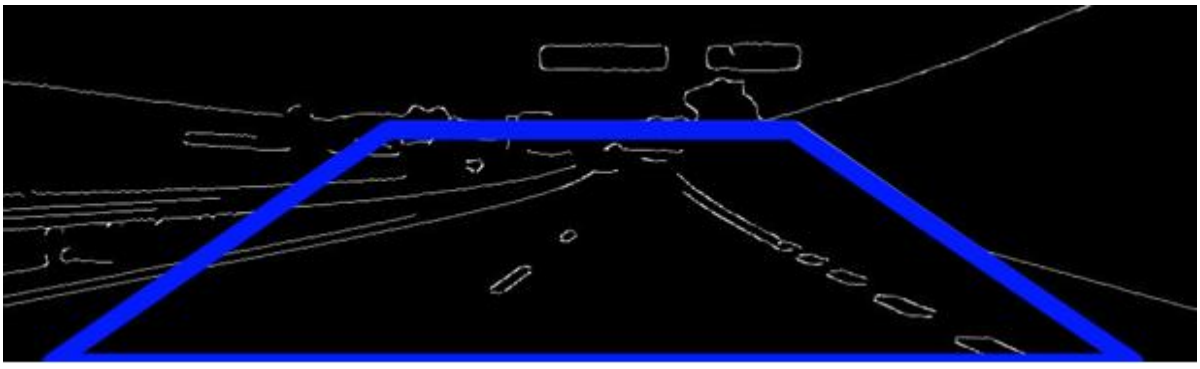


Рис. 4. Выделенная трапециевидная область интереса

Все, что находится снаружи вне этой области, «отбрасывается» алгоритмом т.к. не представляет особого интереса.

Далее к полученному изображению применяется преобразование Хафа [6], которое группирует краевые точки, лежащие примерно на одной линии, в единую прямую, с тем, чтобы получить линии дорожной разметки. В результате получается левая и правая линии, показанные чёрным цветом на рисунке 5, задаваемые обычными уравнениями.

Рис. 5. Линии полосы движения

Следует заметить, что если на изображении дороги отсутствует линия разметки, то полоса движения строится на основе прямых, для которых коэффициенты наклона и смещения были подобраны эмпирическим путём.

Поиск препятствий. После того, как была выделена главная полоса движения для автомобиля, необходимо определить на данной траектории наличие или отсутствие препятствий. Для этого используется гистограмма направленных градиентов и SVM-классификатор [7].

В соответствии с алгоритмом, входное изображение разбивается на отдельные области, представляемые из себя ячейки определённого размера.

На рисунке 6 показан результат применения классификации, к левой части исходного изображения, показанного на рисунке 2.

Рис. 6. Результат классификации препятствий

Для каждого такого квадрата сохраняются координаты левого верхнего и правого нижнего угла и заносятся в один массив. Далее для каждой полученной области выполняются следующие действия:

− преобразование к размеру 64 × 64 пикселя;

− вычисление гистограммы направленных градиентов;

− нормирование получившихся признаков;

− к полученным признакам применяется классификатор, который вычисляет вероятность того, к какому из двух классов относится рассматриваемая область;

− если полученная вероятность превышает некий установленный порог (например, 0.8), то данная область записывается в массив, в котором находятся области, распознанные как препятствия.

Препятствия бывают различных размеров, но в большинстве случаев они достаточно большие, чтобы несколько пересекающихся областей было отнесено к данному классу. Данный метод является весьма точным, однако требует достаточно больших вычислительных ресурсов. Время обработки кадра существенно зависит от размера изображения и задаваемой области поиска, поэтому допустимо ограничить зону рассмотрения лишь нижней частью изображения, исходя из предположения о расположении и ориентации камеры.

Анализ возможных вариантов движения. Цель данного этапа заключается в объединении полученных предыдущих двух результатов и анализе дальнейшего поведения участника движения. Главная полоса дорожного полотна для движения была вычислена на первом этапе анализа изображения, и она характеризуется двумя прямыми, которые в свою очередь представляются обычным уравнением с коэффициентами наклона и смещения. При анализе дорожной обстановки достаточно определить доступность ближайшего участка дороги для дальнейшего движения. Первым делом необходимо проверить область, которая ограничена двумя прямыми главной полосы и горизонтальной прямой. С учётом перспективы, длина данной области составляет 3 – 6 метров, что позволяет водителю совершить необходимое перестроение при необходимости.

На втором этапе были получены области, относящиеся к классу препятствий, которые характеризуются координатами левого верхнего угла и правого нижнего. Если пересечений не возникает, то данная часть дороги считается пригодной для продолжения движения и помечается зелёным цветом, как показано на рисунке 7.

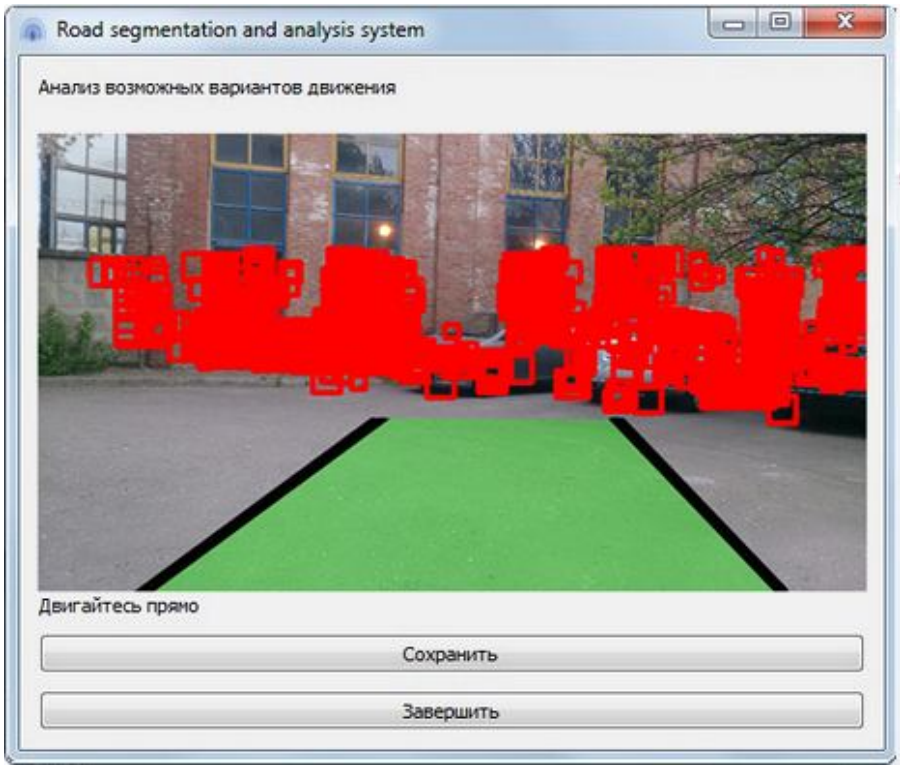


Рис. 7. Программный интерфейс и анализ возможных вариантов движения

Таким образом, анализ доступности данной части дороги для движения сводится к проверке вхождения областей, помеченных как препятствие, в область, которая рассматривается для дальнейшего движения.

Приоритет отдаётся прямолинейному движению, однако такая ситуация не всегда возможна. Если при анализе выясняется, что на данном участке дороги находится препятствие, то происходит поиск альтернативных вариантов.

Заключение. В результате работы исследованы алгоритмы и методы, позволяющие выполнять сегментацию дорожного полотна на изображении или видеоряде. На языке Python и кросс-платформенного фреймворка PyQt разработана программная подсистема моделирования движения транспортного средства по дороге с препятствиями, в которой реализован метод выделения полосы движения и метод распознавания препятствий. Для обработки изображений и ускорения работы программы использованы дополнительные модули: OpenCV, NumPy, Scikit-learn, LinearSVC.

В результате экспериментальных исследований установлено, что метод распознавания препятствий (классификатор), работает с точностью около 96,8%.

Литература:

1. Курейчик В.В., Полупанов А.А. Эволюционные методы разбиения схем на основе адаптивных генетических процедур: монография. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – 160 с.

2. Лукяница А.А., Шишкин А.Г. Цифровая обработка видеоизображений / А.А. Лукяница. – М.: «Ай-Эс-Эс Пресс», 2009. – 518 с.

3. Кольцов П.П. Оценка размытия изображений / П.П. Кольцов // Компьютерная оптика. – 2011. – Т. 35, № 1. – С. 95 - 102. URL: http://www.computeroptics.smr.ru/KO/PDF/KO35-1/12.pdf (дата обращения: 15.06.2018)

4. John F. Canny, A Computational Approach to Edge Detection – [Электронный ресурс]. – Режим доступа к статье: http://perso.limsi.fr/Individu/vezien/ PAPIERS_ACS/ canny1986.pdf (дата обращения: 15.06.2018)

5. Власов А.В., Цапко, И.В. Модификация алгоритма Канни применительно к обработке рентгенографических изображений / А.В. Власов // Вестник науки Сибири. – 2013. № 4(10). URL: http://sjs.tpu.ru/journal/article/download/823/582 (дата обращения: 15.06.2018)

6. Кудрина М.А. Использование преобразования Хафа для обнаружения прямых линий и окружностей на изображении / М.А. Кудрина // Известия Самарского научного центра Российской академии наук. – 2014, Т. 16, №4(2). – С. 476 - 478. URL: http://www.ssc.smr.ru/media/journals/izvestia/2014/2014_4_476_478.pdf (дата обращения: 15.06.2018)

7. Лисицын С.О., Байда О.А. Распознавание дорожных знаков с помощью метода опорных векторов и гистограмм ориентированных градиентов / С.О. Лисицын // Компьютерная оптика. – 2012, Т. 36, №2. – С. 1 - 8. URL: http://sergey.lisitsyn.me/ papers/lisitsyn12a.pdf (дата обращения: 15.06.2018)

Прокопенко А.Н., Гуржий А.А.
Белгородского юридического института МВД России имени И. Д. Путилина

ЕДИНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО МВД РОССИИ, КАК ОСНОВА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ МИНИСТЕРСТВА НА СОВРЕМЕННОМ ЭТАПЕ

Информационные ресурсы правоохранительных органов создавались всегда для обеспечения их деятельности, учета преступлений и правонарушений, ведения статистики, регистрации граждан и других целей. Но на современном этапе это направление деятельности МВД России приобрело новое наполнение, особые задачи и цели, поскольку она осуществляется в рамках единых государственных проектов по созданию

комплексных государственных информационных ресурсов и общегосударственного единого информационного пространства.

Необходимо отметить, что каждое правоохранительное ведомство создает собственные информационные ресурсы самостоятельно и крайне неохотно делится ими с другими министерствами и ведомствами, что объясняется спецификой оперативно-розыскной и правоохранительной деятельности, а также обеспечением информационной безопасности. Однако, в случае с МВД России исторически сложилась другая ситуация: информационные ресурсы милиции, а впоследствии – полиции, являются «общими» для всех правоохранительных органов не только нашей страны, но и других государств СНГ. Подобная ситуация сложилась из-за того, что МВД России является правопреемником МВД СССР, которое обобщало всю информацию о преступности и гражданах в Советском Союзе. В результате в МВД России были накоплены одни из самых крупных информационных ресурсов в Европе.

Для организации работы с накопленными информационными ресурсами потребовалось создание возможности для пользователей по доступу к информации. В течении десятилетий доступ к информации осуществлялся по запросу, срок исполнения которого составлял от суток до десяти дней, в зависимости от того, кто осуществлял запрос. В 2000-е годы был реализован механизм, который позволял осуществлять запросы в электронном виде. Соответственно скорость получения информации сократилась и составляла уже от 1-2 часов до трех суток. Впоследствии осуществлялась модернизация информационных ресурсов, их объединение, совершенствование механизма доступа. Однако, задачу доступа всех пользователей в реальном масштабе времени удалось решить только в начале 2010-х годов.

В настоящий момент все информационные ресурсы МВД России объединены в единое информационное пространство, которое представляет собой совокупность банков данных и информационно-телекоммуникационных сетей, функционирующих на основе единых принципов, а также технологий их сопровождения и использования.

Правовой основой функционирования единого информационного пространства является Федеральный закон «О полиции» [1], который в пункте 4 статьи 11 определил, что федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных. Перечень персональных сведений, накапливаемых в банках данных, зафиксирован в пункте 3 статьи 17 ФЗ «О полиции». Указанные сведения объединены в специализированные информационные ресурсы для решения задач по отдельным направлениям деятельности министерства.

Положения Федерального закона «О полиции» конкретизированы в Положении о Министерстве внутренних дел Российской Федерации [2], утвержденном Указом Президента РФ. В соответствии с Положением в целях осуществления своих полномочий МВД России имеет право:

формировать и вести в соответствии с законодательством Российской Федерации федеральные учеты, информационные системы, в том числе банки данных оперативно-справочной, розыскной, криминалистической, статистической и иной информации, а также пользоваться в установленном порядке учетами и информационными системами других федеральных органов исполнительной власти;

создавать в соответствии с законодательством Российской Федерации информационные системы, системы связи и передачи данных, а также использовать в своей деятельности достижения в области науки и техники, современные технологии и информационно-телекоммуникационную инфраструктуру;

применять в порядке, установленном законодательством Российской Федерации, электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, а также электронные формы взаимодействия с другими федеральными органами исполнительной власти, иными государственными органами, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, общественными объединениями и организациями и т.п.

Для реализации указанных полномочий созданы государственные информационные системы, базовые государственные информационные ресурсы и информационные ресурсы МВД России по направлениям деятельности.

МВД России является оператором пяти ГИС:

Федеральная автоматизированная дактилоскопическая информационная система (федеральная АДИС-МВД);

Система обеспечения предоставления информации МВД России в рамках межведомственного электронного взаимодействия МВД России (ВИС-СМЭВ);

Интегрированный банк данных федерального уровня (ИБД-Ф);

Государственная информационная система миграционного учета (ГИСМУ);

Государственная система изготовления, оформления и контроля паспортно-визовых документов нового поколения (ГС ПВДНП).

Для предоставления государственных услуг или исполнения государственных функций на уровне межведомственного взаимодействия в МВД России сформированы базовые государственные информационные ресурсы:

«Автомобиль» (подсистема «Транспортные средства») – о зарегистрированных транспортных средствах и их владельцах;

«Водитель» (подсистема «Водительские удостоверения) – о выданных водительских удостоверениях и других сведениях для допуска водителя к участию в дорожном движении;

«Адмпрактика» (подсистема «Административные правонарушения») – об административных правонарушениях в области обеспечения безопасности дорожного движения;

Единая автоматизированная информационная система технического осмотра транспортных средств;

Центральный банк данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, в том числе участников Государственной программы по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом;

Банк данных по учету иностранных граждан и лиц без гражданства, ходатайствующих о признании беженцами, лиц, признанных беженцами, лиц, обратившихся с заявлением о предоставлении временного убежища, лиц, получивших временное убежище, и прибывших с ними членов их семей, а также выдаваемых им документов, в том числе содержащих электронный носитель информации;

Учет выданных, утраченных и похищенных паспортов граждан Российской Федерации, удостоверяющих личность граждан Российской Федерации на территории Российской Федерации;

Базовый государственный информационный ресурс регистрационного учета граждан Российской Федерации по месту пребывания и по месту жительства в пределах Российской Федерации;

Общефедеральный учет выданных паспортов граждан Российской Федерации, удостоверяющих личность граждан Российской Федерации за пределами территории Российской Федерации, в том числе содержащих электронный носитель информации.

Большинство государственных услуг МВД России предоставляются в режиме «онлайн» на портале «Госуслуги» в сети Интернет.

В министерстве создано большое количество информационных ресурсов, которые используются для решения задач, стоящих перед отдельными подразделениями МВД России. Можно также отметить, что в едином информационном пространстве функционирует система электронного юридического значимого документооборота, внедрена ведомственная видеоконференцсвязь, электронная почта.

Технологической основой современного единого информационного пространства ОВД стала единая информационно-телекоммуникационная система органов внутренних дел, которая была создана в рамках выполнения Федеральной целевой программы «Электронная Россия (2002-2010 годы)» [3].

Необходимо отметить, что в процессе развития информационных ресурсов МВД России и совершенствования компьютерной сети министерства возникал вопрос, по какому пути пойти. Предлагалась реализация создания сети дешевая и быстрая – посредством арендованных каналов связи. Однако была выбрана концепция, позволяющая обеспечить соблюдение требование информационной безопасности – на основе собственных каналов связи. Несмотря на то, что еще используется много арендованных линий связи, в настоящий момент можно констатировать, что МВД России имеет свою, автономную корпоративную компьютерную сеть к которой подключено более полумиллиона пользователей.

В настоящий момент универсальной связующей сетью для работы единого информационного пространства МВД России является интегрированная мультисервисная телекоммуникационная система органов внутренних дел Российской Федерации, которая включает:

магистральную сеть передачи данных на базе собственных каналов, а также арендуемых каналов связи и сетей российских операторов связи;

сеть проводного доступа на базе линий связи МВД России, а также каналов связи, операторов проводной связи;

сеть беспроводного доступа на базе собственных технических средств и арендуемых у российских операторов сетей беспроводной связи;

подсистему мониторинга и управления сетью.

Отдельным направлением развития интегрированной мультисервисной телекоммуникационной системы стала организация мобильного доступа сотрудников патрульно-постовой службы, ДПС ГИБДД МВД России, участковых уполномоченных полиции и т.п. к информационным ресурсам с использованием 3G/4G сетей операторов связи либо систем спутниковой связи. Кроме доступа к информационным ресурсам, подразделения МВД России имеют возможность подключения к навигационным системам ГЛОНАСС и GPS.

Доступ к информации, поступающей от средств видеонаблюдения и контроля, предоставляется дежурным частям территориальных органов МВД России. Доступ к средствам видеонаблюдения и контроля, не находящимся на балансе подразделений МВД России, организовывается посредством шлюза между сетью МВД России и узлом подключения указанных средств на основании соглашений. Внешнее информационное взаимодействие МВД России с гражданами и сторонними организациями осуществляется через защищенный шлюз между интегрированной мультисервисной телекоммуникационной системой МВД России и информационно-телекоммуникационной сетью Интернет.

Необходимо отметить, что в 2010 – 2012 годах система информационного обеспечения органов внутренних дел претерпела значительные изменения. В процессе реформирования МВД России были созданы Департамент информационных технологий, свя-

зи и защиты информации Министерства внутренних дел Российской Федерации МВД России и ФКУ «Главный центр связи и защиты информации Министерства внутренних дел Российской Федерации» МВД России. В ведение Департамента были переданы вопросы защиты информации и связи, разработки и использования информационных технологий, которые ранее курировали разные подразделения, как в федеральном центре, так и в регионах. Таким образом, была создана дополнительная управленческая структура, которая определяет политику развития Министерства в информационной сфере. В качестве положительного эффекта необходимо отметить, что вопросы защиты информации, оказания государственных услуг в электронном виде и внедрение цифровых технологий впервые курируются одним подразделением, которое может определять вектор развития всех указанных направлений в комплексе.

Произошедшие организационные изменения привели к организационно-технической революции в области создания и функционирования единого информационного пространства МВД России.

С 2011 года в министерстве создается единая система информационно-аналитического обеспечения деятельности МВД России (далее – ИСОД МВД России) в соответствии с Приказом МВД России от 30.07.2011 № 891 «О мероприятиях по созданию единой системы информационно-аналитического обеспечения деятельности МВД России» [4]. ИСОД МВД России создается в рамках Государственной программы «Информационное общество (2011-2020 годы)» [5] на основании Концепции информатизации МВД России до 2012 года [6]. После опытной эксплуатации было принято решение о реализации программы по созданию ИСОД МВД России на базе ранее созданной ЕИТКС в полном объеме [7].

Система взглядов на дальнейшее развитие единого информационного пространства МВД России, изложенных в Концепции создания ИСОД, была пересмотрена и кардинально отличалась от принятых ранее. В отличие от предыдущих концепций, опиравшихся на создание обособленных информационных систем по каждому направлению деятельности, новый документ предусматривал централизацию информационных систем и ресурсов на единой технологической платформе.

Концептуальная архитектура ИСОД МВД России разрабатывалась с учетом применения передовой технологии облачных вычислений**,** позволяющей использовать единую технологическую платформу и обеспечить информационную поддержку оперативно-служебной деятельности сотрудников ОВД в режиме клиент – сервер.

К 2015 году в ИСОД МВД России было обеспечено функционирование подсистем и сервисов обеспечения повседневной и оперативно-служебной деятельности подразделений МВД России. Информация размещена в системе центров обработки данных МВД России, доступ к которым осуществляется через интегрированную мультисервисную телекоммуникационную сеть.

Таким образом, вопросы создания единого информационного пространства МВД России реализуются с 70-х годов XX века. Единое информационное пространство создается в соответствии с требованиями законодательства и предназначено для обеспечения выполнения функции министерства и обеспечения потребностей всех правоохранительных органов Российской Федерации. Однако только созданное в 2014-2015 годах информационное пространство МВД России можно назвать по настоящему единым, отвечающим всем современным требованиям.

Литература:

1. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ // Собрание законодательства РФ. 14.02.2011. № 7. Ст. 900.

2. Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних

дел Российской Федерации по субъекту Российской Федерации: Указ Президента РФ от 21.12.2016 № 699 // Собрание законодательства РФ. 26.12.2016. № 52 (Часть V). Ст. 7614.

3. Федеральная целевая программа «Электронная Россия (2002-2010 годы)»: Постановление Правительства РФ от 28.01.2002 № 65 // СЗ РФ. - 2002. - № 5. - Ст. 531.

4. О мероприятиях по созданию единой системы информационно-аналитического обеспечения деятельности МВД России: Приказ МВД России от 30.07.2011 № 891 // Доступ из Базы данных «Нормативно-правовые акты МВД России».

5. О государственной программе Российской Федерации «Информационное общество (2011 - 2020 годы): Распоряжение Правительства РФ от 20.10.2010 № 1815-р // Собрание законодательства РФ. 15.11.2010. № 46. Ст. 6026.

6. Об утверждении Концепции информатизации органов внутренних дел РФ и внутренних войск МВД России до 2012 года: Приказ МВД России от 04.04.2009 № 280 // Доступ из Базы данных «Нормативно-правовые акты МВД России».

7. Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012 - 2014 годах: Приказ МВД России от 30.03.2012 № 205 // Доступ из Базы данных «Нормативно-правовые акты МВД России».

8. Лапин В.В., Слесарева Е.А., Старостенко И.Н. Информационные системы в деятельности органов внутренних дел. Учебное пособие. – М.: Московский университет МВД России, 2014.

10. Прокопенко А.Н. Концептуальные вопросы создания единого информационного пространства МВД России // Общество и право. 2010. № 2. С. 284-287.

11. Прокопенко А.Н. Особенности правового регулирования формирования и использования информационных ресурсов МВД России после принятия ФЗ «О полиции» // Эволюция государственных и правовых институтов в условиях развития информационного общества / Сборник научных работ. – М.: ИГП РАН, юридическое издательство «ЮРКОМПАНИ», 2012. – С. 264–275.

Пузарин А.В., Иванов В.Ю.
Московский университет МВД России им. В.Я. Кикотя

ПРОБЛЕМЫ «DARK WEB» ДЛЯ ПОДРОСТКОВОГО ВОЗРАСТА

Подростковые годы являются серьезным испытанием для ребенка и его родителей. Подростки часто спорят с родителями, они пытаются добиться большей самостоятельности и минимума контроля со стороны взрослых.

В России ежедневно пользуются интернетом 89%, подростков 12–17 лет. В будние дни проводят в интернете от 3 до 8 часов 37% их них, в выходные — 47%. Мобильный интернет у детей в два раза более популярен, чем у их родителей.

Большинство подростков используют интернет для поиска интересной информации. На втором месте по популярности — поиск информации для учебы.

Как оказалось, почти треть опрошенных детей считают, что интернет лишен каких-либо недостатков, а у каждого десятого вызвал затруднения сам вопрос о «минусах» интернета.

Отличительная черта Интернета – его анонимность. Поэтому зачастую подросток с кем-то общаясь, даже не знает, кто скрывается за маской того или иного пользователя. В этом-то и беда, что Интернет «укрывает» злоумышленников.

В последнее время для полной анонимизации пользователи интернета пользуются сетью Tor или “черным интернетом”. В Википедии говорится, что Tor (сокр. от англ. The Onion Router)] – свободное и открытое программное обеспечение для реализации

второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

От обычного привычного интернета (даркнет, фринет – по всякому его именуют) черный интернет отличается запрещёнными сделками. Через запрещенный интернет идёт оружие, наркотики, фальшивые документы и так далее, а также идёт информация, которой нет в открытом доступе.

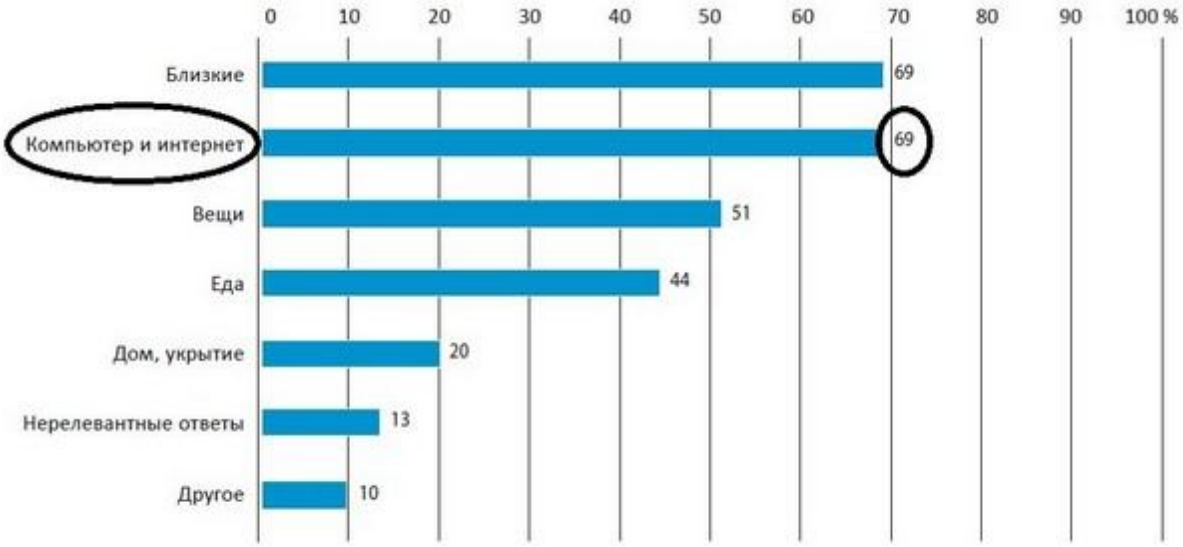


Рис. 1. Ответы подростков на вопрос «Что Вы взяли бы с собой на необитаемый остров?», в %. Выборка: подростки 12-17 лет, пользующиеся интернетом

Рис. 2. TOR Browser

Tor не позволяет стороннему пользователю узнать ваш ip-адрес, найти, где вы живёте, отследить маршрутизацию и историю просмотров страниц, посещаемых вами. В торе всё закрыто – там запутанные сети. Поэтому там всё работает и загружается медленно, а сайты выглядят примитивно, без всяких излишеств. Единственная цель – конфиденциальный обмен информацией. Там, на этих сайтах, продаётся буквально все. И без рецепта. И без разрешения. И закрыть эти сайты не могут ни ФСБ, и никакой-либо другой орган.

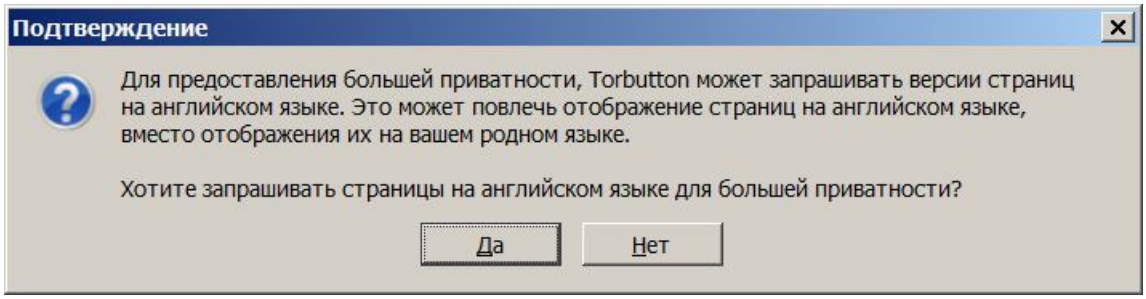


Рис. 3. Язык запроса страниц

Интерфейс браузера приведен на рисунке 2. Одним из параметров, которым можно деанонимизировать пользователя является разрешение экрана и количество мониторов, поэтому для обеспечения большей анонимности необходимо не разворачивать окно браузера на полный экран.

Еще одним из деанонимизирующим фактором является запрашиваемый язык у WEB-сервера язык страниц, рис. 3. Для обеспечения большей анонимности рекомендуется установить английский язык.

После завершения всех настроек узнаем свой IP-адрес, воспользуемся сервисом https://whoer.net, рис. 5.

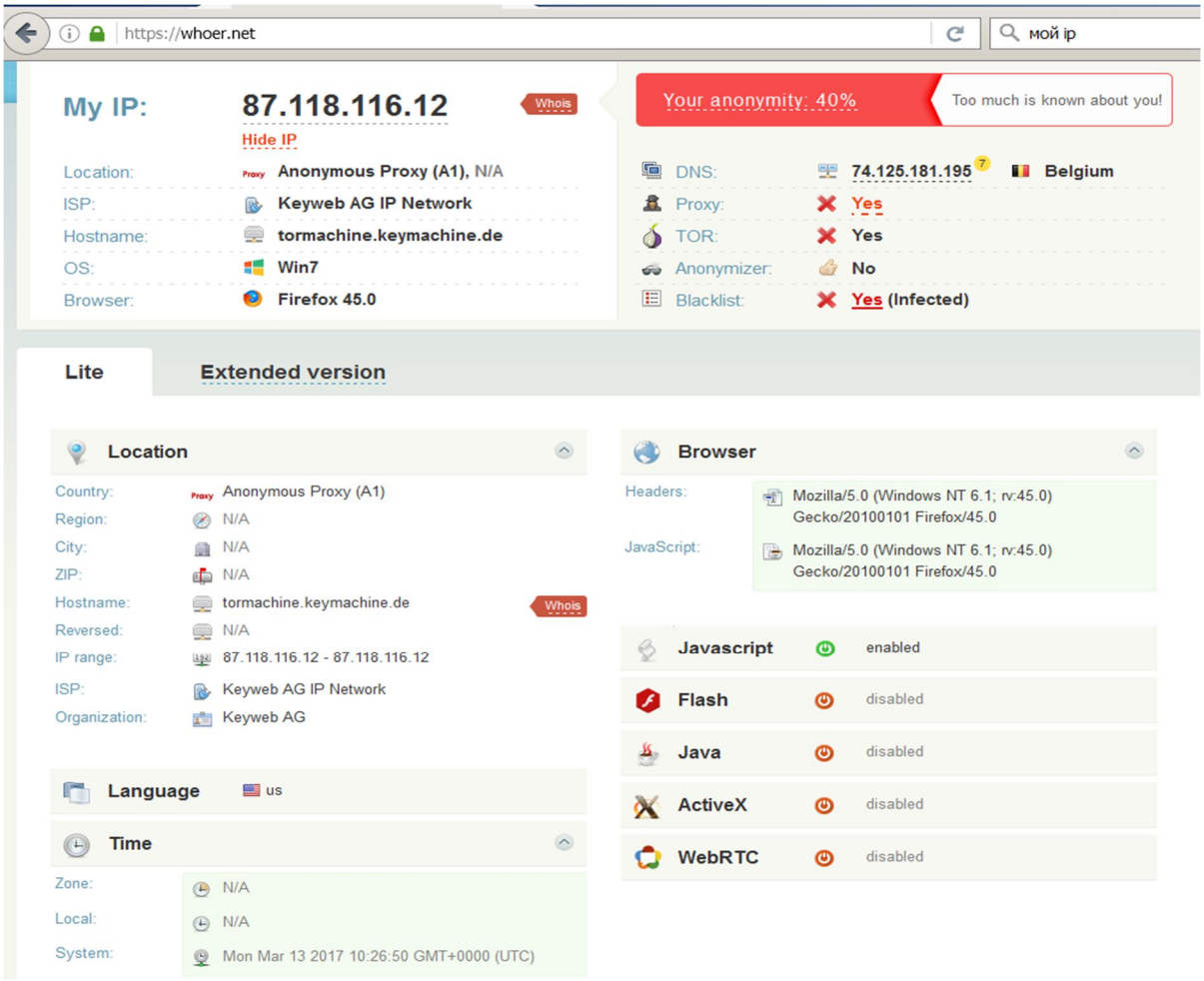


Рис. 4 whoer.net

В результате IP-адрес, который остается в логах веб-сервера изменился с 80.253.22.126 на 87.118.116.12.

С точки зрения пользователя цепочка TOR выглядит следующим образом, рис. 6

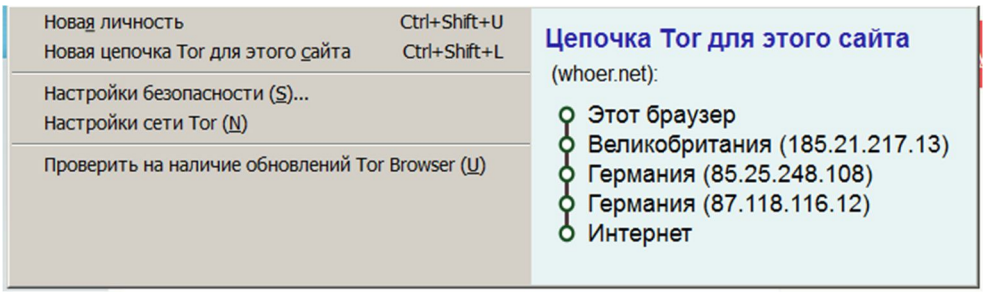


Рис. 5. Цепочка Tor для этого сайта

Еще одним способом обеспечения анонимности является использование подключение к удаленному VPN-серверу. Существует большое количество платных и бесплатных VPN-серверов с клиентами под любые платформы (от настольных компьютеров до мобильных устройств).

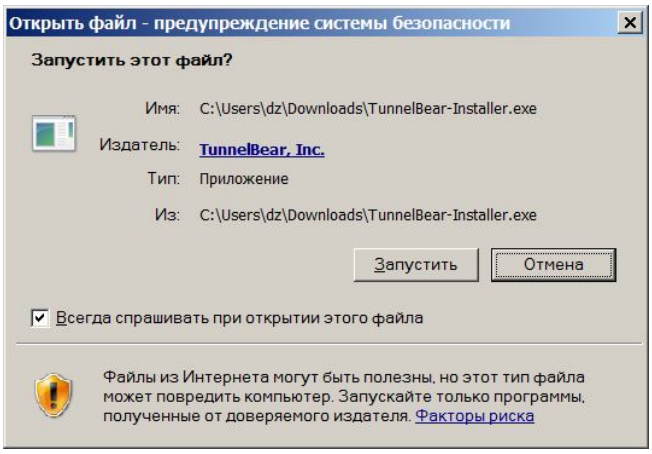


Рис. 6. Установка TunnelBear

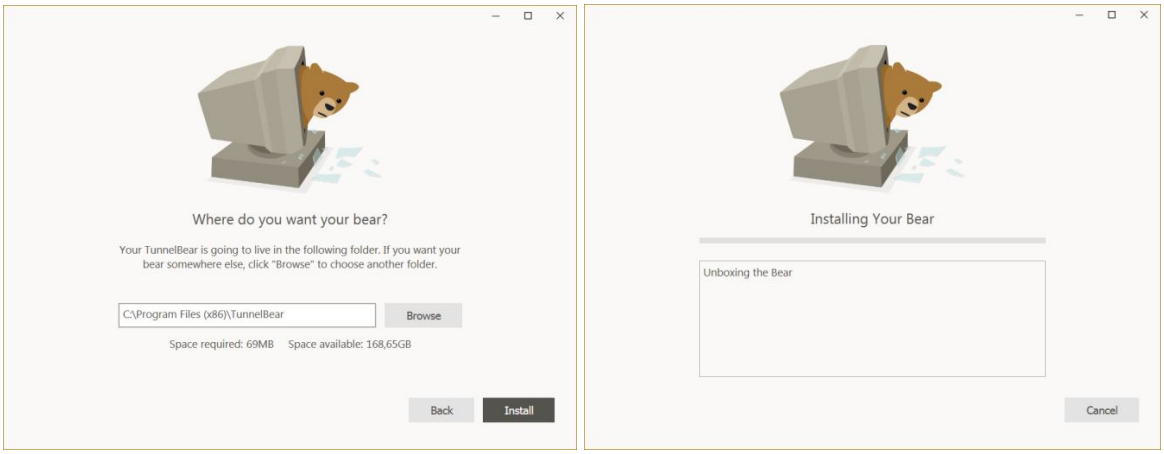


Рис. 7. Установка TunnelBear

Установка TunnelBear приведена на рисунке 8. После завершения установки необходимо авторизоваться в VPN-клиенте, рис. 9. Если учетная запись имеется, то необходимо ввести ее реквизиты. Если учетной записи нет, то необходимо создать учетную запись, щелкнув по ссылке Create a Free Account.

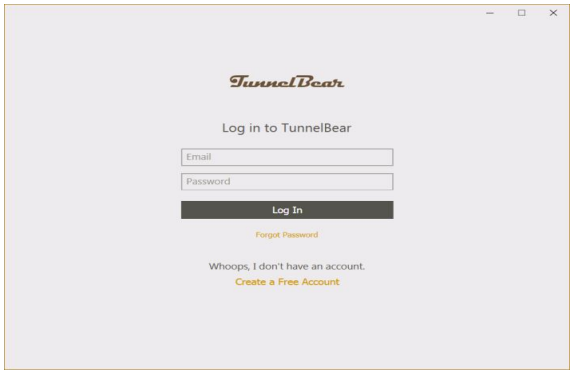


Рис. 8. Авторизация

После успешной авторизации необходимо выбрать VPN-сервер из имеющихся по всему миру и подключиться к нему, рис. 10

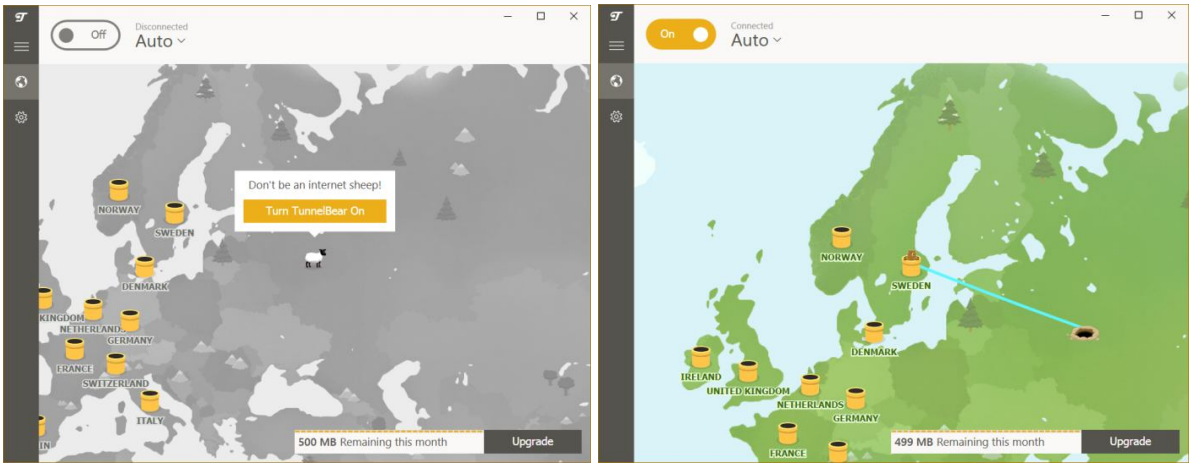


Рис. 9, 10. TunnelBear

Повторно проверим свой IP-адрес с помощью сервиса https://whoer.net, рис. 11. IP-адрес изменился и определяет регион как Швеция, Стокгольм.

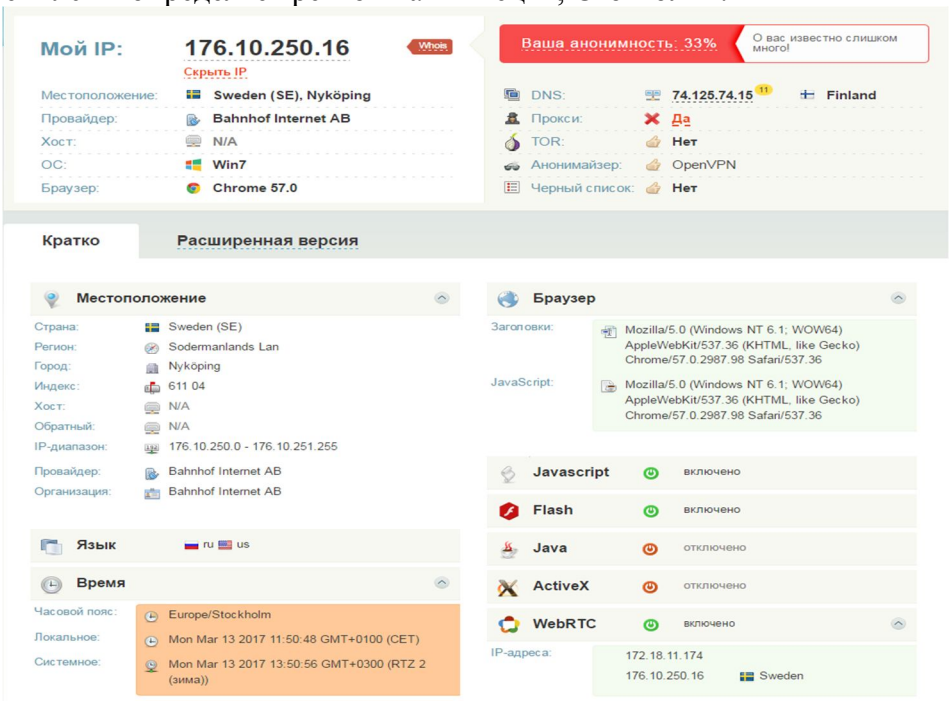


Рис. 11 Определение IP-адреса

Опасности в Интернете могут подстерегать каждого. Важно правильно пользоваться Сетью в любом возрасте. Важно составить список домашних правил пользования Интернетом. Следует поставить ограничение на общение в чатах. С подростками нужно вести беседы об их общении. При этом родители должны спрашивать об этом так, будто о реальных друзьях из школы. Можно интересоваться людьми, с которыми общается подросток при помощи мгновенных сообщений. Однако не следует устраивать допрос. Беседа должна быть дружеской. Иначе подросток не станет допускать родителей в свое личное пространство. Уберечь его от беды в этом случае будет непросто. Всю информацию, которую подросток найдет в Интернете, он может обсудить с родителями. Это не должно быть чем-то постыдным, запретным.

Рассмотрев основные опасности в Интернете, можно предпринять соответствующие действия, чтобы избежать негативных последствий.

Литература:

1. Электронный ресурс URL: https://100-k-1.ru/kogo-ili-chto-vy-vzyali-by-s-soboj-na-neobitaemyj-ostrov/

Разбегаев П.В.
Волгоградская академия МВД России

ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ: ИСТОРИЧЕСКИЙ АСПЕКТ

На современном этапе развития в Российской Федерации происходит внедрение новой образовательной системы, ориентированной на вступление во всемирное информационно-образовательное пространство. Благодаря этой тенденции электронные образовательные ресурсы (ЭОР), которые представляют собой не только образовательный контент в электронном виде, но также программное обеспечение, техническую и организационную поддержку учебного процесса, все чаще внедряются в практику высших учебных заведений.

Основой проектирования электронных образовательных ресурсов является информационно-образовательная среда учебного заведения, определяющаяся как программная система, которая обеспечивает единые технологические средства для проведения образовательного процесса, его информационного обеспечения и документирования [1].

Достижения в области компьютерных технологий и развитие интернета сделали возможным представлять учебную информацию с помощью различных электронных образовательных ресурсов, история развития которых начинает свое исчисление с 90-х годов, с момента появления первых электронных учебников.

Изучение исторического опыта электронного обучения имеет большое значение для определения взаимосвязи между развитием современных технологических стандартов и этапов возникновения и развития проектирования ЭОР. Это позволит создать эффективные стандарты ЭОР, которые бы соответствовали требованиям современных технологий.

Электронные образовательные ресурсы представляют собой учебные материалы, для воспроизведения которых применяются электронные устройства. ЭОР необходимы, в первую очередь, для экономии времени преподавателя. В электронном образовательном ресурсе могут использоваться аудио- и видеоматериалы, а также мультимедийные технологии.

Преподаватель в данной деятельности выступает в качестве куратора-менеджера обучения, наставника, готового предложить обучающимся весь требуемый набор учебных пособий, оказать необходимую помощь [2].

Образовательная информация применяется преподавателем в ЭОР как средство организации познавательной деятельности. Обучающийся в данном процессе также выступает в качестве субъекта деятельности, а его личностное развитие в ходе обучения выступает в качестве одной из основных образовательных целей [3].

Концепция ЭОР является общепринятой. В отличие от обычных образовательных ресурсов ЭОР можно трактовать как средство, предназначенное для получения образования, как ресурс, содержащий информацию образовательного типа. ЭОР включает в себя учебную, методическую, справочную, организационную и другую информацию, важную для продуктивной организации учебного процесса, представленного в цифровой форме. На современном этапе существует множество определений электронных образовательных ресурсов.

Следует отметить, что исследователи рассматривают электронные образовательные ресурсы как [4]:

1) материалы, созданные и применяемые в учебном процессе в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по разработке государственной политики и нормативно-правовому регулированию в области образования;

2) набор данных в электронной форме и средств информационно-коммуникационных технологий, который реализует возможности педагогической деятельности;

3) источник информации, содержащий графическую, текстовую, цифровую, речевую, музыкальную, видео, фото и другую учебную информацию;

4) интерактивное содержание (перемещение учебного объекта, к которому можно приблизиться, осмотреть со всех сторон; влияние на изучаемый процесс посредством изменения начальных условий).

Уникальное техническое свойство электронных образовательных ресурсов, по мнению А.В. Осина, заключается в способности объектов и процессов в ЭОР представляться как можно реалистичнее, используя мультимедиа, то есть все возможные способы представления: текст; звук; графику; фото; видео; анимацию, вплоть до объемных управляемых изображений [5].

Методологические различия в интерпретациях ЭОР позволяют преподавателю адекватно ориентироваться в многообразии электронных образовательных ресурсов. Еще одним из походов является понимание ЭОР как структурированного учебного материала, позволяющего сформировать у обучающегося личный тезаурус научно-предметных знаний, развить навыки владения профессиональными приемами, методами и способами их применения.

На сегодняшний день имеются разнообразные классификации электронных образовательных ресурсов: исходя из целей и вида преподавания, методологических оснований и функций обучения, технических характеристик применяемых технологий.

Электронные образовательные ресурсы можно классифицировать по следующим признакам: методу обучения; целевой аудитории и уровню образования; форме обучения; темы; цели и функциям, выполняемым в учебном процессе; виду учебной деятельности; характеру представленной информации; степени интерактивности; степени соответствия существующим государственным образовательным стандартам [6].

В настоящее время выделяются следующие виды ЭОР [3]:

- электронный учебно-методический комплекс (ЭУМК), обеспечивающий комплексную поддержку всех видов учебных занятий, предусмотренных программой соответствующей дисциплины;

- электронный учебный модуль (ЭУМ), поддерживающий все виды занятий по разделу (теме) учебной дисциплины;

- электронное учебное пособие;
- электронное методическое пособие;
- электронный задачник;
- средства поддержки практических занятий;
- компьютерные модели изучаемых процессов и объектов;
- лабораторный практикум, обеспечивающий удаленный доступ к реальному оборудованию;
- Интернет-ресурсы;
- модули проверки знаний по разделам (темам дисциплины);
- атласы конструкций и деталей изучаемого оборудования;
- средства обработки и визуализации результатов исследований;
- компьютерные тренажеры;
- базы данных учебного назначения.

Также существует деление по следующим видам:

- учебные (обеспечивают качественное усвоение учебного материала, могут составить основу формирования компетентности обучающихся);
- самостоятельные (способствуют выполнению различных видов самостоятельных работ, выработки способности анализировать и отбирать нужный учебный материал, навыков критического мышления обучающихся);
- демонстрационные (дают возможность осуществлять процесс визуализации исследуемых объектов, явлений, действий, способствуя наглядному представлению образовательной информации);
- тренинговые (предусмотрены с целью отработки различного рода умений и навыков, повторения и укрепления изученного материала);
- диагностирующие и тестирующие (дают оценку знаний, умений, способностей, определяют степень обученности, развития личностных свойств, уровень интеллектуального развития);
- контролирующие (позволяют автоматизировать процессы контролирования результатов изученного материала, выявления степени освоения образовательной информации) [7];
- экспертные (распоряжаются образовательным процессом, образуют диалог между пользователем и обучающей системой при решении учебной задачи);
- коммуникативные (предоставляют доступ к любым данным в локальных и глобальных сетях, удаленное интерактивное взаимодействие субъектов образовательного процесса);
- вычислительные (автоматизируют процессы обрабатывания результатов обучения, расчетов, измерений в изучаемых процессах и явлениях);
- сервисные (занимаются обеспечением защищенности и удобства работы пользователя в сети);
- досуговые *(к*омпьютерные игры и ресурсы компьютерной коммуникации для обеспечения досуговой деятельности, самостоятельной работы и индивидуального формирования умений и навыков обучающихся).

Специалисты выносят на обсуждение следующие критерии оценки качества электронных образовательных ресурсов:

- соответствие образовательной программе;
- научная аргументированность представляемого материала;
- соотношение общей методологии («от простого к трудному», выполнение очередности представления материалов и т.д.);
- отсутствие фактографических погрешностей, безнравственных, неэтичных данных;

- приемлемость научно-технических свойств учебного продукта (к примеру, свойство полиграфии),

- предоставление абсолютно всех элементов образовательного процесса (получение данных; практические занятия; аттестация (контроль учебных достижений)).

Все виды ЭОР в образовательном процессе имеют ограниченный круг характерных задач, поэтому их применение возможно и в качестве вспомогательного материала в образовательном процессе с традиционными педагогическими технологиями и в сочетании друг с другом. Все они способствуют повышению наглядности и доступности обучения.

Компьютерные технологические процессы формирования, сбережения и распространения познаний, в том числе технологии для проектирования электронных образовательных ресурсов, непосредственно связаны с проблемами создания искусственного интеллекта.

Идея создания искусственного интеллекта, похожего на человеческий мозг, была озвучена еще в XIV в. Р. Луллием, вслед за которым Г. Лейбниц и Р. Декарт в XVIII веке продолжили попытки создания искусственного разума посредством систематизации понятий всех наук. Активное формирование интеллектуальных систем берет свое начало с компьютерной эпохи.

Для автоматизированных обучающих систем (АОС) особенно существенную роль играют такие важные направления как автоматическое распознавание семантики текста и речи, извлечение и структурирование знаний, формирование баз данных образовательных ресурсов, поиск необходимых сведений в большом объеме информации [8].

В истории развития проектирования электронных образовательных ресурсов можно выделить четыре основных этапа. Начало формирования электронных образовательных ресурсов было положено дистанционным обучением, которое возникло со времен появления почты, когда преподаватель мог отсылать обучающимся учебные материалы для самостоятельного образования.

Первый этап развития электронных образовательных ресурсов начинается в начале 90-х годов, когда появляются первые персональные компьютеры и электронные учебники. Данный этап характеризуется активным использованием электронных образовательных ресурсов в виде презентация и программ тестирования, разработкой электронных учебников, возможностью без труда распространять учебные материалы [9].

После принятия концепции создания и развития дистанционного образования в 1992 году, в некоторых крупных университетах страны были введены первые прообразы систем дистанционного образования.

Отечественные исследователи в конце 1980-х - начале 1990-х годов на базе Новосибирского государственного университета создали большой ряд советских систем ЭОР. В НГУ образовательная система терминал ТЕВУС (1982-1983) проработала около десяти лет. В течение этого времени она использовалась более чем в 150 вузах СССР, включая Московский государственный университет [10].

Первая система обучения с использованием электронных образовательных ресурсов онтологии предметных областей была система CTS, созданная на базе МГТУ им. Н.Э. Баумана в 1993 г. В нынешнем варианте методика делимых единиц контента на основе онтологического подхода, показана в концепции БиГОР [11].

В 1993 году, международная ассоциация AICC выпускает спецификацию под названием CMI001 (Guidelines for Interoperability), в которой были представлены требования к взаимодействию учебного материала и компьютерной системы управления обучением. Это были первые документы, регламентирующие электронные образовательные ресурсы [12].

2000 год характеризуется наступлением периода централизации в образовательных информационных технологиях. Начинают активно использоваться системы управления обучением, в международном формате принято использовать определение Learning manager system (LMS).

В 1997 году компанией IMS был разработан проект глобального консорциумного обучения (IMS Global Learning Consortium), который первоначально был ориентирован на разработку стандартов электронного обучения для высшего образования. В 2000 году был реализован стандарт IMS QTI (унифицированные вопросы и тесты).

Подход к типизации электронных образовательных ресурсов у IMS носит систематический характер: каждое из направлений взаимодействия обучаемого, образовательного материала и системы управления обучением описано в отдельном документе. Такого рода стандарт дает возможность без ограничений обмениваться средствами создания учебных материалов, систем тестирования и т. д.

Между 2000 и 2004 годами, начинают активно разрабатываться стандарт в области электронных образовательных ресурсов, а к 2004 году был запущен процесс централизации и проектирование ЭОР стало обще популярным явлением. Начали появляться в большом количестве системы, поддерживающие ЭОР. Возникла потребность централизовать систему ЭОР, что позволило координировать имеющиеся системы с целью создания общей среды, которая поддерживается и управляется централизованно. С 2004 по 2008 год происходит активное развитие и формирование облачных сервисов и постепенный переход проектирования ЭОР в «облако», который можно назвать третьим этапом развития ЭОР.

Благодаря организации образовательного процесса, реализуемого при помощи облачных технологий, создаются условия для развития профессиональной педагогической деятельности и реализации новых возможностей проектирования ЭОР.

Создание новых ЭОР при помощи облачных технологий способствовало более эффективному формированию познавательной деятельности, развитию аналитических способностей, познавательных потребностей, функции передачи и воспроизводства социального опыта с применением данных технологий, созданию условий, позволяющих стимулировать познавательную активность обучаемых, исследовательские и проектные навыки и развитие общеинтеллектуальных умений [13], [14].

С 2008 года и по настоящее время сформировался последний на современном этапе развития этап, который характеризуется революцией в области открытия массовых открытых онлайн-курсов.

На сегодняшний день многие отечественные университеты занимаются разработкой собственных ЭОР, а общемировая тенденция заключается в том, чтобы сделать их открытыми и универсальными. Происходит процесс интеграция баз ЭОР разных вузов, а также унификация и стандартизация интерфейсов.

Работу в этом направлении ведут разные организации Образовательный консорциум по проблемам систем управления обучением IMS GLC (Instructional Management Systems Global Learning Consortium); Комитет стандартизации в области технологий обучения LTSC (Learning Technology Standards Committee in Institute of Electrical and Electronic Engineers); организация «Продвинутое распределенное обучение» ADL (Advanced Distributed Learning Initiative, США) [15].

Формирование проектирования ЭОР вызвало необходимость унификации системы электронных образовательных продуктов и разработки единого формата функционирования. Общим итогом стало создание открытой образовательной модульной мультимедийной системы. Ресурсы, созданные в данной системе, именуются ЭОР нового поколения, которые становятся полноценным инструментом образовательной деятельности.

Применение электронных образовательных ресурсов раскрывает высокие возможности образовательного процесса. Они имеют все шансы гарантированной результативности в обеспечение продуктивности не только системы образования, но и развития общества в целом.

История развития проектирования электронных образовательных ресурсов можно разделить на четыре основных этапа. Каждый этап характеризуется появлением новой технологии, формы ЭОР и стандарта.

Первый этап (начало 90-х – 2000 г.) – характеризуется активным использованием электронных образовательных ресурсов в виде презентаций и программ тестирования, разработкой электронных учебников, возможностью без труда распространять учебные материалы.

Второй этап (2000-2004 гг.) – характеризуется процессом централизации в образовательных информационных технологиях, который привел к координации существующих систем с целью создания единой среды, поддерживаемой и управляемой централизованно. Начинают активно использоваться СДО - системы управления обучением.

Третий этап (2004-2008 гг.) – характеризуется активным развитием и формированием облачных сервисов и постепенный переход ЭОР в «облако», позволяющее более эффективно осуществлять формирование познавательной деятельности и создание условий, позволяющих стимулировать познавательную активность обучаемых, исследовательские и проектные навыки, развитие общеинтеллектуальных умений и т.д..

Четвертый этап (2008 - по настоящее время) – характеризуется развитием массовых открытых онлайн-курсов, происходит процесс интеграция баз ЭОР разных вузов, а также унификация и стандартизация интерфейсов.

Таким образом, в настоящее время использование современных информационных технологий, внедрение современных электронных образовательных ресурсов играет важную роль в системе образования. Именно электронные образовательные ресурсы выступают одним из основных ключевых показателей развития образования.

Литература:

1. Разбегаев П.В. Электронная информационно-образовательная среда образовательной организации МВД России. // Математические методы и информационно-технические средства: материалы XII Всерос. науч._практ. конф., 17 июня 2017 г. / ред. кол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2017.

2. Суворова Т.Н., Исупова Н.И. Электронные образовательные ресурсы как ключевое понятие информатизации образования // Научные труды SWorld. 2016. Т. 4. № 2 (43). С. 11-15.

3. Лежнина М.В. Электронные образовательные ресурсы, виды, классификации // В сборнике: НАУКА СЕГОДНЯ сборник научных трудов по материалам международной научно-практической конференции. Научный центр «Диспут». 2014. С. 52-53.

4. Использование электронных образовательных ресурсов нового поколения в учебном процессе: Научно-методические материалы / Г.А. Бордовский, И.Б. Готская, С.П. Ильина, В.И. Снегурова - СПб.: Изд-во РГПУ им. А.И. Герцена, 2007. С. 24.

5. Осин, А.В. Открытые образовательные модульные мультимедиа системы / А.В. Осин. - М.: Агентство «Издательский сервис», 2010. С. 125.

6. Электронные образовательные ресурсы (Общие положения). - М., 2011. С. 5.

7. Разбегаев П.В. Инновационные оценочные средства в оценке уровней сформированности компетенций //Процесс формирования компетенций: проблемы эффективности [Электронный ресурс] : сб. науч. тр. / редкол. : А. А. Тимофеева [и др.]. – Электрон. дан. (2,8 Мб). – Волгоград: ВА МВД России, 2015.

8. Шевко Н.Р. Проблемы определения информационной компетентности на современном этапе. // Ученые записки КГАВМ. Т. 212. – Казань, 2012. С. 505.

9. Казанская О.В. От дистанционного обучения к электронному / О.В. Казанская // Информационные технологии в образовании. - 2009. - № 1 (17). - С. 4-5.

10. Можаева Г.В. Электронное обучение в вузе: современные тенденции развития / Г. В. Можаева // Гуманитарная информатика. - 2013. - № 3. - С. 126-138.

11. Норенков И. П. Электронные образовательные ресурсы. М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. С. 48.

12. Калдыбаев С.К., Онгарбаева А.Д. Электронные образовательные ресурсы: роль и назначение // Международный журнал экспериментального образования. 2016. № 11-2. С. 159-161.

13. Шевченко В.Г. Применение облачных технологий в обучении // Педагогическая информатика. - 2013. - №1. С. 84.

14. Разбегаев П.В. Формирование самостоятельной деятельности у курсантов в обучении информатике с использованием облачных технологий // Математические методы и информационно-технические средства: материалы XII Всерос. науч._практ. конф., 17 июня 2016 г. / ред. кол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2016.

15. Андреев, А.А. Российские открытые образовательные ресурсы и массовые открытые дистанционные курсы / А.А. Андреев // Высшее образование в России. - 2014. - № 6. -С. 150-155.

Ремизов Ю.А., Алымов Н.Л.
Академия ФСО России, г. Орел

ПРИМЕНЕНИЕ КОМПЛЕКСА ВИРТУАЛЬНЫХ ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Один из самых основных методов закрепления теоретических знаний и обучения практическим навыкам и умениям это лабораторные работы. Применение автоматизированных измерительных систем является одним из приоритетных направлений развития метрологии, как науки об измерениях, методах и средствах обеспечения их единства и требуемой точности. Для обеспечения качественного образования требуется высокий уровень технической оснащенности учебных лабораторий, предполагаемый полную или частичную автоматизацию приборов. Министерства образования и науки последними указаниями обязывает учебные заведения повсеместно внедрять в образовательный процесс информационные технологии.[1]

Основная проблема, с которой сталкиваются обучающиеся при проведении лабораторных работ – недостаток времени для качественного проведения нескольких видов измерений и полноценной обработки их результатов. Лаборатория измерительной техники, имеющаяся на кафедре, в значительной степени перегружена (в течение одного семестра через нее проходят более пятнадцати учебных групп, в каждой группе до восьми лабораторных работ), а в послеобеденное время лаборатория, как правило, занята подготовкой к новому занятию или ремонтом оборудования. Кроме того, для работы с электроустановками, имеющими питающее напряжение, опасное для жизни, требуется присутствие либо преподавателя, либо инженера лаборатории, что для внеплановых занятий не всегда возможно.

К этому добавляются трудности, связанные с реализацией обучающимися обязанностей военной службы (нарядами), участием в различных спортивных мероприятиях и болезнями. Таким образом, становится актуальной задача предоставления возможности проведения измерительных экспериментов с моделями исследуемых объектов и виртуальными средствами измерений во внеурочное время.

Выделяется несколько этапов при выполнении лабораторных работ: теоретическая и практическая подготовка; выполнение задания лабораторной работы; обработка результатов и оформление отчета.

Как показывает опыт, большая часть времени у обучающихся уходит на подготовку, а также на обработку результатов измерений и оформление отчета лабораторной работы (ЛР). На сам эксперимент времени остаётся мало, хотя именно получение практических навыков работы с физическими приборами и является одной из целей лабораторного курса. Нехватка времени на освоение сложной аппаратуры, имеющей более десяти органов управления и разъемов, является проблемой обучающихся при выполнении практических работ. Поэтому логично предположить, что работа с виртуальными моделями позволит решить эту проблему. Выполнение задания ЛР на персональной ЭВМ, не требует присутствия обучающегося в лаборатории измерительной техники.

Разработанный и внедренный метод, использующий комплекс виртуальных лабораторных работ как раз и предназначен для повышения эффективности преподавания дисциплины "Метрология, стандартизация и сертификация в инфокоммуникациях" за счет использования информационных технологий, а также применения виртуального лабораторного практикума, моделирующего реальный эксперимент при проведении измерений во время лабораторной работы. Виртуальные лабораторные работы охватывают темы:

– «Исследование аналоговых и цифровых вольтметров».

– «Исследование возможностей измерительных генераторов».

– «Исследование параметров радиоэлектронных элементов с помощью типовых измерительных приборов».

– «Исследование возможностей электронно-лучевого осциллографа».

– «Исследование возможностей электронно-счетных частотомеров при измерении частотных и временных параметров».

– «Измерение рабочего затухания и усиления типовых каскадов средств связи с помощью комплекта измерительных приборов ИК-300».

– «Измерение параметров амплитудно-модулированных и частотно-модулированных сигналов и нелинейных искажений с помощью типовых измерительных приборов».

– «Исследование параметров измерительных радиотехнических сигналов».

Для реализации метода требуется доступ к ПЭВМ и среда программирования *LabVIEW*, что в настоящее время в стенах большинства ВУЗов практически осуществимо. Кроме того, для углубленного самостоятельного изучения курса ЛР по метрологии не запрещается использование и домашних компьютеров.

Разработанные виртуальные модели средств измерений предлагается использовать и для повышения эффективности подготовки обучающихся к лабораторным работам. Изучив накануне переднюю панель электронной копии измерительного прибора и отработав порядок подготовки его к работе, обучающийся сможет быстрее и правильнее воспользоваться физическим прибором при проведении реальных лабораторных работ.

Виртуальная модель измерительного прибора представляет собой сложную структуру различных преобразователей электрического сигнала, смоделированных на основе их математического представления на ЭВМ.

Рис. 1. Структурная схема лабораторной работы

Структурная схема виртуальной лабораторной работы представлена на рисунке 1. В разработанных в среде *LabVIEW* виртуальных приборах (ВП) имитируются внешние интерфейсы и работа реальных приборов, таких как генераторы, осциллографы, вольтметры и др. Набор инструментов этих ВП позволяют измерить, сохранить и представить полученные данные для анализа. На каждый ВП разработана лицевая панель (пользовательский интерфейс) с органами управления и индикаторами, аналогичными типовым приборам и обладающими всеми метрологическими характеристиками, присущими им.

Дополнительно разрабатывается модель исследуемого объекта с характеристиками (параметрами, свойствами), аналогичными реальному объекту. ВП, используются каждым обучающимся одинаковые, но за счет того, что объекты исследования могут видоизменяться, результаты измерений получаются индивидуальными для каждого обучающегося. Вариативность полученных результатов при проведении виртуальных экспериментов подразумевает и различные выводы по результатам анализа работы, что обеспечивает персонификацию оценки каждого обучающегося.

Виртуальный измерительный прибор, с помощью устройств ввода/вывода, линии связи и дополнительного программного обеспечения (драйверов), подключается к стандартному порту ПЭВМ, что позволяет измерять и реальные физические объекты. Для этих целей лабораторная установка (объект измерения) позволяет работать со всеми портами типовой ПЭВМ (*LPT, COM, PCI, USB* и др.). На перспективу, объекты измерения могут предоставляться обучающемуся удаленно по локальной сети, либо с использованием *Internet*.

Так как обучающийся при выполнении лабораторной работы существенную часть времени тратит на сборку схемы, освоение органов управления новых средств измерений и процедуры проведения их подготовки к работе (калибровки), то теперь он имеет возможность, загрузив виртуальный лабораторный практикум, испытать работу ВП на правильно собранной схеме. Это также позволит обучающемуся заранее подготовиться к выполнению лабораторной работы, освоив порядок работы с реальными средствами измерений в различных режимах. Он получает возможность, без боязни вывести из строя (сломать) вследствие неумелого использования, практически применять изучаемые средства измерений. Итоговый файл данных также помогает подготовке, так как обучающийся может заранее провести анализ результатов и сделать выводы в соответствии с заданием лабораторного практикума.

Использование технологий виртуальных инструментов позволяет полностью воспроизводить интерфейс реального прибора в виде виртуальной модели и сохранить все его функциональные возможности.

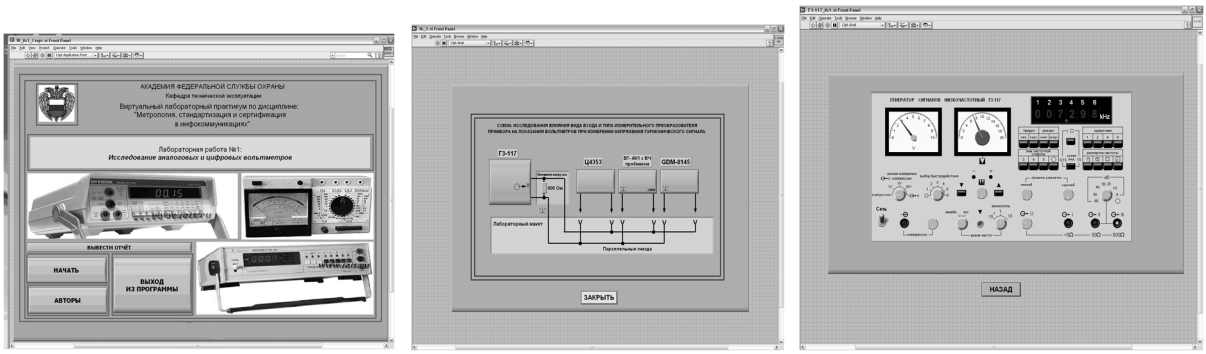


Рис. 2. Примеры лицевых панелей виртуального лабораторного практикума по ЛР№1 «Исследование аналоговых и цифровых вольтметров»

Обучающийся запускает программу на своём компьютере и, работая с ней согласно описания лабораторной работы, приобретает практические навыки эксплуатации приборов и осваивает методику проведения измерений. Это значительно экономит время на практических занятиях. Кроме того, при формировании эмулятора используются модели устройств, работающие по тем же принципам, что и реальные. Изменяя их параметры и принцип работы можно наблюдать, как это изменение отразится на результатах измерений. В качестве дополнительных исследовательских работ по соответствующим курсам, возможно обучающимися давать задание на самостоятельное проектирование подобных компонентов.

Примеры лицевых панелей виртуального лабораторного практикума по ЛР№1 приведены на рисунках 2, 3.

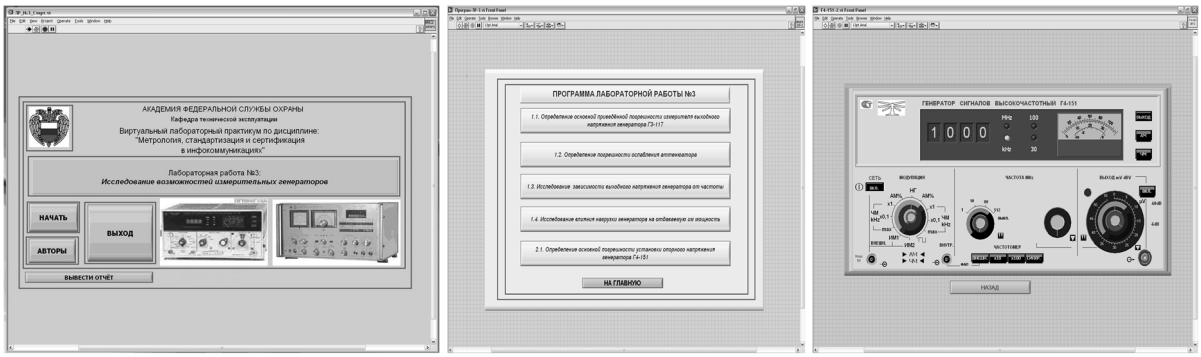


Рис. 3. Примеры лицевых панелей виртуального лабораторного практикума по ЛР№3 «Исследование возможностей измерительных генераторов»

В результате применения виртуальных моделей мы получаем следующие основные возможности: качественной подготовки обучающихся к выполнению лабораторных работ и работе с реальными средствами измерений; углублённого изучения обучающимися явлений в измерительных системах при проектировании моделей таких систем и средств измерений; подготовки обучающихся, решая реальные, а не абстрактные измерительные задачи; проведения измерительных экспериментов на виртуальных моделях при дистанционном обучении. [2]

Литература:

1. Ходжаев И.А., Алымов Н.Л., Ремизов Ю.А. Формирование компетенций дисциплины "Метрология, стандартизация и сертификация в инфокоммуникациях" согласно требованиям ФГОС ВПО // сборник научных трудов XIII Международной научно-методической конференции ВУЗов и факультетов, "Инфокоммуникационные технологии и системы связи", 2014 – Ярославский государственный университет им. П.Г. Демидова, г. Ярославль

2. Воронцов Е.В. и др. Применение способа виртуальных тренировок при подготовке к лабораторным работам по дисциплине «Метрология, стандартизация и сертификация в инфокоммуникациях» // инновационный метод, свидетельство о регистрации №0156 от 28.10.2014 г. – Академия ФСО России, 2014

Романов Н.А., Мещеряков Д.С., Басан Е.С.
Институт компьютерных технологий и информационной безопасности
Инженерно-технологическая академия г. Таганрог

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЗАЩИЩЕННОСТИ И ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ ДЛЯ МАЛОГАБАРИТНЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

В наше время благодаря новым информационным технологиям и всеобщей компьютеризации, малые беспилотные летательные аппараты (МБПЛА) используются все чаще и чаще. Они задействуются во всех сферах жизни. В земледельческой отрасли их используют, для точного земледелия – так называется комплексная система агроменеджмента, при которой с помощью высокотехнологичного оборудования более продуктивно выращивают урожай, основываясь на анализе состояния почвы и внешних факторов. В подразделениях МЧС России их используют для многих задач: поиска объектов, мониторинга района катастрофы, контроль заторов, поиск пострадавших, использование в качестве ретранслятора. Обычные пользователи могут использовать МБПЛА для фото, видео сьемки или просто для отдыха.

В связи с распространением МБПЛА, возникает проблема защиты аппаратов от несанкционированного доступа. Злоумышленники могут получить доступ к информации, передаваемой беспилотным аппаратом, могут получить доступ к показанию датчиков или видео камере. Для того чтобы пресечь данные нарушения, нужно развивать безопасность МБПЛА.

Целью создания стенда является создание набора образов виртуальных машин со встроенными уязвимостями.

Цель конкретизируется задачами:

1.Изучение банка данных угроз ФСТЭК, выбор угроз характерных для малогабаритных беспилотных летательных аппаратов (МБПЛА).

Из банка данных угроз ФСТЭК можно выделить несколько угроз, характерных для МБПЛА:

УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации [1]

Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путем подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.

Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок. Эта угроза характерна для автономных МБПЛА, т.к. на нем присутствует большое количество датчиков.

УБИ.069: Угроза неправомерных действий в каналах связи [2].

Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику.

Эта угроза характерна для автономных МБПЛА, т.к. для передачи данных используются радиопередатчики.

УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными [3]

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов.

Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными.

2. Обнаружение и исследование уязвимостей, характерных для МБПЛА, отсутствующих в банке данных угроз ФСТЭК.

– Угроза подмены источника радиосигнала. Угроза заключается в возможности нарушителем подмены источника радиосигнала и дальнейшими манипуляциями с МБПЛА. Данная угроза обусловлена слабостями протоколов и возможностью пеленгации радиосигнала Реализация данной угрозы возможна при условии получения доступа к линиям связи системы

– Угроза радиопеленгации. Угроза заключается в возможности злоумышленником определения направления источника радиосигнала. Имея знания о направлении сигнала, злоумышленник может провести атаку на источник или вызвать помехи сигнала. Реализация данной угрозы возможна при условии получения доступа к линиям связи системы.

3. Разработка модели угроз и уязвимостей для МБПЛА

– Угроза радиопеленгации. Уязвимость заключается в том, что в nRF24L01+ имеется 126 каналов с шагом 1 МГц [4]. Зная это, с помощью перебора каналов, можно найти нужный канал.

– Угроза искажения вводимой и выводимой на периферийные устройства информации и Угроза отключения контрольных датчиков

– Угроза неправомерных действий в каналах связи. Уязвимость заключается в том, что nRF24L01+ может принимать данные без проверки CRC. Это возможно если перевести nRF24L01+ в смешанный режим. Для этого устанавливаем длину адреса в 2 байта, а сам адрес как 0x00AA (Рисунок 1).

4.Возможные способы реализации угроз безопасности информации

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

– Несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

– Несанкционированного доступа и (или) воздействия на объекты на сетевом

уровне (сетевое оборудование, сетевые приложения, сервисы);

– Несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации.

5. План реализации атаки

План реализации

1. Поиск канала
2. Обход CRC проверки
3. Обработка данных
4. Перехват управления

1. Ищем нужный нам адрес и канал.

2. Изменение регистра AW nRF24L01+ для получения данных без проверки CRC.

3. Фильтруем получаемые данные, установив длину пакета до 10 байт.

4. Просматривая и разбирая протокол, смотрим за что отвечает каждый байт. Какой отвечает за газ, тангаж, рысканье, крен. После этого формируем собственные пакеты, в котором передаются значения изменения положения МБПЛА.

Реализация атаки внешнего злоумышленника на МБПЛА. nRF24L01+ не имеет promiscuous mode. Однако мы можем перевести nRF24L01+ в promiscuous mode – установив длину адреса в 2 байта, а сам адрес как 0x00AA или 0x0055.

03	SETUP_AW				Setup of Address Widths (common for all data pipes)
	Reserved	7:2	000000	R/W	Only '000000' allowed
	AW	1:0	11	R/W	RX/TX Address field width '00' - Illegal '01' - 3 bytes '10' - 4 bytes '11' – 5 bytes LSByte is used if address width is below 5 bytes

Рис. 1. Datasheet nFR24

В одном из вариантов мы будем получать данные, сдвинутые на 1 бит. Кроме того, можно принимать данные без проверки CRC. После этого для реализации перехвата управления МБПЛА, нам нужно убрать в библиотеке RF24 проверку валидности (рис.).

```
void RF24::setAddressWidth(uint8_t a_width){

    if(a_width -= 2){
        write_register(SETUP_AW,a_width%4);
        addr_width = (a_width%4) + 2;
    }else{
        write_register(SETUP_AW,0);
        addr_width = 2;
    }

}
```

Рис. 2. Проверка валидности в RF24

После этого происходит поиск канала и адреса МБПЛА. Так как для газа, рысканья, крена и тангажа используются отдельные каналы, то смотрим каналы с самой большой активностью. Так же при наблюдении за МБПЛА мы можем наблюдать изменения на каналах и таким образом найти нужный нам канал и понять за что он отвечает (газ, рысканье, крен и тангаж).

Выяснив адрес и канал МБПЛА, мы устанавливаем адрес для фильтра и начинаем обрабатывать данные, просматривая список пакетов можно заметить, что первые заканчиваются на 02 (Рисунок 3), а дальше идут помехи, которые мы можем убрать, сменив длину пакета.

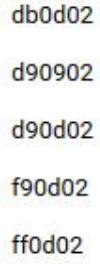


Рис. 3. Фильтрованные пакеты для тангажа

Таким образом мы получаем знание о том, как формируются пакеты. После этого мы можем создавать собственные пакеты и посылать на МБПЛА. Для этого нам требуется создать пакет и направить его на один из четырех каналов, отвечающих за управление. Поэтому для непосредственного управления МБПЛА в режиме реального времени нужно постоянно отправлять пакеты для управления.

Таким образом произведя атаку на МБПЛА, мы увидели недокументированные недостатки nRF модулей. Для того чтобы такие атаки не работали стоит ввести шифрование пакетов при передаче от источника к приемнику.

Работа выполнена при поддержке Гранта РФФИ № 17-07-00106 Разработка метода и эффективной системы защиты беспроводных сенсорных сетей от активных атак злоумышленников.

Литература:

1. БДУ ФСТЭК России [Электронный ресурс] // bdu.fstec.ru: Банк данных угроз безопасности информации. URL: http://bdu.fstec.ru/threat/ubi.027 (дата обращения: 9.06.2018)

2. БДУ ФСТЭК России [Электронный ресурс] // bdu.fstec.ru: Банк данных угроз безопасности информации. URL: http://bdu.fstec.ru/threat/ubi.069 (дата обращения: 9.06.2018)

3. БДУ ФСТЭК России [Электронный ресурс] // bdu.fstec.ru: Банк данных угроз безопасности информации. URL: http://bdu.fstec.ru/threat/ubi.034 (дата обращения: 9.06.2018)

4. nRF24L01 Datasheet [Электронный ресурс] // sparkfun.com. URL: https://www.sparkfun.com/datasheets/Components/SMD/nRF24L01Pluss_Preliminary_Product_Specification_v1_0.pdf (дата обращения: 10.06.2018)

Салищев Д.Н., Баранов А.Н., Баранова Е.М.
Тульский государственный университет

СРАВНИТЕЛЬНАЯ ОЦЕНКА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Сегодня в России действует достаточное большое количество документов, затрагивающих тему информационной безопасности, а именно тему информационной защиты автоматизированных систем управления технологическими процессами (АСУ ТП).

Большинство таких документов были разработаны в 2007 году, в дальнейшем дорабатывались и модернизировались. Они распространяются под грифом «для служебного пользования» (ДСП), который до сих пор с них не снят.

Таким образом, у специалистов по информационной безопасности (ИБ-специалистов) промышленных предприятий имеется в распоряжении достаточно полная и применимая на практике база нормативных документов.

При разработке большинства автоматизированных систем управления технологическими процессами подразумевалось (или подразумевается), что они не будут изменяться в будущем. Другими словами, системы, сконфигурированные 20 лет назад, до сих пор функционируют «в первозданном виде». Программное обеспечение (ПО), используемое в АСУ ТП, долгое время не обновлялось из-за того, что любое изменение может повлечь за собой сбои в работе системы управления [1].

Принципиальное отличие АСУ ТП от привычных для специалистов по информационной безопасности (ИБ) информационных систем заключается в том, что из триады «конфиденциальность – целостность – доступность» в данном случае наиболее критичной является доступность.

В «классических» системах речь идет об обеспечении конфиденциальности информации, ее защите от перехвата и компрометации.

В индустриальных системах, в первую очередь, важно, чтобы управляющий сигнал был вовремя принят и оказал необходимое воздействие.

Таким образом, создание и работа подсистемы обеспечения безопасности АСУ ТП не должны мешать функционированию системы управления. Для обеспечения безопасности АСУ ТП крайне редко используются криптографические решения, поскольку они, как правило, порождают избыточность вычислений и могут замедлить или вовсе остановить отправку и получение управляющего сигнала.

Стандартным механизмом, предлагаемым производителями решений для защиты АСУ ТП, является периметровая защита – разделение (логическое или физическое) сетей на сегменты, которое позволяет выделить или изолировать индустриальные решения [1].

Большое распространение получили разработанные для АСУ ТП межсетевые экраны. В таблице 1 представлена характеристика основных методов защиты АСУ ТП.

Таблица 1

Характеристика основных методов защиты АСУ ТП

Метод	Вид информации	Применение	Характеристика
Криптографические методы	Шифрование информации (считываемой и вводимой)	Не применимо	Порождают избыточность вычислений и замедляют действие
Периметровая защита	Разделение (логическое или физическое) сетей на сегменты, которое позволяет выделить или изолировать индустриальные решения	Применимо	Позволяют исключать несанкционированную модификацию индустриального решения
Межсетевые экраны	Фильтрация трафика осуществляется на основе набора предварительно сконфигурированных правил, которые называются ruleset. Удобно представлять межсетевой экран как последовательность фильтров, обрабатывающих информационный поток. Межсетевые экраны последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие	Применимо	Позволяют фильтровать информацию и исключать вбросы

Исходя из различных методологий обеспечения информационной безопасности АСУ ТП, сформировался перечень наиболее применимых на практике ИБ-решений.

В таблице 2 представлена сводная информация по эффективности и активности внедрения наиболее практически применимых подсистем информационной безопасности.

Таблица 2.

Информация по эффективности и активности внедрения наиболее практически применимых систем безопасности на предприятиях России

№	Наименование подсистемы информационной безопасности АСУ ТП	Активность применения (отношение количества предприятий, применяемых метод, из 10 проанализированных)	Эффективность, (средняя по оценке 10 российских предприятий),%
1	Подсистема сетевой безопасности	0,9	80
2	Подсистема двухфакторной (многофакторной) аутентификации	0,9	90
3	Подсистема обеспечения целостности данных	0,8	95
4	Подсистема быстрого восстановления конфигураций и данных	0,7	80
5	Подсистема криптографической защиты	0,6	95
6	Подсистема предотвращения утечек конфиденциальной информации	0,5	60
7	Подсистема управления патчами (автоматизация внесения изменений в компьютерные файлы)	0,5	55
8	Подсистема управления мобильными устройствами	0,4	65
9	Подсистема управления неструктурированными данными	0,2	70
10	Подсистема анализа защищенности	0,1	40

Первые три ИБ-подсистемы являются ключевыми в АСУ ТП, поскольку позволяют наиболее эффективно сохранять доступность автоматизированной системы управления.

Диаграмма, показывающая активность применения подсистем защиты информации АСУ ТП российскими предприятиями, показана на рисунке 1.

Рис. 1. – Активность применения подсистем защиты информации АСУ ТП российскими предприятиями

Следует отметить, что процесс внедрения некоторых подсистем защиты АСУ ТП на российских предприятиях (подсистема управления неструктурированными данными, подсистема анализа защищенности) находится в зачаточном состоянии.

Таким образом, российский рынок решений для информационной защиты автоматизированных систем управления технологическими процессами и индустриальных сетей находится в развивающемся состоянии. Каждый конкретный проект подразумевает сугубо индивидуальное решение. Кроме того, обеспечить безопасность АСУ ТП исключительно с помощью серийных технических средств крайне сложно. Добиться максимального эффекта позволяет поиск уязвимостей каждой конкретной применяемой на производственном предприятии системы [2].

Диаграмма, показывающая эффективность функционирования внедренных в деятельность российских предприятий подсистем защиты информации АСУ ТП, показана на рисунке 2.

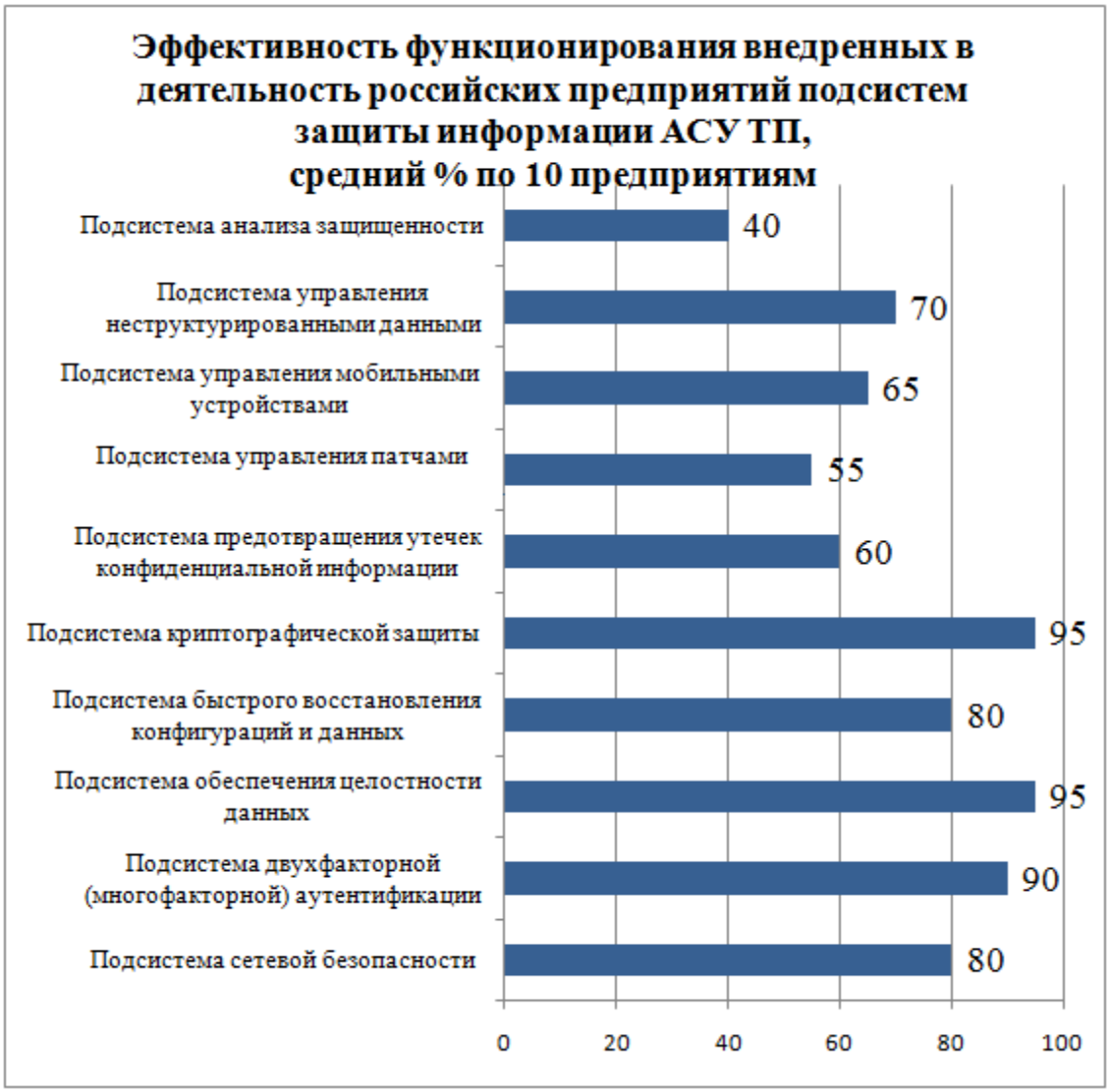


Рис. 2. Эффективность функционирования внедренных в деятельность российских предприятий подсистем защиты информации АСУ ТП

Кроме того, специфика АСУ ТП (приоритет доступности) не позволяет использовать ИБ-решения с большой интеллектуальной составляющей [3].

Одним из распространенных подходов к построению ИБ-системы АСУ ТП является эшелонированная защита, которая включает в себя уровни, показанные в таблице 3.

Таблица 3.

Уровни эшелонированной защиты АСУ ТП

Уровень эшелонированной защиты АСУ ТП	Характеристика уровня эшелонированной защиты АСУ ТП	Степень заинтересованности российских предприятий	Степень реализации на российских предприятия (на 9 из 10 российских предприятиях)
1	2	3	4
Физическая безопасность	Ограничение физического доступа к панелям управления, диспетчерским и другим помещениям, устройствам, кабелям	Высокая	1

1	2	3	4
Сетевая безопасность	Сетевая инфраструктура (межсетевые экраны со встроенными сенсорами систем предотвращения вторжения) и средства защиты, интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы)	Высокая	0,8
Безопасность рабочих станций и серверов	Управление обновлениями ПО, применение антивирусного ПО, удаление неиспользуемых приложений, протоколов и сервисов	Высокая	0,8
Безопасности приложений	Аутентификация, авторизация и аудит при доступе к приложениям	Высокая	0,9
Безопасность устройств	Контроль над изменениями и ограничение доступа	Наивысшая	0,7

Диаграмма, отражающая степень реализации на российских предприятия уровней эшелонированной защиты АСУ ТП, показана на рисунке 3.

Рис. 3. Степень реализации на российских предприятия уровней эшелонированной защиты АСУ ТП

Многие компоненты АСУ ТП подключены к сетевой инфраструктуре IP/Ethernet, но для них не всегда возможна установка средств обеспечения ИБ, таких как антивирусы или системы предотвращения вторжений на уровне хоста.

Литература:

1. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

2. Кочкин К.Ю., Баранова Е.М. Разработка программы для эффективного кодирования текстовой информации и комбинаций в комбинаторных задачах//Мехатроника, автоматика и робототехника. 2018. № 2. С. 224-229.

3. NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security» и NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations».

Семенистый В.В., Гамолина И.Э., Дурягина В.В.
Южный Федеральный Университет

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРЯМЫХ ПАРАЛЛЕЛЬНЫХ МЕТОДОВ ДЛЯ ЗАДАЧИ ТЕЧЕНИЯ СОВЕРШЕННОГО ГАЗА ПО КАНАЛУ ПЕРЕМЕННОГО СЕЧЕНИЯ

Основные затраты времени вычислительной системы приходятся на алгебраический расчет дробных шагов алгоритма, где обращаются ленточные матрицы большой размерности. Такие системы характерны для многих неявных итерационных методов решения задач аэрогидродинамики. Для современных многоядерных (многопроцессорых) вычислительных сред создается новое программное обеспечение. Создание и исследование параллельных алгоритмов является частью этой задачи. При построении параллельных вычислений для одномерных задач механики основной акцент приходится на исследование параллельных методов решения алгебраических уравнений.

Для решения ленточных систем используются различные прямые параллельные методы, одним из которых является метод параллельной прогонки. Исходная матрица системы расщепляется на подсистемы той же структуры, число которых зависит от количества вычислительных устройств многопроцессорного комплекса. Разбиение матричного оператора непосредственно связано с декомпозицией расчетной области задачи. Построение параллельного алгоритма зависит и от структуры вычислительной системы.

Рассмотрим течение совершенного газа по каналу переменного сечения (рисунок 1).

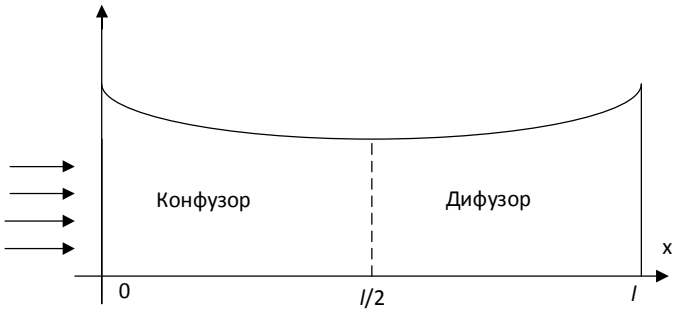


Рис. 1. Расчетная область задачи

Задавая уравнения стенок канала и осредняя (по Рейнольдсу) газодинамические параметры в поперечных сечениях канала, запишем одномерную систему уравнений газовой динамики, описывающую течение [4]

$$\begin{cases} \frac{d}{dt} r\rho + \frac{d}{dx} r\rho u = 0 \\ \frac{d}{dt} r\rho u + \frac{d}{dx} r\rho u^2 + r\frac{dp}{dx} = 0, \\ \frac{d}{dt} r\rho E + \frac{d}{dx} r\rho u(E+p) = 0, \\ p = \rho\varepsilon(\gamma - 1). \end{cases} \quad (1)$$

Здесь $(\rho, u, p)^T$ – вектор искомых газодинамических функций и $\gamma = C_p/C_v \approx 1.4$ – показатель адиабаты для совершенного газа.

Верхняя стенка канала задается следующим уравнением с двумя параметрами, позволяющими менять протяженность и высоту канала в критическом сечении: $r(x) = \frac{a}{l}(x - \frac{l}{2})^2 + \frac{al}{4}$, где α, l – положительные числа и $x \in [0,l]$.

Физическая модель описывает течения в аэродинамических трубах, реактивных двигателях.

Система (1) после преобразования может быть представлена в следующей недивергетной операторной форме [4]:

$$\frac{df}{dt} + \Omega f + G = 0, \tag{2}$$

где

$$\Omega f = \begin{bmatrix} \frac{d}{dx}u & 0 & 0 \\ 0 & u\frac{d}{dx} & \frac{r}{\rho^*}\frac{d}{dx} \\ 0 & \gamma p\frac{d}{dx} & u\frac{d}{dx} \end{bmatrix} \begin{bmatrix} \rho^* \\ u \\ p \end{bmatrix} \tag{3}$$

и свободный вектор $G = (0,0,\gamma\frac{r'}{r}pu)^\tau$.

Для численного расчета системы (3) используется метод расщепления оператора Ω по физическим процессам.

Схемы расщепления в различных газодинамических переменных имеют различный вид, поэтому параллельные алгоритмы их реализации тоже разные [9]. Для системы (1) выбор искомого вектора в переменных $f = (\rho^*, u, p)^\tau$ позволяет отдельно решать уравнение неразрывности от остальных уравнений системы.

Построим в расчетной области Q=[0,l]x[0,T] равномерную сетку $Q_{\tau,h}: \{(x_i = ih, t_n = n\tau),\ i = 0,1,\dots,N; n = 0,1,\dots,M\}$. Для аппроксимации второго и третьего уравнения системы (1) воспользуемся разностной схемой с весом α (в дальнейшем считаем $\alpha = 1$ - случай неявной схемы):

$$\frac{g^{n+1} - g^n}{\tau} + \sum_{j=1}^{2} \Omega_{jh}^k \left(\alpha g^{n+1} - (1-\alpha)g^n\right) = -G_h^n, \tag{4}$$

где $g = (u,p)^\tau$ – искомый вектор;

$\Omega_h^k = \sum_{j=1}^{2} \Omega_{jh}^k = \begin{bmatrix} u^n\Lambda_-^k & 0 \\ 0 & u^n\Lambda_-^k \end{bmatrix} + \begin{bmatrix} 0 & (r/\rho^*)^n\Lambda_+^k \\ \gamma p^n\Lambda_-^k & 0 \end{bmatrix}$ – разностный оператор, представленный в виде суммы разностных операторов, аппроксимирующих различные физические процессы.

При численной реализации схемы (4) применяем метод дробных шагов [4]:

$$\begin{cases} (\mathrm{I} + \tau\alpha\Omega_{1h}^k)\xi^{n+1/2} = -\Omega_h^k g^n - G_h^n \\ (\mathrm{I} + \tau\alpha\Omega_{2h}^k)\xi^{n+1} = \xi^{n+1/2} \\ g^{n+1} = g^n + \tau\xi^{n+1}. \end{cases} \tag{5}$$

Для получения стационарного (установившегося) течения проводим итерации до выполнения условия установления:

$$\delta = \left|\frac{1}{\rho}\frac{d\rho}{dt}\right| < \varepsilon. \tag{6}$$

Численный алгоритм расчета системы (1) состоит из десяти этапов. Остановимся подробнее на каждом из них.

Этап 1. Вычисление (задание) граничных и начальных условий для моделируемого течения газа.

Этапы 2 и 3. Вычисление значений переменных u (этап 2), p (этап 3) на новом временном шаге по схеме (5). На первом дробном шаге при нахождении значений газодинамических функций каждое из двух уравнений системы решается независимо друг от друга методом скалярной прогонки.

Этап 4. Сохранение результатов расчета первого дробного шага.

Этапы 5 и 6. На втором дробном шаге методом скалярной прогонки находим сначала значение *p* (этап 5) на новом дробном шаге, и, по найденному давлению, пересчитываем значения *u* (этап 6). Краевые условия на дробных шагах выбираем равными нулю.

Этап 7. Сохранение результатов расчета второго дробного шага.

Этап 8. Вычисление значений переменных u^{n+1}, p^{n+1} на новом целом шаге.

Этап 9. Вычисляются значения переменной ρ на новом целом временном шаге, учитывая найденные значения u^{n+1}, p^{n+1}. Решается первое уравнение системы (2).

Этап 10. Проверка условия установления (6). Если условие выполнено, прекращаем расчет, если нет – переходим к этапу 2.

Параллельный алгоритм реализуется на определенной модели параллельной вычислительной системы [1]. Для проведения расчетов физической задачи будем использовать многопроцессорную систему (МВС) с распределенной памятью и перестраиваемыми коммутационными связями, состоящую из p однородных решающих устройств с локальной памятью, управляемых центральным устройством управления (рисунок 2).

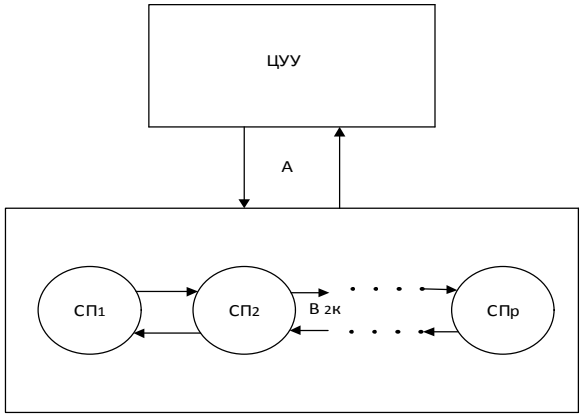


Рис. 2. Конфигурация МВС

При вычислении одномерной задачи коммутируется линейная топология связи. Исследование параллельного алгоритма проведем на этапах 2–7.

Для обращения ленточных матриц в работе используется метод параллельной прогонки (П-прогонки) [2,3]. Рассмотрим более подробно решение второго уравнения системы (5)

$$\begin{cases} \xi_{1,i}^{n+1} + \tau \dfrac{r_i}{\rho_i^{*n}} \Lambda_+^1 \xi_{2,i}^{n+1} = \xi_{1,i}^{n+1/2}, \\ \xi_{2,i}^{n+1} + \tau\gamma p_i^n \Lambda_-^1 \xi_{1,i}^{n+1} = \xi_{2,i}^{n+1/2}, \\ i = 1,2,\dots,N-1. \end{cases}$$

Здесь $\xi = (\xi_1, \xi_2)$ - вектор значений искомых переменных *u*, *p* на дробных шагах алгоритма.

Из первого уравнения выразим переменную $\xi_{1,i}^{n+1}$ и подставим во второе, получаем:

$$\begin{cases} \xi_{1,i}^{n+1} = \xi_{1,i}^{n+1/2} - \tau \dfrac{r_i}{\rho_i^{*n}} \Lambda_+^1 \xi_{2,i}^{n+1}, \\ \xi_{2,i}^{n+1} - \tau\gamma p_i^n \Lambda_-^1 \left(\tau \dfrac{r_i}{\rho_i^{*n}} \Lambda_+^1 \xi_{2,i}^{n+1} \right) = \xi_{2,i}^{n+1/2} - \tau\gamma p_i^n \Lambda_-^1 \xi_{1,i}^{n+1/2}. \end{cases}$$

Расписывая разностные операторы Λ_-^1 и Λ_+^1, второе уравнение системы сводится к следующему трехточечному разностному уравнению:

$$-a_i \xi_{2,i-1}^{n+1} + c_i \xi_{2,i}^{n+1} - b_i \xi_{2,i+1}^{n+1} = q_i, \qquad (7)$$

где коэффициенты

$$a_i = \frac{\tau^2}{h^2}\gamma p_i^n \left[\frac{r}{\rho^{*n}}\right]_{i-1},\ b_i = \frac{\tau^2}{h^2}\gamma p_i^n \left[\frac{r}{\rho^{*n}}\right]_i,\ c_i = \frac{\tau^2}{h^2}\gamma p_i^n \left|\left[\frac{r}{\rho^{*n}}\right]_i + \left[\frac{r}{\rho^{*n}}\right]_{i-1}\right| + 1,$$

$$q_i = \xi_{2,i}^{n+1/2} - \frac{\tau}{h}\gamma p_i^n\left[\xi_{1,i}^{n+1/2} - \xi_{1,i-1}^{n+1/2}\right].$$

Заметим, что для системы (7) имеет место условие $|c_i| > |a_i| + |b_i|$ (строгое диагональное преобладание), гарантирующее корректность метода прогонки.

Для решения на МВС уравнение (7), с учетом краевых условий, запишем в виде:

$$\begin{cases} c_1\xi_{2,1}^{n+1} - b_1\xi_{2,2}^{n+1} = q_1, \\ -a_i\xi_{2,i-1}^{n+1} + c_i\xi_{2,i}^{n+1} - b_i\xi_{2,i+1}^{n+1} = q_i, \\ i = 2,3,\dots,N-1, \\ -a_N\xi_{2,N-1}^{n+1} + c_N\xi_{2,N}^{n+1} = q_N. \end{cases} \quad (8)$$

Для решения системы (8) воспользуемся алгоритмом П-прогонки [2]:

а) выбираем на разностной сетке номера узловых точек I_j. Номера $I_j \in [0, N]$ можно выбирать произвольно в указанном интервале, но для более равномерной загрузки спецпроцессоров вычисляем их по формуле: $I_j = [jN/p]$, $j \in [0, p]$. Здесь $I_0 = 0$, $I_p = N$ - номера граничных узлов сетки и p - число процессоров системы;

б) решение системы (8) распадается на решение $j \in [0, p-1]$ независимых подсистем следующего вида:

$$\begin{cases} c_{I_j+1}\xi_{2,I_j+1}^{n+1} - b_{I_j+1}\xi_{2,I_j+2}^{n+1} = q_{I_j+1} + a_{I_j+1}\xi_{2,I_j}^{n+1}, \\ -a_I\xi_{2,I-1}^{n+1} + c_I\xi_{2,I}^{n+1} - b_I\xi_{2,I+1}^{n+1} = q_I, \quad I = I_j+2,\dots,I_{j+1}-2, \\ -a_{I_{j+1}-1}\xi_{2,I_{j+1}-2}^{n+1} + c_{I_{j+1}-1}\xi_{2,I_{j+1}-1}^{n+1} = q_{I_{j+1}-1} + b_{I_{j+1}-1}\xi_{2,I_{j+1}}^{n+1} \end{cases} \quad (9)$$

или в матричной форме

$$A_j\overline{\xi_j} = \overline{d_j},\ j \in [0, p-1]. \quad (10)$$

Здесь $\overline{\xi_j} = (\xi_{2,I_j+1}^{n+1}, \xi_{2,I_j+2}^{n+1}, \dots, \xi_{2,I_{j+1}-1}^{n+1})^\tau$. Так как система (10) линейная, то ее решение представимо виде суперпозиции

$$\overline{\xi_j} = \xi_{2,I_j}^{n+1}\overline{x_j} + \xi_{2,I_{j+1}}^{n+1}\overline{y_j} + \overline{z_j},\ j \in [0, p-1]. \quad (11)$$

Считаем, что $\xi_{2,I_0}^{n+1} = \xi_{2,I_p}^{n+1} = 0$. Векторы $\overline{x_j}, \overline{y_j}, \overline{z_j}$ – решение системы (10) с правыми частями соответственно:

$$d_{j_1} = (a_{I+1}, 0, \dots, 0),\ d_{j_2} = \left(0,0,\dots,b_{I_{j+1}-1}\right) \text{ и } d_{j_3} = \left(q_{I_j+1}, q_{I_j+2}, \dots, q_{I_{j+1}-1}\right);$$

в) для вычисления по формуле (11) окончательного решения системы (9) необходимо знать значения переменных ξ_{2,I_j}^{n+1} в узловых точках. Эти значения находим при решении следующей редуцированной трехдиагональной системы (12), коэффициенты которой являются функциями от коэффициентов системы (8) и компонентов векторов $\overline{x_j}, \overline{y_j}, \overline{z_j}$:

$$\begin{cases} c_1^1\xi_{2,I_1}^{n+1} - b_1^1\xi_{2,I_2}^{n+1} = q_1^1 \\ -a_j^1\xi_{2,I_{j-1}}^{n+1} + c_j^1\xi_{2,I_j}^{n+1} - b_j^1\xi_{2,I_{j+1}}^{n+1} = q_j^1, j = 2,3,\dots,p-1, \\ -a_{p-1}^1\xi_{2,I_{p-2}}^{n+1} + c_{p-1}^1\xi_{2,I_{p-1}}^{n+1} = q_{p-1}^1, \end{cases} \quad (12)$$

где

$$\begin{aligned} &c_1^1 = c_{I_1} - a_{I_1}y_{I_1-1},\ b_1^1 = b_{I_1}y_{I_1+1}, q_1^1 = q_{I_1} + a_{I_1}z_{I_1-1} + b_{I_1}z_{I_1+1}, a_1^1 = 0, \\ &a_j^1 = a_{I_j}z_{I_j-1},\ c_j^1 = c_{I_j} - a_{I_j}y_{I_j+1} - b_{I_j}x_{I_j+1}, \\ &b_j^1 = b_{I_j}y_{I_j+1},\ q_j^1 = q_{I_j} + a_{I_j}z_{I_j-1} + b_{I_j}z_{I_j+1}, j = 2,3,\dots,p-2; \\ &a_{p-1}^1 = a_{I_{p-1}}x_{I_{p-1}-1},\ c_{p-1}^1 = c_{I_{p-1}} - b_{I_{p-1}}x_{I_{p-1}+1}, b_{p-1}^1 = 0, \\ &q_{p-1}^1 = q_{I_{p-1}} + a_{I_{p-1}}z_{I_{p-1}-1} + b_{I_{p-1}}z_{I_{p-1}+1}. \end{aligned} \quad (13)$$

Решение системы (12 – 13) можно находить обычной скалярной прогонкой.

Таким образом, для вычисления системы (8) методом П-прогонки на p-процессорной МВС необходимо на каждом процессоре:

а) решить три системы вида (10) с общей матрицей A_j и правыми частями $d_{j_1}, d_{j_2}, d_{j_3}$;

б) по формулам (13) вычислить коэффициенты и правую часть для системы (12) и решить её;

в) решить уравнение (11).

На этапах решения а) и в) удается полностью распараллелить вычисления, выделив p независимых участков расчета задачи. На этапе б) при решении редуцированной системы уравнений каждый процессор последовательно вычисляет значение искомой переменной, обмениваясь информацией только с соседними процессорами.

Исследуем эффективность параллельных вычислений при решении системы (8) методом П-прогонки на МВС (рисунок 2).

Остановимся на параллельном решении всей задачи течения газа [6,7,8] по каналу переменного сечения (для одного итерационного шага и при постоянном знаке скорости в расчетной области). Выше определены основные этапы расчета.

На первом этапе в памяти $СП_j$ $(1 \le j \le p)$ размещаем векторы начальных и граничных значений газодинамических функций ρ, u, p; массивы точек $r_i = r(x_i)$, $r_i' = r'(x_i)$, $i = 0,1, \dots, N$, постоянные τ, h, γ. Используем часть памяти для хранения массивов значений промежуточных вычислений.

На втором и третьем этапах решаем систему (5) на первом дробном шаге. Учитывая диагональный вид оператора Ω_{1h}^k (первое уравнение схемы (5)), на первом дробном шаге решаем независимо друг от друга две системы линейных уравнений:

$$\begin{cases} \xi_{s,0}^{n+1/2} = 0, \\ -a_i \xi_{s,i-1}^{n+1/2} + c_i \xi_{s,i-1}^{n+1/2} = -q_i^s, \ \ i = 1,2, \dots, N-1; s = 1,2, \end{cases} \tag{14}$$

отличающихся векторами правых частей.

Здесь

$$a_i = \frac{\tau}{h} u_i^n,\ c_i = 1 + \frac{\tau}{h} u_i^n,\ q_i^1 = u_i^n \frac{u_i^n - u_{i-1}^n}{h} + \frac{1}{\rho_i^n} \frac{p_i^n - p_{i-1}^n}{h},$$

$$q_i^2 = \gamma p_i^n \frac{u_i^n - u_{i-1}^n}{h} + u_i^n \frac{p_i^n - p_{i-1}^n}{h} + \left(\gamma \frac{r'}{r} pu\right)_i^n.$$

Решение системы (14) может быть найдено по схеме бегущего счета на одном процессоре, но для организации параллельных вычислений на МВС используем метод П-прогонки, учитывая, что коэффициенты b_i равны нулю.

После декомпозиции расчетной области каждый процессор:

1) для вычисления коэффициентов и правых частей системы (14) затрачивает $T_1 = 20t_a + 4t_0$ временных тактов.

2) Решает независимо от других вспомогательные системы

$$\begin{cases} x_{s,I_j+1} = \dfrac{a_{I_j+1}}{c_{I_j+1}} \\ x_{s,I} = \dfrac{a_1}{c_1} x_{s,I-1}, \ \ I = I_j + 2, \dots, I_{j+1} - 1; \end{cases} \tag{15}$$

$$\begin{cases} z_{s,I_j+1} = \dfrac{q_{I_j+1}^s}{c_{I_j+1}} \\ z_{s,I} = \dfrac{q_I^s}{c_I} + \dfrac{a_I}{c_I} z_{s,I-1}, \ \ I = I_j + 2, \dots, I_{j+1} - 1 \\ j = 0,1, \dots, p-1. \end{cases} \tag{16}$$

Система (15) одинакова для s=1,2, поэтому общее время вычисления равно $T_2 = 10(m-2)t_a$ тактам.

3) Вычисляет коэффициенты редуцированной системы в I_j узле (для s=1,2):

$c_j^1 = c_{I_j}, = q_j^s + a_{I_j} z_{s,I_j-1}, j = 1, \dots, p-1,$

$a_j^1 = a_{I_j} x_{s,I_j-1},\ j = 2, \dots, p-1$

за время $T_3 = 5t_a$.

4) Временные затраты при решении на МВС редуцированной системы

$$\begin{cases} \xi_{s,I_1}^{n+1/2} = \frac{q_1^{s,1}}{c_1^1} \\ \xi_{s,I_j}^{n+1/2} = \frac{q_j^{s,1}}{c_1^1} + \frac{a_j^1}{c_j^1}\xi_{s,I_{j-1}}^{n+1/2}, j = 2,3, \dots, p-1 \end{cases} \quad (17)$$

составят $T_4 = 2[(4p-11)t_a + (p-2)t_0] = (8p-22)t_a + 2(p-2)t_0$ тактов (для s=1,2).

5) Окончательно каждый $СП_j$ $(1 \le j \le p)$ находит вектор искомых газодинамических переменных первого дробного шага по формуле: $\bar{\xi}_{s,j}^{n+1/2} = \xi_{s,I_j}^{n+1/2}\bar{x}_j + \bar{z}_{s,j}$ за время $T_5 = 4(m-2)t_a$ временных тактов. Здесь векторы $\bar{x}_j, \bar{z}_{s,j}$ - решение систем (15) и (16).

Суммарное время решения первого дробного шага составит

$T^1 = (34m + 8p - 43)t_a + 2pt_0$ временных тактов.

На пятом и шестом этапах решаем систему (5) на втором дробном шаге. С учетом времени $(T = (12m+4)t_a + 3t_0)$ нахождения коэффициентов и правой части системы (7) полное время вычисления этапа составит $T^/ + T = (32m + 8p - 28)t_a + (3p+1)t_0$ временных тактов.

На шестом этапе по найденному значению давления на втором дробном шаге пересчитывается значение скорости. Решается уравнение $\xi_{1,i}^{n+1} = \xi_{1,i}^{n+1/2} - \tau\frac{r_i}{\rho_i^{*n}}\Lambda_+^1\xi_{2,i}^{n+1}$. При этом каждый процессор затрачивает $T = (5m-4)t_a + t_0$ временных тактов. Суммарное время решения второго дробного шага оценивается в $T^2 = (37m + 8p - 32)t_a + (3p+2)t_0$ временных тактов.

На восьмом этапе за время $T^3 = 4mt_a$ тактов вычисляем значения u, p на новом итерационном шаге. Здесь все $СП_j$ работают независимо.

На девятом этапе рассчитывается плотность на верхнем временном слое. Решаем первое уравнение системы (2), которое в разностном виде может быть записано

$$\frac{\rho_i^{*n+1} - \rho_i^{*n}}{\tau} + \frac{u_i^{n+1}\rho_i^{*n+1} - u_{i-1}^{n+1}\rho_{i-1}^{*n+1}}{h} = 0$$

или в каноническом виде

$$-a_i\rho_{i-1}^{*n+1} + c_i\rho_i^{*n+1} = q_i. \quad (18)$$

Здесь $a_i = \frac{\tau}{h}u_{i-1}^{n+1}, c_i = 1 + \frac{\tau}{h}u_i^{n+1}, q_i = \rho_i^{*n}$.

Уравнение (18) решается аналогично одному из уравнений системы (14), поэтому время, затрачиваемое на его решение с учетом времени $T = 3mt_a + t_0$ вычисления коэффициентов и пересчета значения плотности по формуле: $\rho_i^{n+1} = \rho_i^{*n+1}/r_i$ составит: $T^4 = (11m + 4p - 28)t_a + (p-1)t_0$. На этом завершаются вычисления одного итерационного шага.

Полное время работы МВС на всех этапах алгоритма расчета течения газа составит

$T = T^1 + T^2 + T^3 + T^4 = (86m + 20p - 103)t_a + (6p+1)t_0$ временных тактов.

Для однопроцессорной вычислительной системы оно составляет $T \approx (69N+1)t_a$ временных тактов.

Коэффициент ускорения решения газодинамической задачи на МВС выбранной архитектуры оценивается формулой:

$$\overline{K}_y \approx \frac{69N}{86m+(20+6a)p} \quad (19)$$

Из оценок следует, что параллельный расчет всей задачи происходит в два с половиной раза быстрей, чем расчет методом П-прогонки уравнения (8).

Таким образом, построен параллельный алгоритм для решения одномерной задачи течения совершенного газа по каналу переменного сечения. Проведен анализ свойств данного алгоритма для неявной итерационной схемы, основанной на использовании прямых параллельных методов решения алгебраических уравнений.

Литература:

1. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. – СПб.: БХВ-Петербург, 2004. С.134-154.

2. Яненко Н.Н., Коновалов А.Н., Бугров А.Н. Об организации параллельных вычислений и «распараллеливании» прогонки// Численные методы механики сплошной среды. - Новосибирск: 1978.- т.9., №7. - С.139-146.

3. Гамолина И.Э., Семенистый В.В. Параллельная организация вычислений при расчете задач аэрогидродинамики прямыми методами. Международное Научное Сотрудничество, Образование и Культура. Ростов-на-Дону: Изд-во Summa-Rerum, 2014, № 3(4). С. 23-28.

4. Ковеня В.М. Алгоритмы расщепления при решении многомерных задач аэрогидродинамики. - Новосибирск. Изд-во СО РАН.2014.-280 с.

5. Гамолина И.Э., Дурягина В.В., Семенистый В.В. Дозвуковое обтекание профилей // Известия ЮФУ. Технические науки. 2013. № 4. С. 61-67.

6. А.В. Базовкин, В.М. Ковеня. Распараллеливание алгоритма расщепления на многопроцессорных системах при моделировании течений вязкой несжимаемой жидкости / Вестн. НГУ. Сер. матем., мех., информ., 13:4 (2013), С.3–15.

7. Е.Н. Акимова, В.Е. Мисилов, А.Ф. Скурыдина, А. И. Третьяков. Градиентные методы решения структурных обратных задач гравиметрии и магнитометрии на суперкомпьютере “Уран”, Выч. мет. программирование, 2015. том 16, выпуск 1, С.155–164.

8. Сухинов А.И., Лапин Д.В., Чистяков А.Е. Моделирование прямых и обратных задач диффузии-конвекции на многопроцессорных системах для прогноза и ретроспективности анализа водных экостстем // Труды конференции «Параллельные вычислительные системы (ПАВТ)». Челябинск. 2013. С.248- 257.

9. Семенистый В.В., Гамолина И.Э., Дурягина В.В, Богданов Д.С. Моделирование и анализ параллельного алгоритма решения задачи обтекания плоской пластины методом глобальных итераций // Сборник материалов XIII международной научно-практической конференции (13 июня 2017 г.) «Вопросы современной науки: проблемы, тенденции, перспективы». М.: Научный журнал «Chronos», 2017. часть 1 - С. 79-85.

Сидельников О.В.
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

ВЫЯВЛЕНИЕ ЦЕЛЕВОГО ПРИЗНАКА КЛАССА ОПАСНЫХ СОСТОЯНИЙ АРМ АС ВН НА ОСНОВЕ ПОИСКА ИМПЛИКАТИВНЫХ ЗАКОНОМЕРНОСТЕЙ В ФОРМЕ КОНЪЮНКЦИЙ ОГРАНИЧЕННОГО РАНГА

Эффективность функционирования автоматизированной системы военного назначения (АС ВН) определяется техническим состоянием (ТС) составляющих ее объектов [1]. На каждом из этапов проектирования и производства, хранения, эксплуатации и регла-

мента АС ВН – к ней предъявляются технические требования. Соответствие системы заданным требованиям определяет ее ТС. Важной подсистемой АС ВН является подсистема мониторинга. Подсистема мониторинга АС ВН обеспечивает получение необходимой информации о ТС объектов мониторинга [2]. От качества функционирования подсистемы мониторинга зависит достоверность информации о ТС объектов АС ВН, которая используется для принятия решений при управлении контролируемыми объектами АС ВН [6]. Термин «мониторинг объекта», в основном, аналогичен термину технического диагностирования объекта [3]. Мониторинг ТС объектов АС ВН направлен на поддержание установленного уровня надежности, обеспечение требований безопасности и эффективности использования объекта. Следовательно, необходим текущий контроль состояния надежности и безопасности, так как на исправном оборудовании АС ВН может возникнуть опасная ситуация.

В статье [4] рассмотрена адаптация метода логического вывода закономерностей состояний информационно-телекоммуникационных систем (ИТКС) для обнаружения компьютерных атак. Автор предлагает основывать классификацию (распознавание) образов в булевом пространстве признаков на предварительном построении «области запрета», описываемой посредством дизъюнктивной нормальной формы (ДНФ) с конъюнкциями ограниченного ранга. Данные конъюнкции задают запретные интервалы в булевом пространстве и интерпретируются как импликативные закономерности. Простота этой закономерности оценивается числом переменных, входящих в нее, т.е. рангом конъюнкции, а мощность – объемом области запрета. Распознавание основано на решении задачи реконструкции множества «реальных» объектов, подчиняющегося определенным импликативным закономерностям по его случайной выборке. Распознавание сводится к логическому выводу, т.е. к выбору значений целевого признака, не вступающих в противоречие с системой, обнаруживаемых на этапе обучения закономерностей.

Целью статьи является описание способа выявления целевого признака класса опасных состояний автоматизированных рабочих мест (АРМ) АС ВН на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга.

1. Опасное состояние АРМ АС ВН

Опасное состояние АРМ АС ВН – это синоним чрезвычайного состояния, при котором возник ущерб «большого» масштаба [5]. Низкая своевременность обнаружения опасных состояний АС ВН, выхода контролируемых параметров за пределы допустимых значений, выхода из строя одного элемента или нескольких элементов системы может повлечь отказ всей системы. Отказ всей системы может развиться за достаточно короткий промежуток времени, что может вызвать развитие опасной ситуации. Так как АС ВН относятся к структурно-сложным системам, входящих в состав критической информационной инфраструктуры (КИИ) Вооруженных Сил (ВС) Российской Федерации (РФ), предназначенных для задач управления войсками и оружием, нарушение (или прекращение) функционирования которых может нанести ущерб обороноспособности РФ, привести к снижению боеготовности ВС, срыву выполнения поставленных стратегических задач, а так же стать причиной аварий и катастроф вооружения и военной техники [6].

Проблемы анализа состояния надежности и безопасности, своевременность выявления перехода в опасное состояние АСУ рассмотрены в трудах Дружинина Г.В., Ушакова И.А., Можаева С.А., Рябинина И.А., Острейковского В.А., Швыряева Ю.В., Шарай В.А. и др. [7-9]. В данных работах рассматриваются фундаментальные основы логико-вероятностного анализа безопасности и надежности объектов мониторинга АСУ, аналитические и графические формы представления опасного состояния (ОС) системы.

Описание возможного сценария опасных состояний (СОС) системы в процессе ее

функционирования представляет наибольшую трудность при исследовании безопасности. Описание СОС не имеет алгоритма и является творческим процессом [10]. На рисунке 1.1 представлено замедление выполнения технологического цикла управления (ТЦУ) АС ВН и переход ее в опасное состояние (чрезвычайная ситуация).

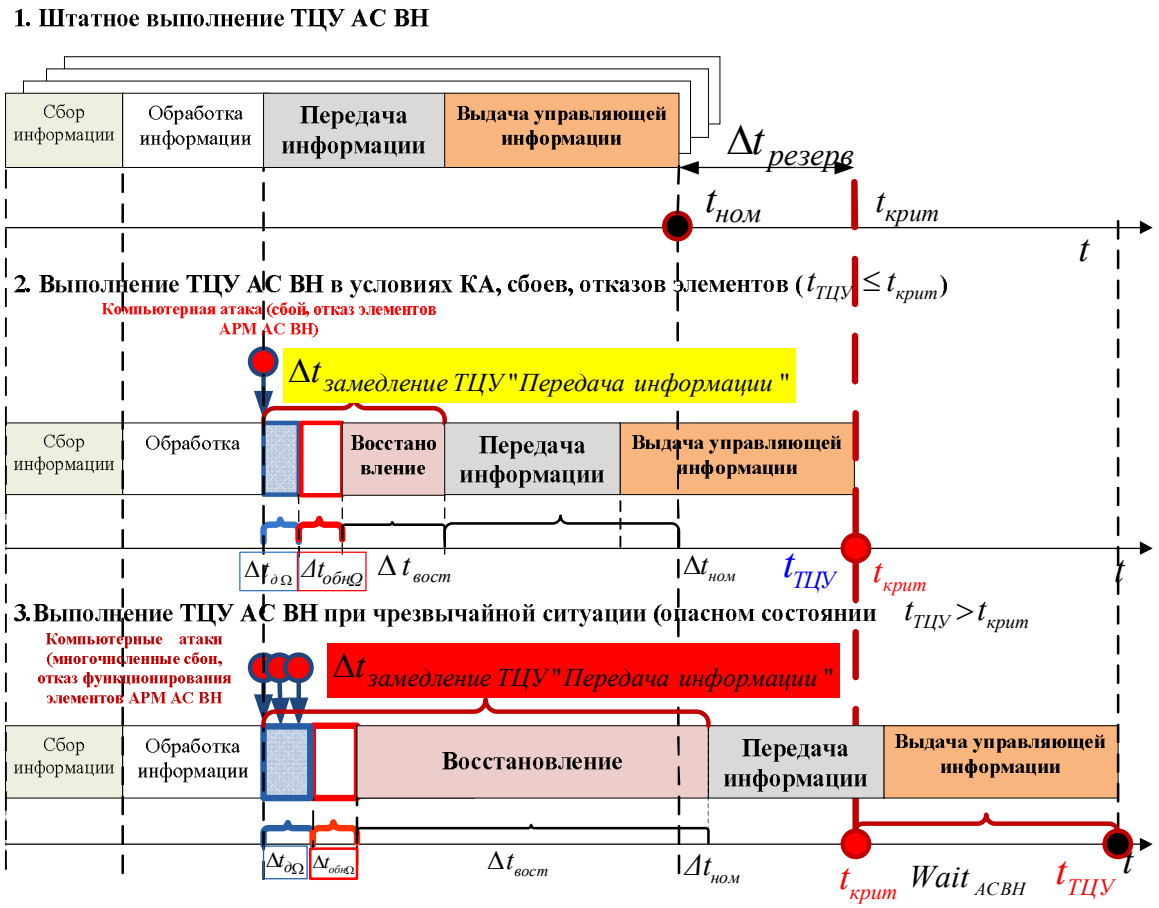


Рисунок 1.1 – Замедление выполнения ТЦУ АС ВН и переход ее в опасное состояние (чрезвычайная ситуация)

В логико-вероятностной теории безопасности СОС осуществляется с помощью логической функции опасности системы (ФОС), аргументами которой выступают инициирующие события и условия, в качестве которых могут быть короткие замыкания в электросети, разряды молнии, искрение электрооборудования, сварочные работы, диверсионные акты, отказы, нарушения правил эксплуатации, ошибки операторов, деструктивные воздействия, в том числе, заключительная фаза КА, различные повреждающие воздействия и иные причины, приводящие к чрезвычайной ситуации [5,10].

В качестве прототипа для определения опасных состояний АРМ АС ВН рассмотрим модуль анализа состояния АРМ системы обнаружения атак (СОА).

Модуль анализа состояния АРМ АС ВН обеспечивает обнаружение факта атаки на основе локальных данных АРМ: динамических характеристик, системных журналов и попыток несанкционированного доступа (НСД). В качестве событий безопасности используются события:

событие, формируемое при фиксации попытки несанкционированного доступа к файлам, каталогам, устройствам;

событие, формируемое при фиксации попытки несанкционированного использования утилиты «sudo»;

событие, формируемое при фиксации попытки несанкционированного входа в систему;

событие, формируемое при фиксации попытки подмены MAC-адресов;
события, формируемые при превышении использования системных ресурсов.

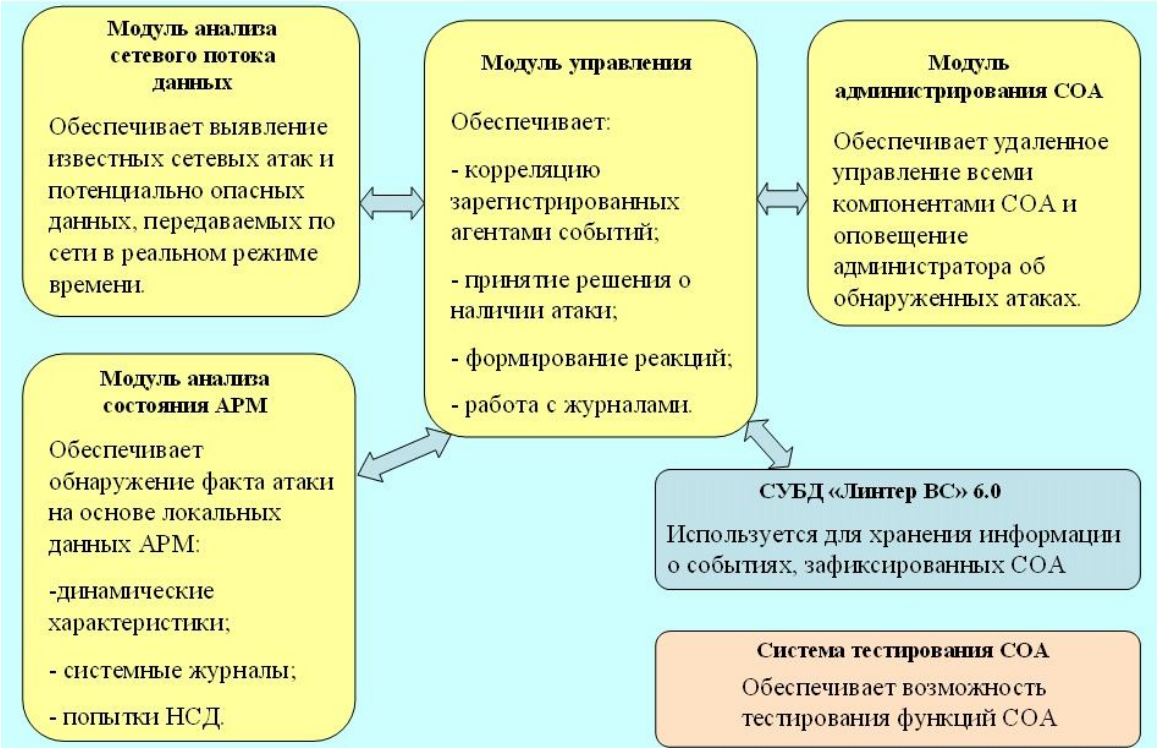


Рисунок 1.2 – Схема СОА

На рисунке 1.3 представлена схема мониторинга опасных состояний АРМ АС ВН.

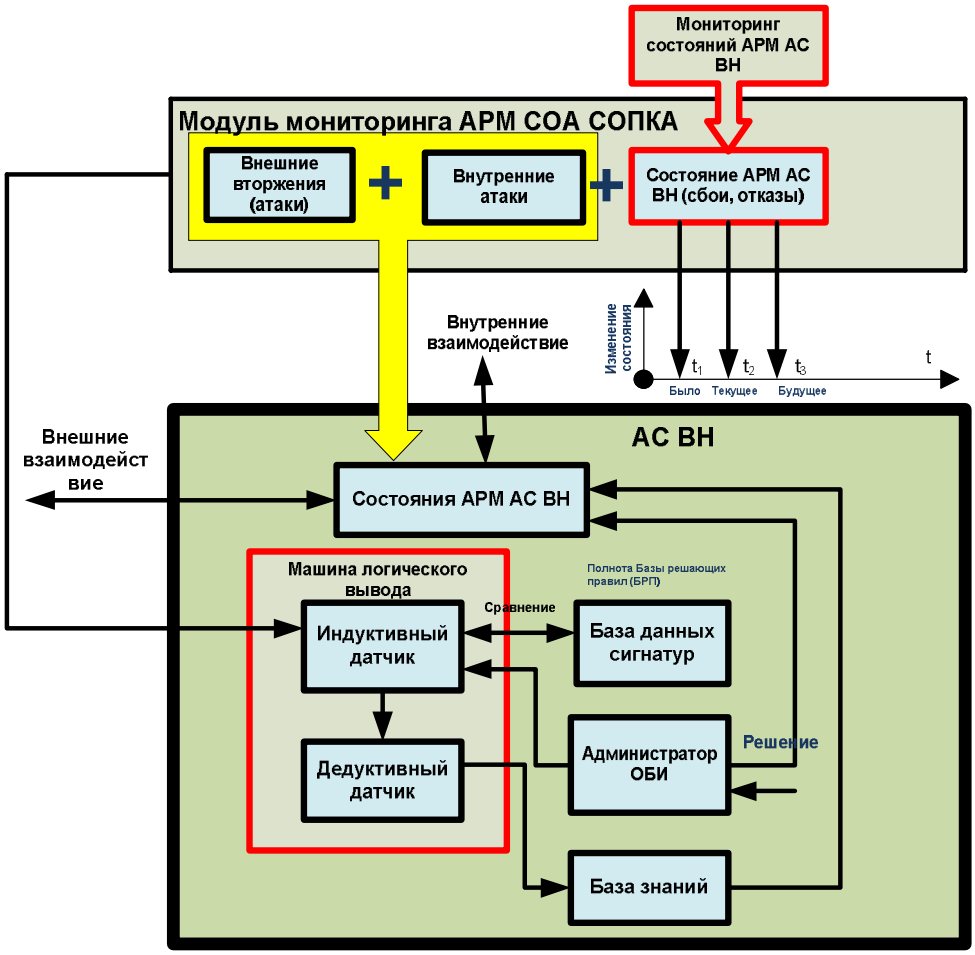


Рисунок 1.3 – Схема мониторинга опасных состояний АРМ АС ВН

2. Мониторинг опасных состояний АРМ АС ВН на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга

Рассмотрим алгоритм мониторинга опасных состояний АРМ АС ВН на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга (рис. 2.1).

Шаг 1. Формирование пространства признаков.

Допустим, предметами мониторинга параметров сетевого трафика ЛВС АС ВН служат объекты некоторые класса (сетевые пакеты протокола IP), моделируемые в булевом пространстве признаков $x_1, x_2, ..., x_m$. Предположим, что на этапе обучения наблюдению подверглось 64 конкретных объектов (пакетов $K_1 - K_{64}$) в результате чего составлена таблица, в которой некоторые строки могут обладать одинаковыми значениями.

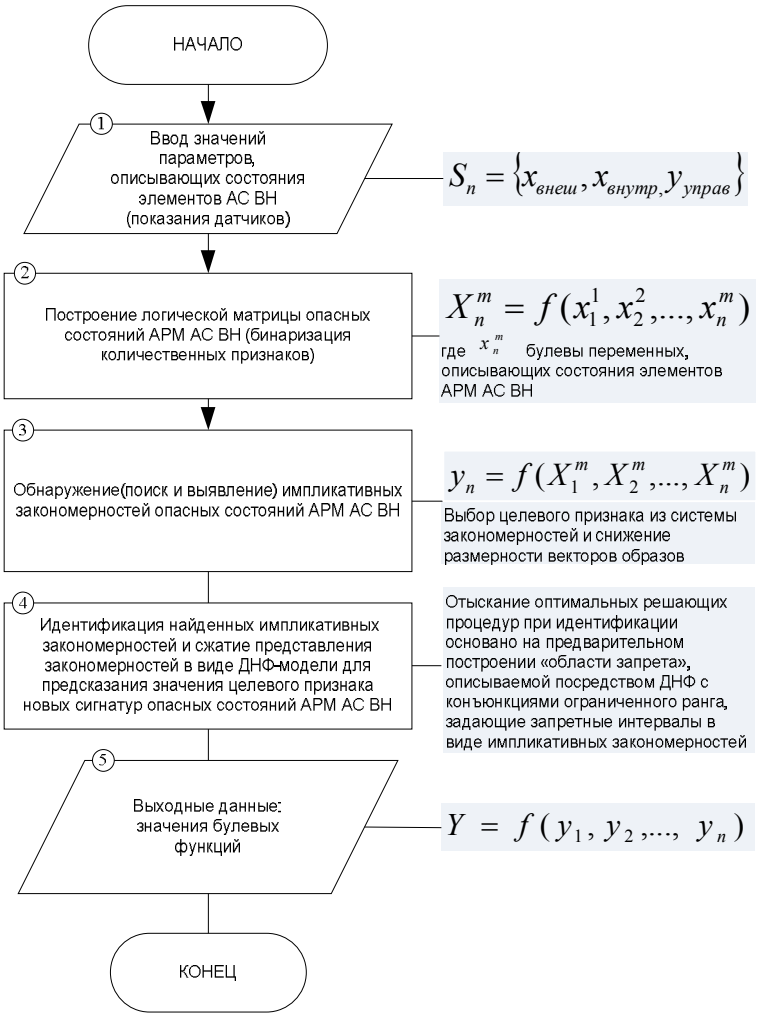


Рисунок 2.1 – Способ мониторинга опасных состояний АРМ АС ВН на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга

Для мониторинга опасных состояний АРМ АС ВН построим матрицу информативности признаков КА. Логические переменные (ЛП) $x_1, ..., x_2$ описывают параметрами инициирующего состояния АРМ (значение «1» соответствует появлению инициирующего события; значение «0» соответствует отсутствию инициирующего события).

В качестве наблюдаемых свойств объектов исследуемого класса параметров опасных состояний АРМ используются состояния X_i^j, где $j \in \{1,2,3,4,5,6\}$.

Поиск закономерностей опасных состояний АРМ АС ВН будем осуществлять в форме конъюнкций. Число термов *k* в конъюнкции называется её рангом. Конъюнкции небольшого ранга обладают важным преимуществом - они имеют вид привычных для человека логических высказываний и легко поддаются содержательной интерпретации.

Максимальный ранг конъюнкций *k* обычно устанавливают от 3 до 7, из соображений интерпретируемости (понятности), потому что невозможно уследить за смыслом высказываний, содержащих слишком большое количество условий. На практике используют различные эвристики для сокращённого целенаправленного поиска конъюнкций, близких к оптимальным. Идея всех этих методов заключается в том, чтобы не перебирать огромное количество заведомо неинформативных предикатов [14].

Таблица 2.1

Формирование пространства признаков

	x_1	x_2	x_3	x_4	x_5	x_6
Объект X_1	0	0	1	1	1	1
Объект X_2	1	1	0	0	0	0
…….	.	.	.	.	.	.
Объект X_{64}	1	0	0	0	1	1

Шаг 2. Построение модели исследуемого класса в алгебраической форме:

в виде дизъюнктивной нормальной форме (ДНФ) запрета, если признаков минимально;

в виде характеристической функции – булева функции запрета.

При рассмотрении булевых функций с большим числом переменных описанные способы приведут к слишком громоздким таблицам и матрицам. В этих случаях более практичным окажется алгебраический способ представления, когда булева функция записывается формулой, задающей некоторую суперпозицию достаточно простых и имеющих специальные обозначения функций, которые образуют базис алгебраического представления.

Элементами булевой алгебры являются булевы константы, булевы переменные и булевы функции. Булевых констант всего две, и их принято обозначать через 0 и 1. Значениями булевых переменных могут служить только булевы константы. Булевы функции, называемые иногда функциями алгебры логики (ФАЛ), также принимают значения из множества {0, 1}. Аргументами булевых функций являются булевы переменные. Будем полгать, что их число всегда конечно. Комбинации значений булевых переменных $x_1,x_2,...x_n$ называют наборами. Множество наборов образуют булево пространство M, содержащее 2^x элементов. Наборы будем рассматривать как булевы векторы, в которых последовательно перечисляются значения переменных. Например, вектор 111010 задает следующую комбинацию значений переменных: $x_1 = 1$, $x_2 = 1$, $x_3 = 1$, $x_4 = 0$, $x_5 = 1$, $x_2 = 1$. Расстоянием между двумя элементами в булевом пространстве принято считать число переменных, принимающих различные значения в этих элемента. Например, расстояние между элементами 111010 и 010110 равно 3. Чтобы задать булеву функцию, надо определить ее значения на всех наборах, тогда функция будет полностью, или всюду, определена. Мы будем рассматривать в основном именно такие функции. Случаи, когда значения функции определены лишь на некото-

рых наборах называются не полностью, или не всюду, определенными. Простейшим способом задания булевой функции является табличный, при котором строится таблица всех наборов и соответствующих им значений функции. Можно ограничиться перечислением лишь тех наборов, на которых булева функция f принимает значение 1. Множество таких наборов называется характеристическим множеством функции *f* и обозначается через M_f. Это представление более компактно, особенно в тех случаях, когда мощность (для конечного множества – число элементов) множества M_f относительно невелика. Множество M_f удобно представлять при этом в форме булевой матрицы, строками которой служат отдельные элементы из M_f. Назовем этот способ задания булевой функции поэлементным. При рассмотрении булевых функций с большим числом переменных описанные способы приведут к слишком громоздким таблицам и матрицам. В этих случаях более практичным окажется алгебраический способ представления, когда булева функция записывается формулой, задающей некоторую суперпозицию достаточно простых и имеющих специальные обозначения функций, которые образуют базис алгебраического представления. Наиболее известен и во многих отношениях удобен булев базис, состоящий из одноместной функции «отрицание» ($\neg$x , или $\bar{x}$) и двуместных функций «конъюнкция» ($x_1 \wedge x_2$, или x_1x_2) и «дизъюнкция» ($x_1 \vee x_2$). Эти функции, называемые также функциями НЕ, И и ИЛИ соответственно. Конъюнкция и дизъюнкция являются коммутативными и ассоциативными операциями, что означает выполнение равносильностей: $x_1x_2 = x_2x_1$, $x_1 \vee x_2 = x_2 \vee x_1$, $(x_1x_2)x_3 = x_1(x_2x_3)$, $(x_1 \vee x_2) \vee x_3 = x_1 \vee (x_2 \vee x_3)$. Это позволяет ввести в рассмотрение соответствующие многоместные функции: дизъюнкцию $x_1 \vee x_2 \vee ... \vee x_k$ принимающую значение 1 тогда и только тогда, когда хотя бы один из аргументов примет значение 1, и конъюнкцию $x_1x_2...x_k$, принимающую значение 1 в том и только том случае, если все аргументы примут это значение. Многоместная конъюнкция различных переменных, когда некоторые из них могут быть заменены их отрицаниями, называется элементарной конъюнкцией (минтерм). Элементарная дизъюнкция (макстерм) образуется дизъюнкцией конечного множества логических переменных (аргументов) и их отрицаний. Примеры элементарных конъюнкций: x_1, $x_2\bar{x}_3$, $x_1\bar{x}_2\bar{x}_5x_6$. Если в элементарной конъюнкции присутствуют все из рассматриваемых переменных $x_1,x_2,...x_n$, она называется полной. Примеры полных элементарных конъюнкций при *n=4*: $x_1\bar{x}_2\bar{x}_3x_4$, $\bar{x}_1\bar{x}_2\bar{x}_3x_4$, $x_1x_2\bar{x}_3x_4$. Число аргументов, образующих элементарную конъюнкцию или дизъюнкцию, является её рангом. Число минтермов и макстермов совпадает с числом наборов различных аргументов, т.е. для *n* аргументов их будет соответственно $N=2^n$. Общее число различных функций от n аргументов равно 2^{2^n} (пример, *n =1, 2, 3* соответственно *2, 16, 256*). Если логическая функция представлена через инверсию, конъюнкцию и дизъюнкцию, то такая форма ее представления называется нормальной. Любая булева функция может быть представлена в дизъюнктивной нормальной форме (ДНФ), из чего следует полнота системы функций, образующих булев базис, т.е. возможность представления суперпозициями этих функций любых булевых функций. При использовании аналитических форм представления логических функций используется принцип суперпозиции, заключающийся в замене одних аргументов данной функции другими. Например, если аргументы $Z = Z(X,Y)$ являются в свою очередь, функциями других аргументов $X = X(a,b)$ и $Y = Y(c,d)$, можно образовать функцию $Z = Z(a,b,c,d)$. Существует простой способ перехода от табличной формы представления булевой, функции к частному случаю ДНФ, а именно к совершенной дизъюнктивной нормальной форме (СДНФ), в которой все элементарной конъюнкции должны быть полными. Члены СДНФ получаются из

элементов характеристического множества M_f путем замены их компонент символами соответствующих переменных и простановки знаков отрицания над символами переменных, принимающих в рассматриваемом наборе значение 0. Например, $M_f = \{000,001,101\}$, то СДНФ функции f представляется выражением $\bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \vee x_1\bar{x}_2x_3$.

Представим каждую элементарную конъюнкцию рассматриваемой ДНФ *троичным вектором*, компоненты которого получают значения «–», 0 ИЛИ 1, если соответствующие им переменные отсутствуют в конъюнкции, входят в неё под знаком отрицания или входят в неё без знака отрицания соответственно. Интерпретируем этот вектор как множество двоичных векторов, которые можно получить из него заменой значений «–» всевозможными комбинациями нулей и единиц, данное множество, называемое интервалом булева пространства *M*, оказывается характеристическим множеством рассматриваемой элементарной конъюнкции. В множество М попадают *2к* наборов, где *k* – число значений «-» в троичном векторе, или, что то же самое, число переменных, символы – которых отсутствуют в рассматриваемой элементарной конъюнкции. Характеристическое множество булевой функции, представленной некоторой ДНФ, оказывается равным объединению всех интервалов, соответствующих элементарным конъюнкциям, входящим в состав данной ДНФ. Элементарная конъюнкция $\bar{x}_1x_4x_6$ представляется троичным вектором *0--1-1* (полагаем *n=6*), которое можно представлять сжатое представление множества, образованного наборами *000101, 000111, 001101, 001111, 010101, 010111, 011101, 011111*, легко получаемого из вектора *0--1-1*. Подставляя вместо «-»произвольные комбинации нулей и единиц, получаем все элементы интервала. Поэтому множество рассматриваемого типа называется интервалом. Булевы функция, заданная посредством ДНФ $(x_1\bar{x}_3\bar{x}_4 \vee x_2x_3 \vee \bar{x}_1x_2\bar{x}_4)$ может быть отображена троичными векторами, объединение этих интервалов приведет к характеристическому множеству данной функции, упорядочив его *{0100, 0110, 0111, 1000, 1100, 1110, 1111}*. Анализ ДНФ и их характеристических множеств в ряде случаев существенно облегчается, если представляющие их множества троичных и булевых векторов группируются в матрицы. Заданная ДНФ, может быть задана троичной матрицей:

$$\begin{bmatrix} 1 & - & 0 & 0 \\ - & 1 & 1 & - \\ 0 & 1 & - & 0 \end{bmatrix}.$$

Кроме операций булева базиса (отрицания, конъюнкции и дизъюнкции), в алгебраических представлениях используются иногда двуместные операции «дизъюнкция с исключением» $(x_1 \oplus x_2)$, «эквиваленция» $(x_1 \sim x_2)$ и «импликация» $(x_1 \to x_2)$. Таким образом, в алгебраическом представлении булева функция выражается формулой в виде некоторой последовательности символов переменных, операторов $\neg,\wedge,\vee,\oplus,\sim,\to$, а также скобок, указывающих порядок применения операторов. Существуют правила использования формул:

1) любой символ булевой переменной ($x_1,x_2,\ldots x_n$ могут использоваться также символы a,b,…z) являются формулой;

2) если A – формула, то $\neg A$, или $\bar{A}$, – тоже формула;

3) если A и B - формулы, то выражения $(A \vee B)$, $(A \wedge B)$, $(A \oplus B)$, $(A \sim B)$, $(A \to B)$ также являются формулами. Совокупность правил задает порождаемый синтаксис формул. Существуют классы операторов. Оператор связывает формулы тем сильнее, чем меньше номер класса, к которому он принадлежит:

1 класс: $\neg$;

2 класс: $\wedge$;

3 класс: $\vee, \oplus$;

4 класс: $\sim, \rightarrow$.

Преобразование алгебраических выражений логических функций основано на том, что возможно изменение структуры цепей логических схем без изменения их результирующего действия. Часть из них совпадает с соответствующими законами, применяемыми при преобразовании обычных алгебраических выражений, часть же является специфичной для алгебры логики.

В нашем рассматриваемом примере при построении модели класса видим пустыми интервалы третьего ранга и выдвигаем гипотезу о соответствующих импликативных закономерностях.

Предположим, что среди интервалов, ранги которых не превышают трех, пустыми оказались лишь те, которые представлены строками следующей троичной матрицы, где компоненты принимают значения из трехэлементного множества $\{0,1,-\}$:

$$\begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{matrix}$$
$$T = \begin{bmatrix} 1 & - & 1 & - & - & 0 \\ - & 1 & - & - & 0 & 1 \\ 0 & - & - & 0 & 1 & - \\ - & 0 & - & 1 & - & 1 \\ - & 0 & 0 & 0 & - & - \end{bmatrix} \qquad (2.1)$$

Эта матрица будет моделью исследуемого класса. Строки интерпретируются как импликативные закономерности: первая строка утверждает, что в данном классе не существует объектов, обладающих признаками x_1 и x_3, но не обладающих в тоже признаком x_6.

Шаг 3. Выбор целевого признака их системы закономерностей и упрощение.

Пусть в данном примере роль целевого признака играет признак – x_2.

При $x_2 = 0$ становится излишней строка 2, так как задаваемая ею область запрета не содержит элементов с таким значением признака x_2 и следовательно, не пересекается с интервалом возможного существования объекта, не обладающего признаком x_2. Удалив ее вместе со столбцом x_2, получим остаток:

$$\begin{matrix} x_1 & x_3 & x_4 & x_5 & x_6 \end{matrix}$$
$$T = \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & - & 0 & 1 & - \\ - & - & 1 & - & 1 \\ - & 0 & 0 & - & - \end{bmatrix} \begin{matrix} 1 \\ 3 \\ 4 \\ 5 \end{matrix} \qquad (2.2)$$

Если, $x_2 = 1$, следует анализировать остаток матрицы Т.

$$\begin{matrix} x_1 & x_3 & x_4 & x_5 & x_6 \end{matrix}$$
$$\begin{bmatrix} 1 & 1 & - & - & 0 \\ - & - & - & 0 & 1 \\ 0 & - & 0 & 1 & 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \qquad (2.3)$$

Представим в графической форме дерево идентификации признака x_6 (рис. 2.2).

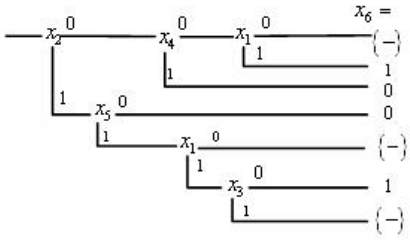


Рис. 2.2. Дерево идентификации признака x_6.

Обнаружение (поиск и выявление) импликативных закономерностей опасных состояний АРМ АС ВН основано на выборе целевого признака из системы закономерностей и снижение размерности векторов образов сигнатур опасных состояний.

Идентификация импликативных закономерностей образов опасных состояний АРМ АС ВН основана на предварительном построении «области запрета», описываемой посредством дизъюнктивной нормальной форме (ДНФ) с конъюнкциями ограниченного ранга, задающие запретные интервалы в виде импликативных закономерностей.

Заключение

Таким образом, алгоритм мониторинга опасных состояний АРМ АС ВН на основе поиска импликативных закономерностей в форме конъюнкций ограниченного ранга, основанный на распознавании признаков опасных состояний АРМ, связанных с запретами на некоторые комбинации признаков, позволяет осуществлять не весь перебор возможных классификационных признаков состояний, а ограничиться сокращенным перебором.

Литература:

1. ГОСТ 20911 – 89. Техническая диагностика Термины и определения.

2. ГОСТ Р 22.1.12-2005. Безопасность в чрезвычайных ситуациях. Структурная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования.

3. ГОСТ 27518-87. Межгосударственный стандарт. Диагностирование изделий. Общие требования. Переиздан. 2009.

4. Сидельников, О.В. Распознавание образов компьютерных атак на основе логического вывода закономерностей состояний информационно-телекоммуникационных систем // Математические методы и информационно-технические средства. Материалы XI Всерос. НПК. – Краснодар: Краснодарский университет МВД России, 2015. – С.263-267.

5. Рябинин И.А. Надежность и безопасность структурно-сложных систем.– СПб.: Политехника, 2000.– 248 с.: ил. – С.98.

6. Федеральный закон РФ № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации».

7. Дружинин Г.В. Надежность автоматизированных систем. Изд. 3-е перераб. и доп. – М: «Энергия», 1977.– 536 с.: ил.

8. Надежность технических систем: Справочник / Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; Под ред. И.А.Ушакова. – М: Радио и связь, 1985.– 608 с.: ил.

9. Можаев А.С. Общий логико-вероятностный метод анализа надежности сложных систем.– СПб.: Политехника, 2000.– 248 с.: ил.

10. Острейковский В.А., Швыряев Ю.В. Безопасность атомных станций. Вероятностный анализ – М: ФИЗМАТЛИТ, 2008.– 352 с.

11 Шарай В.А. Математическое обеспечение информационных систем мониторинга надежности и безопасности сложных технических систем: дис. ... канд. техн. наук: 05.13.01 / Шарай Вячеслав Александрович – Краснодар, 2013.

12 Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств. URL: http://itdefence.ru.

13 Гарбук, С.В., Комаров, А. А., Салов Е. И. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств (по материалам интернет-изданий за 2008-2010 годы) / Защита информации. INSIDE № 6'2010. URL: http://securitylab.ru/analvtics/398184.php.

14. Закревский, А.Д. Логика распознавания / Изд.2-е, доп. – М.: Едиториал УРСС, 2003. – 144 с.

Слесарева Е.А., Задохина Н.В., Страхов А.А.
Московский университет МВД России имени В.Я. Кикотя

ТЕХНОЛОГИЯ ВЫЯВЛЕНИЯ ГРУБЫХ ОШИБОК ИЗМЕРЕНИЙ

Промах (грубая ошибка) – погрешность, существенно превосходящая ожидаемую погрешность. Промахи относятся к аномальным результатам измерений. Обычно возникновение промаха обусловлено резким нарушением условий измерения: грубый просчет экспериментатора, сбой аппаратуры и т.д.

Наличие промаха может сильно исказить окончательный результат. Проще всего, установив причину промаха, устранить его в процессе измерения. Если в процессе измерения промах не был исключен, то это следует сделать при обработке результатов измерений, использовав специальные статистические критерии, позволяющие объективно выделить в каждой серии измерений грубую ошибку, если она имеется.

Пример. Ниже представлены девять независимых равноточных измерений напряжения в электрической цепи, В:

140; 155; 135; 145; 110; 150; 135; 140; 155.

Используя критерий Шовене, сделайте вывод о присутствии или отсутствии грубой ошибки (промаха) в данном массиве.

Решение. Использование статистических функций MS Excel позволяет автоматизировать процесс проверки серии измерений на наличие грубой ошибки (промаха).

1. В ячейки B2:B10 вводим результаты девяти измерений: 140; 155; 135; 145; 110; 150; 135; 140; 155.

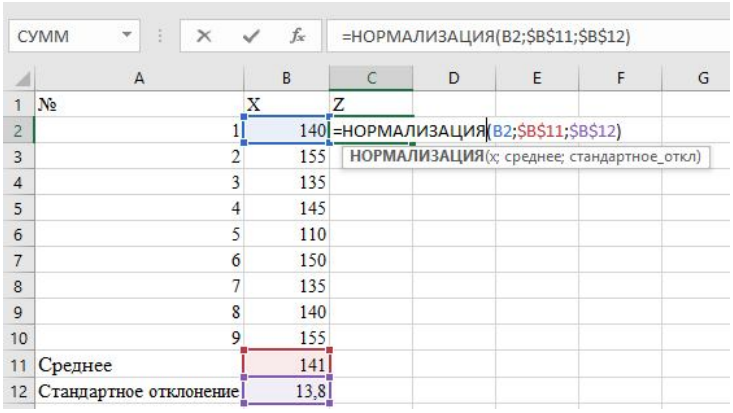
2. Вычисляем среднее арифметическое измерений напряжения в электрической цепи: в ячейку B11 вводим =СРЗНАЧ(B2:B10). В результате получаем $\overline{X} = 141$.

3. Вычисляем стандартное отклонение измерений напряжения: в ячейку B12 вводим =СТАНДОТКЛОН.В(B2:B10). В результате получаем $S = 13{,}8$.

4. Для каждого результата измерения вычисляем Z – число стандартных отклонений, на которое данный результат измерения отклоняется от среднего арифметического измерений: в ячейку C2 вводим =НОРМАЛИЗАЦИЯ(B2;B11;B12). В результате получаем $z_1 = -0{,}04$ (число стандартных отклонений, на которое первый результат измерения $x_1 = 140$ отклоняется от среднего значения $\overline{X} = 141$).

С помощью маркера автозаполнения копируем формулу =НОРМАЛИЗАЦИЯ(B2;B11;B12) в ячейки B3:B10. Для копирования формулы необходимо использовать абсолютную ссылку на ячейки B11 и B12 (рис. 1). Получаем число стандартных отклонений, на которое каждый результат измерения отклоняется от среднего значения.

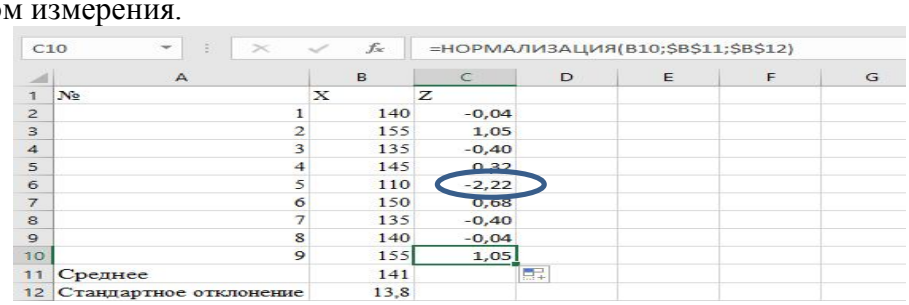
Замечание 2. Функция НОРМАЛИЗАЦИЯ(x; среднее;станд_откл) имеет три аргумента: x (отдельное измерение); среднее (среднее арифметическое измерений); станд_откл (стандартное отклонение);. В нашем случае: $x_1 = 140$; $\overline{X} = 141$ (ячейка B11); $S = 13{,}8$ (ячейка B12).



	A	B	C	D	E	F	G
1	№	X	Z				
2	1	140	=НОРМАЛИЗАЦИЯ(B2;B11;B12)				
3	2	155					
4	3	135					
5	4	145					
6	5	110					
7	6	150					
8	7	135					
9	8	140					
10	9	155					
11	Среднее	141					
12	Стандартное отклонение	13,8					

Рис. 1. Процедура нормализации

5. Анализ полученных результатов делает очевидным, что значение $x_5 = 110$ – аномально маленькое, так как $z_5 = -2{,}22$ (рис. 2). В этой связи необходимо проверить: значение $x_5 = 110$ является промахом (и может быть отброшено) или закономерным результатом измерения.



	A	B	C	D	E	F	G
1	№	X	Z				
2	1	140	-0,04				
3	2	155	1,05				
4	3	135	-0,40				
5	4	145	0,32				
6	5	110	-2,22				
7	6	150	0,68				
8	7	135	-0,40				
9	8	140	-0,04				
10	9	155	1,05				
11	Среднее	141					
12	Стандартное отклонение	13,8					

Рис. 2. Выявление аномального результата измерения

6. Выясняем степень «аномальности» значения $x_5 = 110$. Находим вероятность того, что среди последующих измерений не появятся такие же аномальные результаты (как $x_5 = 110$), то есть результаты последующих измерений окажутся в пределах $\pm 2{,}22$ стандартных отклонений от среднего значения (рис. 3): в ячейку B13 вводим =ABS(2*НОРМ.СТ.РАСП(C6;1)-1). В результате получаем $P = 0{,}973$ (рис. 4).

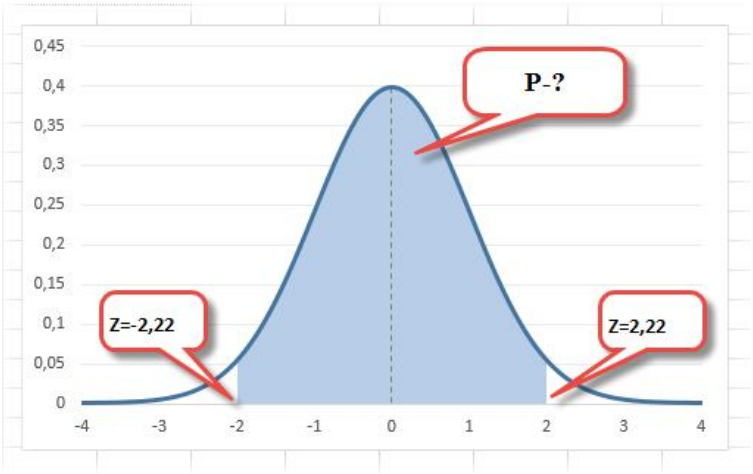
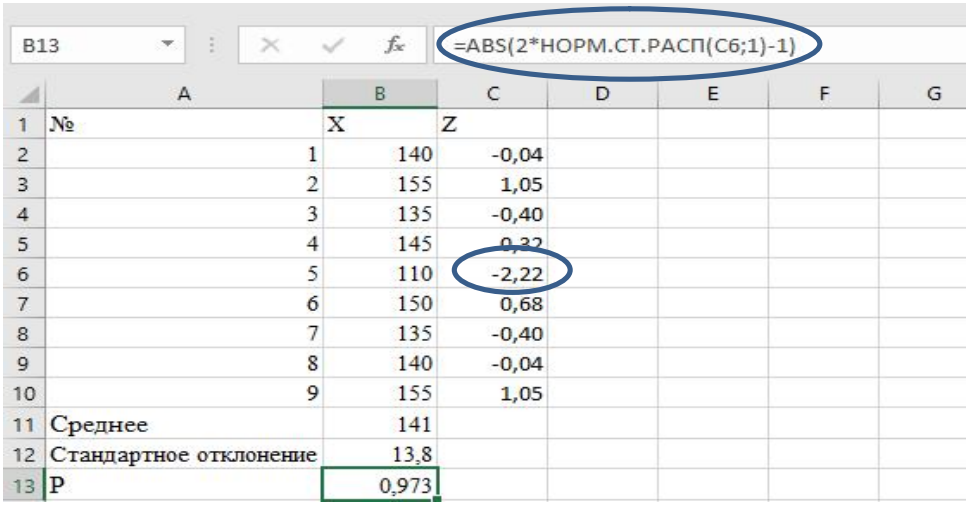


Рис. 2.8 Вероятность того, что результат измерения окажется в пределах $\pm 2{,}22$ стандартных отклонений от среднего значения

Замечание 3. Функция ABS(число) возвращает модуль числового значения.

Замечание 4. Функция НОРМ.СТ.РАСП предназначена расчета вероятности по нормированным данным.

Функция НОРМ.СТ.РАСП(z; интегральная) имеет два аргумента: z (нормированное значение отдельного измерения); интегральная (если установлена 1, то рассчитывается вероятность, в противном случае плотность вероятности). В нашем случае: $z = z_5 = -2{,}22$ (ячейка C6); интегральная (1).

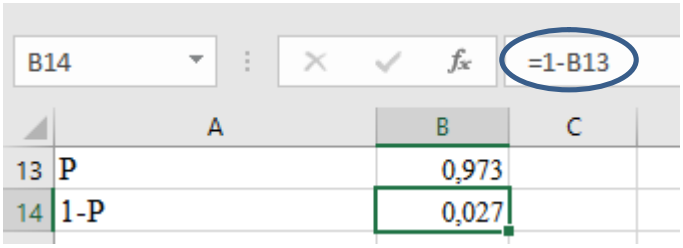


	A	B	C	D	E	F	G
1	№	X	Z				
2	1	140	-0,04				
3	2	155	1,05				
4	3	135	-0,40				
5	4	145	0,32				
6	5	110	-2,22				
7	6	150	0,68				
8	7	135	-0,40				
9	8	140	-0,04				
10	9	155	1,05				
11	Среднее	141					
12	Стандартное отклонение	13,8					
13	P	0,973					

Рисунок 4. Вычисление *P*

Далее находим вероятность того, что при последующих измерениях появятся результаты (не менее аномальные чем $x_5 = 110$), которые будут отличаться по крайней мере на $\pm 2{,}22$ стандартных отклонений от среднего значения: в ячейку B14 вводим =1-B13.

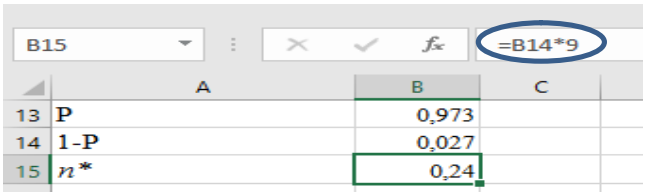
В результате получаем $1 - P = 1 - 0{,}973 = 0{,}027$ (рис. 5).



	A	B	C
13	P	0,973	
14	1-P	0,027	

Рисунок 4. Вычисление *1-P*

7. Вычисляем число ожидаемых измерений n^*, результат которых не менее аномален (чем $x_5 = 110$). (рис. 6): в ячейку B15 вводим =B14*9. В результате получаем $n^* = (1 - P)n = 0{,}027 \cdot 9 = 0{,}24$. То есть для девяти измерений можно получить только 0,24 случаев такого же аномального результата, как $x_5 = 110$.

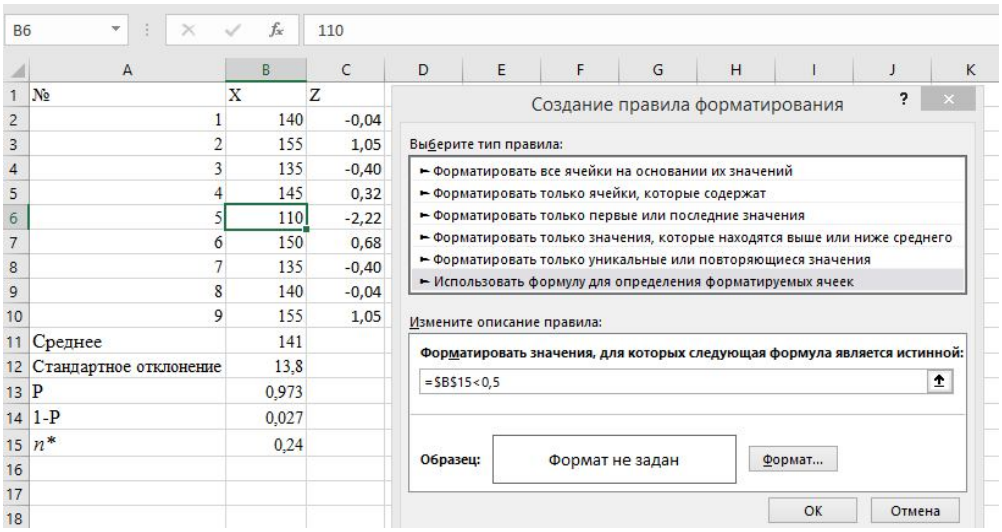


	A	B	C
13	P	0,973	
14	1-P	0,027	
15	n^*	0,24	

Рис. 6. Вычисление n^*

1. Так как $n^* = 0{,}24 < 0{,}5$, результат измерения $x_5 = 110$ не удовлетворяет критерию Шовене. Итак, значение $x_5 = 110$ является грубой ошибкой и может быть отброшено.

Для наглядности выделим ячейку B6 и создадим правило для условного форматирования данной ячейки (рис. 7): если значение $x_5 = 110$ является грубой ошибкой, то ячейка заливается желтым цветом (рис. 2.13, 2.14).



	A	B	C
1	№	X	Z
2	1	140	-0,04
3	2	155	1,05
4	3	135	-0,40
5	4	145	0,32
6	5	110	-2,22
7	6	150	0,68
8	7	135	-0,40
9	8	140	-0,04
10	9	155	1,05
11	Среднее	141	
12	Стандартное отклонение	13,8	
13	P	0,973	
14	1-P	0,027	
15	n^*	0,24	
16			
17			
18			

Рис. 7. Создание правила форматирования

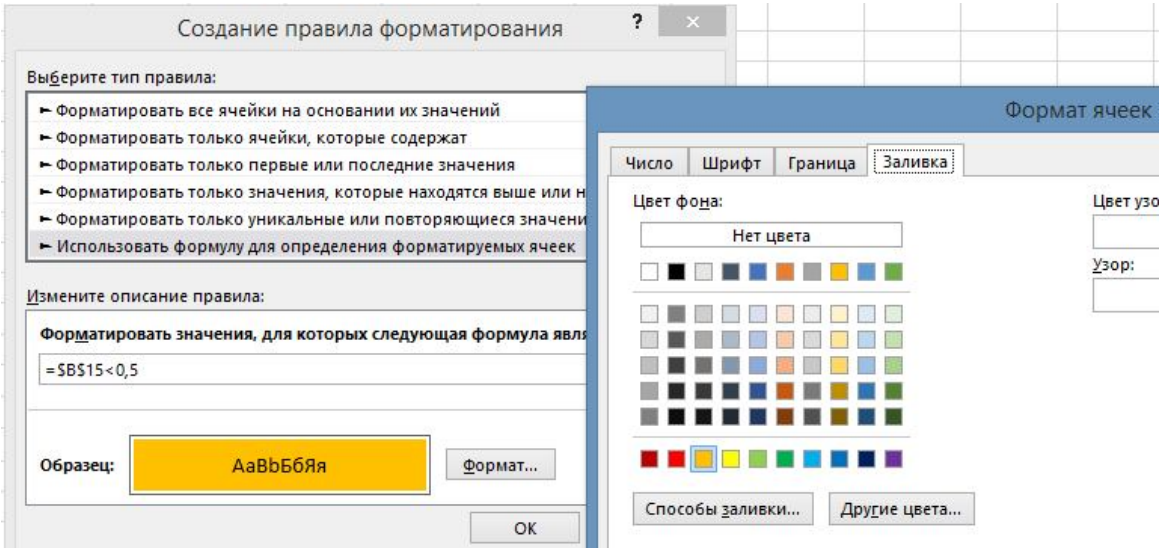


Рис. 8. Установление пользовательского формата

	A	B	C	D	E
1	№	X	Z		
2	1	140	-0,04		
3	2	155	1,05		
4	3	135	-0,40		
5	4	145	0,32		
6	5	110	-2,22		

Рисунок 9. Условное форматирование ячейки, содержащей аномальный результат измерения

Литература:

1. Кинякин В.Н., Слесарева Е.А. Концепт алгоритма для начинающих // Вестник Московского университета МВД России № 7, 2016.

2. Печенкова Е.А. Значение теории копинг-поведения при профессиональной подготовке специалистов силовых структур России (гендерный аспект) // Подготовка кадров для

силовых структур: современные направления и образовательные технологии Материалы двадцать первой всероссийской научно-методической конференции. Иркутск, 2016. С. 111-114.

3. Слесарева Е.А.. Смирнов Д.Е. Информационные технологии как средство решения практических задач в деятельности психолога // Государственная служба и кадры 2016, №4, с. 127-130

4. Савчук В.П. Обработка результатов измерений. Физическая лаборатория. Ч1: Учеб. пособие для студентов вузов / В.П. Савчук.- Одесса: ОНПУ, 202.-54с.

Солодуха Р.А., Мишин С.А., Волков А.А.
Воронежский институт МВД России

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ OLAP И OLTP СЕГМЕНТОВ СТЕГАНОАНАЛИТИЧЕСКОГО ПРОГРАММНОГО КОМПЛЕКСА

Для оптимизации параметров функционирования стеганоаналитического программного комплекса (САПК) [2] предложена ее имитационная модель. Имеется сетевая папка изображений, которую каждые 3-5 минут через FTP-клиент наполняют специалисты экспертно-криминалистических центров (ЭКЦ), после чего в автоматическом режиме начинается процесс обнаружения скрытых стеганоконтейнеров в изображении, и в случае обнаружения вложения, графический файл отправляется специалисту из ЭКЦ, приславшему это изображение с заключением [2-3]. Определена максимальная нагрузка на САПК, при которой система будет работать без перебоев. Проведен оптимизационный эксперимент для расчета значений параметров, при которых достигается наилучший результат моделирования системы.

Для разработки имитационной модели было использовано программное обеспечение, удовлетворяющее требованиям поставленной задачи: AnyLogic 8.1.0 [1].

Разрабатываемую модель можно представить в виде следующих основных блоков (таблица 1).

Первый блок имитирует процесс поступление в САПК новых графических файлов, которые пользователи через FTP – клиент загружают в сетевую папку. Он состоит из элемента генерации поступления картинок (source), через который картинки от пользователей прибывают согласно времени между прибытиями, промежутки времени указаны в исходных данных (3-5 мин.), за один раз может поступить от 1 до 3 картинок. После поступления заявок от пользователей в виде графических файлов, система фиксирует модельное время каждой прибывшей заявки (TimeMeasureStart), после чего файл через FTP – клиент (Service) отправляется в сетевую папку БД_1 (Queue), в которой хранятся графические файлы для проверки. Когда заявка поступила в сетевую папку, запускается скрипт выполнения в автоматическом режиме САПК. Данный скрипт является приложением, написанным на языке Autoit.

Таблица 1.

Блоки имитационной модели САПК

№	Название блока
1.	Блок заполнения хранилища изображений
2.	Блок Autoit
3.	Блок работы приложения GUI MATLAB
4.	Блок работы FTP сервера
5.	Блок распределения графических файлов

6.	Блок хранения файлов без вложения
7.	Блок хранения файлов с вложением
8.	Блок исходных данных

Скрипт обнаруживает наличие графического файла в сетевой папке, если папка имеет хотя бы один файл, скрипт отправляет его в САПК (GUI MATLAB), после чего ожидает поступление новой заявки.

После отправки файла в САПК происходит анализ графического файла на признак вложенности (Delay), после чего файл отправляется (Conveyor) на распределитель графических файлов.

Суть распределителя графических файлов (SelectOutput) заключается в распределении картинок в ту или иную сетевую папку, в зависимости от наличия стегановложения. С вероятностью 0.7 стегановложение в картинке присутствует. Если в графическом файле отсутствует стегановложение, то файл отправляется в блок хранения файлов без вложения. Он состоит из элемента БД_2 (Queue), который является накопителем файлов. За частую картинка содержит в себе некую стегановложенность, такие картинки через FTP – клиент (Service) отправляются в сетевую папку БД_3 (Queue), которая доступна пользователям.

Перед отправкой файла FTP – клиентом в сетевую папку, фиксируется модельное время (TimeMeasureStart), которое показывает время, затраченное на ответ пользователю о наличии стегановложения. FTP – клиент работает на стороне клиента, который удаленно обращается к FTP – серверу (ResourcePool). К FTP – серверу одновременно может быть подключено не более 2-х FTP – клиентов. Это связанно с безопасностью работы сервера. Подключиться к FTP – серверу может только один пользователь, таким образом организована очередь при загрузке графических файлов в БД_1, а второй FTP – клиент использует аналитик при выгрузке картинки со стегановложением в БД_3.

Для отображения распределения длительности ответа экспертом пользователю о наличии стегановложения используется гистограмма и данные гистограммы. Данные гистограммы указывают процентное соотношение времени получения ответа пользователем от общего числа обработанных заявок. Данные в свойствах гистограммы берутся из фиксации модельного времени в блоке хранения файлов с вложением.

Блок исходных данных позволяет задать оптимальные значения функционирования САПК и изменять эти значения динамически в процессе функционирования системы. Для отображения вместимости БД, времени задержки FTP – клиента, времени работы скрипта Autoit, интенсивности потока и количества изображений с вложениями и без них необходимы следующие параметры (таблица 2).

Таблица 2.

Свойства параметров и переменных направлений передачи сообщений

Названия переменных	Тип данных	Значение
Вместимость_БД_1	int()	100
Время_задержки_FTP_1	int()	2
Время_раб_скрипта	int()	4
Время_задержки_FTP_2	int()	2
кол_во_без_вложений	int()	0

кол_во_с_вложениями	int()	0
интенс_потока	int()	0

Для определения значения параметра кол_во_без_вложений в элементе БД_2 необходимо указать действие при проходе к выходу (Рис. 1).

Рис. 1. Действие при подходу к выходу

Найдем количество поступивших заявок в БД_1 [4]: $X = \sum_{i=1}^{n} x_i$, где n – количество поступивших заявок, x_i – i-ая поступившая заявка. Количество файлов без стегановложения: $X' = \sum_{i=1}^{n} x_i'$, тогда $X'' = X - X' = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} x_i'$ – количество файлов с стегановложением.

Случайное время ожидания заявки в очереди начала обслуживания считаем по экспоненциальному закону: $f(t) = \nu e^{-\nu t}$, где ν – среднее число заявок, приходящих на обслуживание в единицу времени $\nu = 1/\overline{t}$, где $\overline{t}$ – среднее время ожидания в очереди. Обслуживание заявки связано зачастую с случайной величиной и обычно подчиняется показательному закону распределения с равновероятной плотностью $f(t_{\text{об}}) = \mu e^{-\mu t}$, где μ – среднее число обслуживаемых заявок в единицу времени. Тогда интенстивность нагрузки на сервер определим по формуле $\rho = \frac{\lambda}{\mu}$, где λ – интенсивность потока заявок, $\lambda = 1/\overline{r}$, где $\overline{r}$ – среднее значение времени между i – ой заявкой и $i + 1$.

Для определения значения параметра кол_во_с_вложениями в элементе БД_3 укажем действие при проходе к выходу (Рис. 2).

Рис. 2. Действие при подходу к выходу

Для подсчета интенс_потока в элементе «Картинка» укажем действие при выходе (Рис. 3).

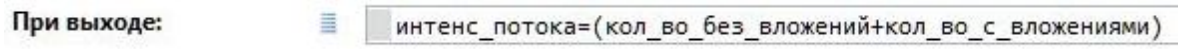


Рис. 3. Действие при выходе

Результат работы имитационной модели представлен на рисунке 4.

По истечению модельного времени (100000 секунд), можно сделать вывод о том, что при заданных параметрах, наиболее загруженным является FTP – сервер, который из-за медленной обработки САПК заявок от пользователей требует много ресурсов. Это обусловлено тем, что для хранения большого количества заявок необходимо либо ускорить процесс работы скрипта Autoit, либо увеличить емкость накопителя БД_1.

Все это говорит о том, что нужно оптимизировать работу производительности САПК, а для этого необходимо оптимальным образом соотнести заполнение емкости БД_1 для хранения изображений, ожидающих обработку и время работы скрипта.

Рис. 4. Запуск модели

Для расчета оптимальных параметров модели системы создается оптимизационный эксперимент.

Максимальной производительности системы, при имеющемся оборудовании можно достигнуть тогда, когда время работы скрипта Autoit будет минимальным, а загруженность БД_1 не более чем на 50%. Для этого в качестве целевой функции установлена зависимость времени работы скрипта от вместимости накопителя БД_1 (Рис. 5).

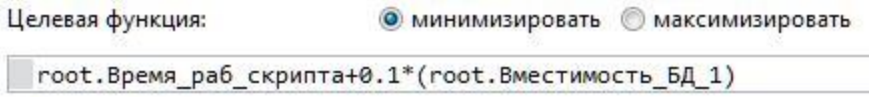


Рис. 5. Целевая функция

Параметрами оптимизации являются время выполнения скрипта и вместимость БД_1. Значения параметров оптимизации представлен на рисунке 6.

Параметры:

Параметр	Тип	Значение		
		Мин.	Макс.	Шаг
Вмести..._БД_1	дискретный	50	99	1
Время_...крипта	дискретный	0.5	5	0.1

Рис. 6. Значения параметра оптимизации

Результаты оптимизации представлены на рисунке 7.

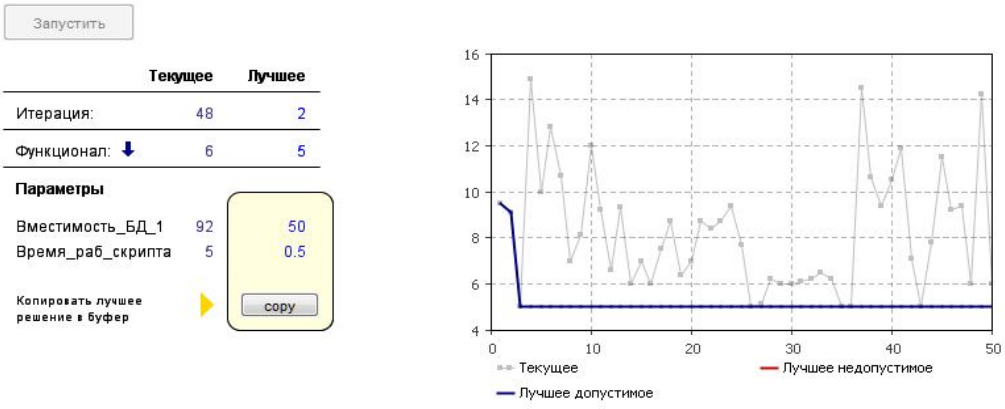


Рис. 7. Оптимизация модели

В правой колонке представлены оптимальные параметры для исследуемой системы:

- Оптимальная вместимость БД_1;
- Наилучшее время работы скрипта.

На рисунке 7 представлен график уменьшения времени обработки заявки в зависимости от вместимости БД_1.

Благодаря полученному значению можно сделать заключение, что для повышения производительности САПК при минимальных финансовых затратах на оборудование, а также для уменьшения времени работы скрипта при оптимальной вместимости БД_1 необходимо уменьшить время выполнения Autoit с соответствующей вместимостью накопителя БД_1.

С помощью построенной модели были проведены компьютерные эксперименты, которые позволили оценить эффективность работы исследуемой системы, а также спланировать мероприятия по оптимизации ее работы.

Также была проведена работа по оптимизации параметров, влияющих на производительность системы, вместимость БД_1 и время обработки ответа скриптом, в ходе которой были предприняты меры по повышению эффективности его функционирования. Результаты полученные в ходе моделирования процесса функционирования системы, отражают основные особенности функционирования реального объекта и позволяют качественно и количественно оценить его поведение.

Литература:

1. Официальный сайт компании AnyLogic [Электронный ресурс]. – Режим доступа: www.anylogic.ru

2. Солодуха, Р.А. Концепция информационного обеспечения стеганоаналитической системы / Р.А. Солодуха // Вестник Воронежского института МВД России. – 2016. – № 4. – С.156–162.

3. Атласов И.В., Солодуха Р.А., Кубасов И.А. Оценка достоверности результатов стеганоанализа серии изображений / И.В. Атласов, Р.А. Солодуха, И.А. Кубасов // Вестник Воронежского института МВД России. – 2018. – № 1. – С.51–65.

4. Аверченков, В.И. Основы математического моделирования технических систем: учебное пособие / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – М: Изд-во «Флинта», – 2011. – С.271.

Старостенко И.Н.

Краснодарский университет МВД России

ОСОБЕННОСТИ РАЗРАБОТКИ ПРАКТИЧЕСКИХ ЗАДАНИЙ В СРЕДЕ СИМУЛЯТОРА СЕТЕЙ И ТЕХНОЛОГИЙ PACKET TRACER

Симулятор Packet Tracer (PT) является ключевым программным средством для обучения компьютерным сетевым технологиям, позволяя создавать свои собственные модели сети, получать доступ к важным графическим представлениям этих сетей, настраивать различные промежуточные устройства, взаимодействовать между несколькими пользователями.

PT разработан для улучшения качества учебного процесса и дополняет обучение на реальном оборудовании. Программное решение PT позволяет осуществлять настройку и имитировать работу маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Настройки, в свою очередь, зависят от характера устройств: одни можно настраивать с помощью команд операционной системы Cisco IOS, другие – с помощью графического веб-интерфейса, третьи – посредством командной строки операционной системы или графического меню [1].

Текущей версией PT является PT 7.2. В новую версию добавлены новые устройства (сервер и устройство безопасности Meraki, домашний маршрутизатор, межсетевой экран ASA 5506), возможность развертывания устройства в конкретной серверной телекоммуникационной стойке, усовершенствованы существующие протоколы, добавлены новые протоколы (PPPoE, 802.1X), дополнительные команды IOS, связанные с безопасностью. Мобильная версия PT предназначена для поддержки мобильной версии CCNA и не включает физический режим и симуляцию Интернета вещей (Internet of Things), не содержит инструментов разработки и редактирования практических заданий.

Важной особенностью PT является невозможность открытия файла в предыдущей версии, если он был сохранен в более поздней версии PT.

Разработка новых заданий и учебных проектов, а также их редактирование в PT осуществляется с помощью специального инструмента – Activity Wizard (AW). Варианты использования AW разнообразны: редактирование существующего задания, разработка собственного задания, создание учебного проекта или реалистичного примера и сценария, разработка задания для соревнований, создание проектов обучающимися в качестве заданий для других обучающихся.

AW включает несколько разделов, ключевыми из которых являются Initial Network и Answer Network.

В Initial Network разработчик задает конфигурацию сети, с которой обучающийся будет начинать работу при первичном открытии файла PT.

Существует несколько вариантов реализации первичной конфигурации сети:

– полностью сконфигурированная сеть. При таком сценарии обучающиеся отрабатывают, как правило, простые навыки. Например, изучение принципов передачи информации, проверка доступности отдельных узлов или промежуточных устройств и др.

– сеть, содержащая ошибки конфигурации. Данный вариант заданий предназначен для проверки у обучающихся наличия навыков диагностики и устранения неполадок сети;

– сеть, в которой создана только физическая топология. Логическая настройка узлов и промежуточных устройств частично или полностью отсутствует. Обучающиеся должны самостоятельно осуществить настройку всех устройств сети, проверить их доступность;

– сеть отсутствует. Данный вариант задания является самым сложным: обучающийся должен создать физическое подключение между узлами и промежуточными устройствами с помощью соответствующих сред передачи данных, осуществить логическую настройку каждого устройства (рис. 1).

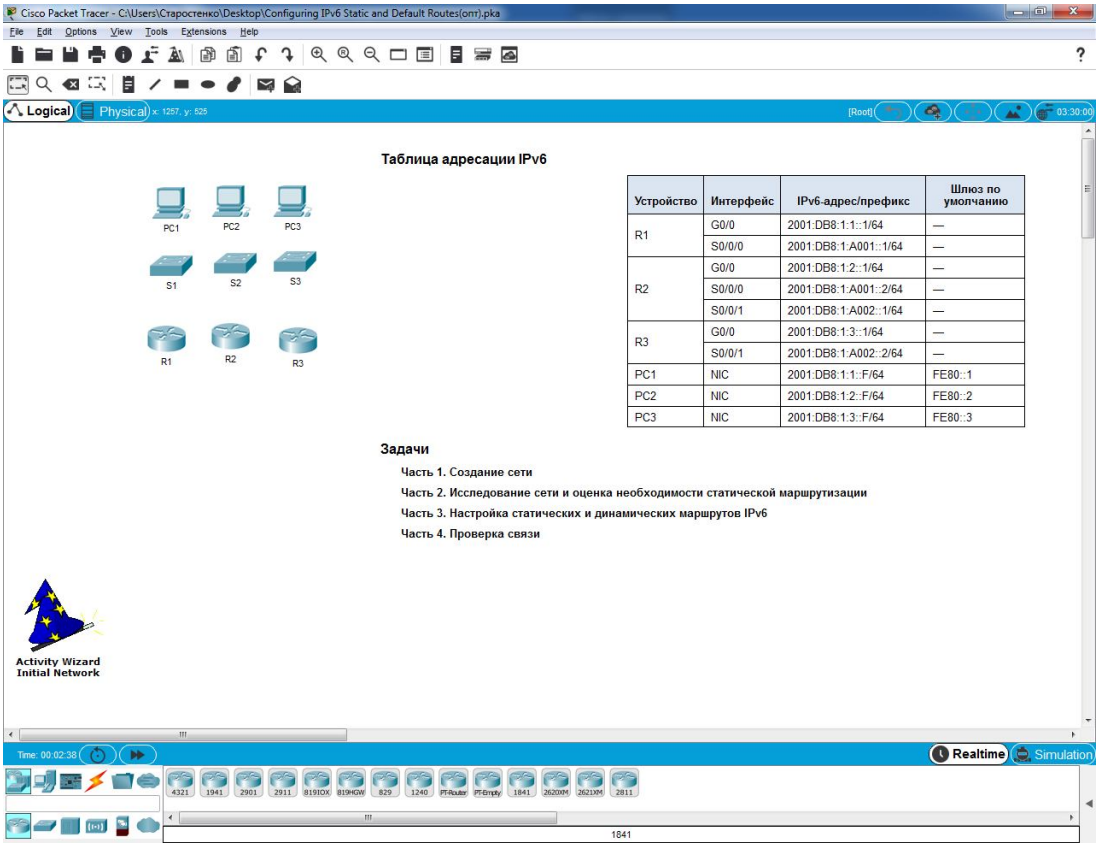


Рис. 1. Initial Network

Одним из способов создания Initial Network является копирование конфигурации из Answer Network и последующим её редактированием. Другой вариант – импорт из файла ранее созданной конфигурации (рис. 2).

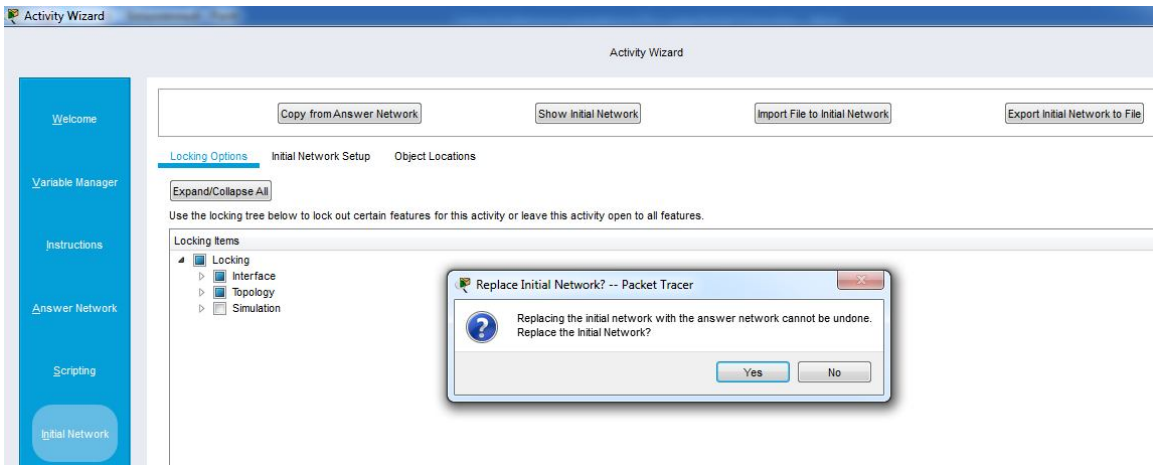


Рис. 2. Создание Initial Network

После создания Initial Network определяются функции, которые будут заблокированы и не будут доступны обучающимся при выполнении задания. Например, можно запретить доступ к физическому режиму или использование функций режима моделирования. Без режима моделирования обучающийся должен использовать командную строку компьютера для отправки сообщений и устранения неполадок. Ограничения могут быть более конкретными. Например, запрет изменения настроек интерфейса на определенном устройстве. Всего доступно блокирование более 100 функций и элементов, которые разделены на три категории: интерфейс, топология, симуляция.

В Answer Network создается «правильная» конфигурация сети, которая будет являться критерием оценки выполненного задания. В демонстрируемом примере сеть содержит три компьютера, три коммутатора и три маршрутизатора. В Answer Network указанные устройства соединяются с помощью соответствующего кабеля, настраиваются компьютеры, интерфейсы маршрутизаторов, задаются статические маршруты, отображается дополнительная информация (рис. 3). Answer Network можно также создать импортированием существующего pkt-файла и использовать его в качестве сети ответа.

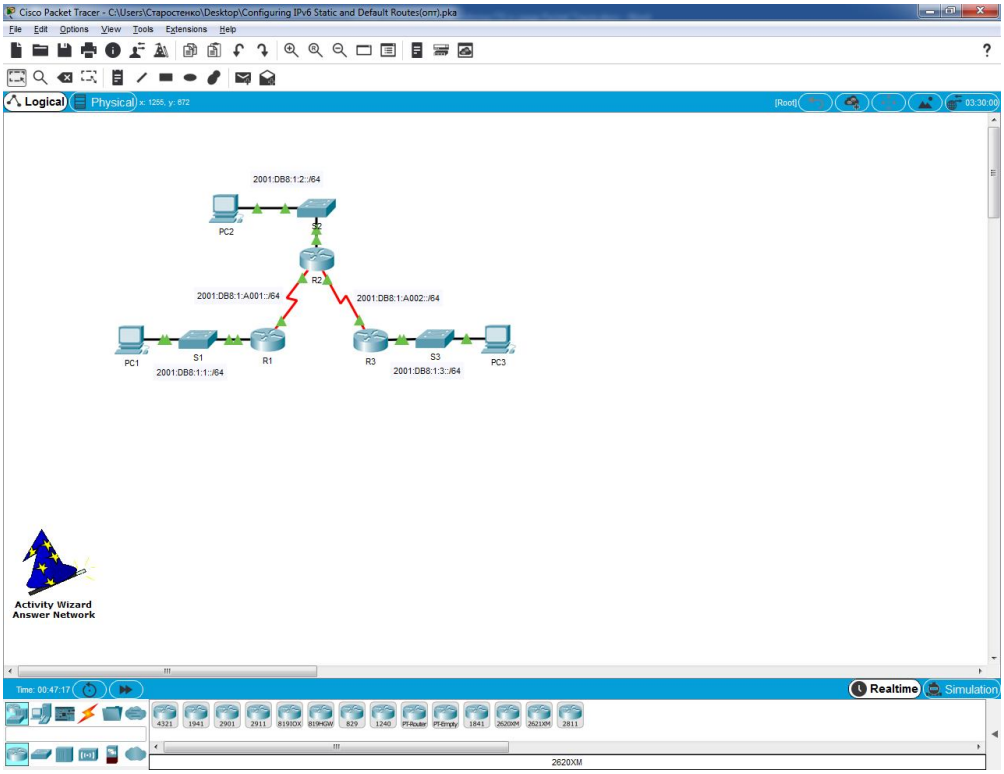


Рис. 3. Answer Network

Кроме создания конечной конфигурации сети в Answer Network определяются оцениваемые элементы на вкладке Assessment Items (рис. 4).

Это могут быть команды конфигурации IOS, назначенные IP адреса, состояние интерфейсов, наличие соединений между устройствами, положение устройств в пространстве. В демонстрируемом примере оценивается более 80 различных параметров: корректность создания физической топологии сети, настройка IPv6-адресации компьютеров и портов маршрутизаторов, статических маршрутов.

Еще одним методом оценки выполненного задания является тестирование соединений, которое создается в Answer Network на вкладке Connectivity Testing. Тестирование соединений позволяет оценивать задание на основе сетевых функций и производительности, а не на основе сопоставления статических параметров конфигурации. Поддерживаемые типы тестирования соединений – это типы созданных пользователем PDU (Protocol Data Unit – обобщённое название фрагмента данных на разных уровнях модели OSI), которые содержатся в первом сценарии сети ответа. Для каждого PDU можно установить условие теста на «Не тестировать», «Успешно» или «Сбой».

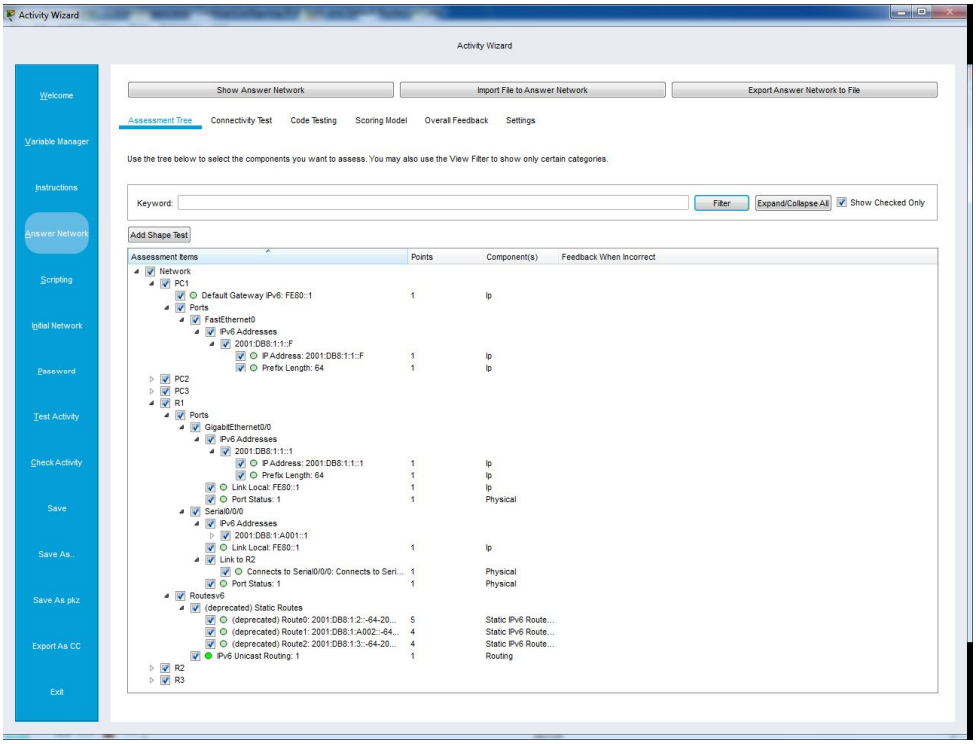


Рис. 4. Настройка оцениваемых элементов

На вкладке Settings в Answer Network разработчик устанавливает дополнительные параметры (рис. 5). Например, Time Settings предполагает установку контроля времени, прошедшего с момента начала выполнения задания. Также возможно внести ограничения по времени с помощью параметра «Countdown».

В Feedback Settings устанавливаются параметры, позволяющие каждые несколько секунд сравнивать настройки сети обучающегося с настройками, установленными в Assessment Items. Для Feedback Settings доступны следующие параметры: нет обратной связи, результат демонстрируется в виде количества баллов, результат демонстрируется в процентах, результат демонстрируется в виде количества баллов и процентах.

Для того, чтобы обучающиеся не изменяли свой профиль во время выполнения задания, рекомендуется включить блокировку профилей пользователей. Если при выполнении задания предпринимается попытка изменить профиль, появится диалоговое окно, предупреждающее о том, что действие будет сброшено.

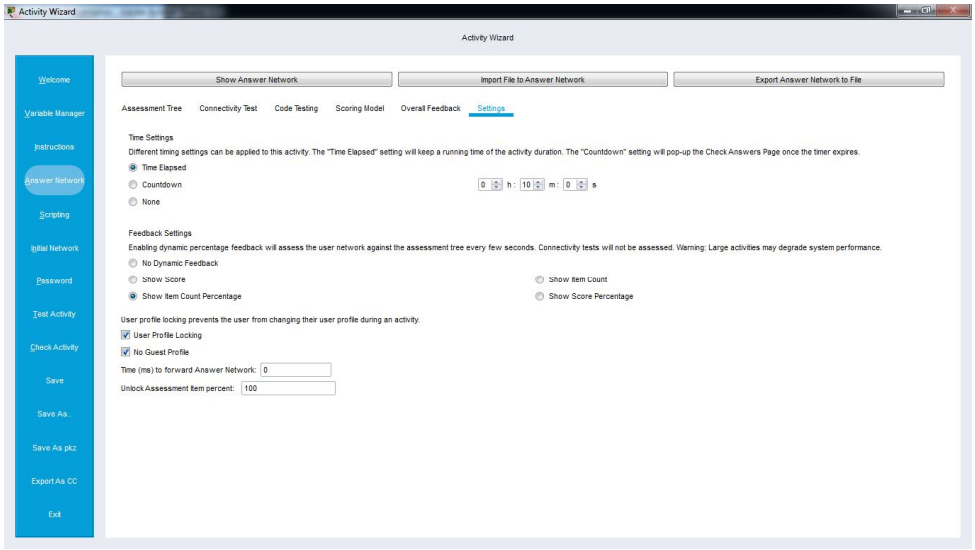


Рис. 5. Вкладка Settings раздела Answer Network

Описательная часть задания создается в разделе Instructions. Описательная часть содержит инструкции для задания, которые создаются с помощью HTML-тегов и выводится в отдельном окне PT Activity (рис. 6).

HTML-теги рекомендуется создавать и редактировать вне AW, с последующим их копированием или импортом в структуру основного файла.

На заключительном этапе разработки задания в разделе Password необходимо указать пароль для доступа к AW, чтобы исключить возможность несанкционированного внесения изменений и сохранить проект. Файл будет сохранен как Packet Tracer Activity (расширение pka).

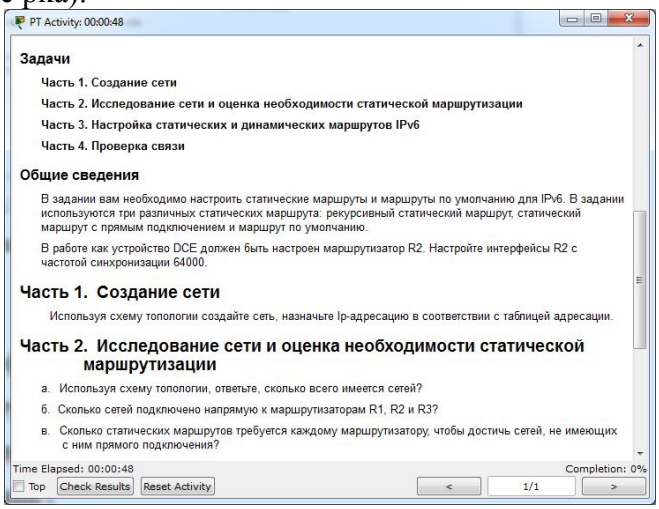


Рис. 6. Окно PT Activity

При создании задания в меню AW разработчику доступны полезные опции Test Activity и Check Activity. Если Test Activity позволяет разработчику выполнить пробный запуск задания, то с помощью Check Activity тестируется готовое задания без перезапуска файла. Это дает возможность разработчику, в случае необходимости, вернуться в среду AW и точно настроить действие, прежде чем окончательно сохранить проект.

Литература:

1. Старостенко И.Н. О некоторых аспектах использования симулятора Packet Tracer в образовательном процессе (на примере создания IoT систем). // Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф., 16 июня 2017 г. / редкол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодар. ун-т МВД России, 2017. – С 269 – 275.

2. Лапин В.В., Слесарева Е.А., Старостенко И.Н. Информационные системы в деятельности органов внутренних дел. Учебное пособие. – М.: Московский университет МВД России, 2014.

Стахно Р.Е., Алексеев С.А., Парфенов Н.П.
Санкт-Петербургский университет МВД России

КОМПЛЕКСНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ЧАСТНЫХ И ИНТЕГРАЛЬНОГО ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ПРАКТИЧЕСКОЙ ПОДГОТОВКОЙ

В настоящее время принято эффективность практической подготовки (ПП) рассматривалось в двух аспектах: 1) с позиции объектных (объекты, методы, условия, средства ПП и т.д.) составляющих, 2) с позиции субъектных (требования к показателям эффективности структуры и функционирования элементов системы ТП и анализ определяющих их факторов) составляющих. Методы моделирования организационного управления (ОУ) ПП, применительно к организационной и дидактической подсистемам системы организационного управления (СОУ) ПП, обеспечивают выделение системы единичных показателей эффективности, определяющих эффективность ОУ ПП. Построение моделей организационных и дидактических подсистем является исходным этапом для проектирования СОУ ПП будущих специалистов ОВД. Вместе с тем построение названных моделей является необходимым, но недостаточным условием определения функций ОУ ПП, являющимся отправной точкой для проектирования СОУ ПП. Множества показателей эффективности ПП сами по себе являются лишь индикаторами функционирования системы ПП, которые не определяют ни технологии управляющих воздействий, ни содержания ПП, не являются средством изменения ни качественных, ни количественных характеристик ПП. Определяющим при принятии и реализации управленческих решений руководителем ПП является информация о числовых значениях показателей эффективности и степени их влияния на интегральную эффективность ПП [1–4].

Исходя из сказанного, могут быть выделены этапы комплексного метода определения частных и интегрального показателей эффективности ОУ ПП:

1. Разработка методик и инструментария для получения числовых значений показателей эффективности ПП.

2. Проведение процедур измерения числовых значений показателей эффективности ПП.

3. Проведение агрегирования единичных показателей эффективности ПП в групповые и последних в интегральный.

4. Вычисление числового значения интегрального показателя эффективности ПП.

5. Сравнение полученного значения интегрального показателя с критериальным (эталонным, заданным) значением.

6. Принятие руководителем ПП решения о необходимости управляющего воздействия на некоторый элемент системы ПП с целью изменения его качественных характеристик для устранения рассогласования с критериальным значением показателя.

7. Определение вида и содержания управляющего воздействия на обучающегося (обучающихся) руководителем ПП (сравнение конкурирующих вариантов и выбор наилучшего).

8. Реализация принятого решения с помощью СОУ ПП.

Следует подчеркнуть, что необходимость принятия и реализации с помощью СОУ ПП управляющего воздействия возникает еще в одном случае, когда руководитель ПП на основании анализа эффективности хода ПП прогнозирует (диагностирует) возможность возникновения нежелательного отклонения. Такой вид управления эффективностью ПП может быть отнесен к классу опережающего управления.

Поскольку успешность профессиональной деятельности выпускника учебного заведения является основным показателей эффективности образовательного процесса в целом и одной из его компонент – ПП, в частности, то возникает необходимость спрогнозировать степень этой успешности. Однако практическое осуществление такого прогноза сопряжено с рядом существенных трудностей. В общем виде задача прогноза может быть задана в следующей постановке. Пусть имеются числовые значения (оценки) показателей эффективности ПП $x_{ij}(t)$ на некоторый момент времени t, а также оценки показателей реальной успешности деятельности выпускника ВУЗа МВД $y_i(t+\Delta t)$ на момент $t+\Delta t$, где $i = \overline{1, n}$, n- количество компонент ПП, $j = \overline{1, m}$, m - количество показателей эффективности компонент ПП. Требуется на основании значений x_{ij} сформировать ряд правил, позволяющих с заданной точностью предсказать значение y_i не только для исходной, но и для некоторой расширенной выборки объектов эксплуатации ОВД. Характеристика y_i - это прогнозируемая переменная, а x_{ij} - прогностический признак, Δt - глубина прогноза.

При решении сформулированной задачи прогноза наиболее часто выбирается класс линейных функций вида

$$y_i = \sum_{j=1}^{m} a_j x_{ij} ,$$

где a_i - весовой коэффициент, $\sum_{j=1}^{m} a_j = 1,\ a_j \geq 0$.

В зависимости от величины Δt выделяют диахронный ($\Delta t > 0$) и синхронный ($\Delta t \approx 0$) прогнозы. Последний вид прогноза – это диагностика. Следовательно, различие между задачами прогноза и диагностики успешности деятельности выпускника, прошедшего ПП в учебном заведении, в реальных условиях профессиональной деятельности по эксплуатации объектов ОВД с точки зрения методов восстановления функции F при $y_i=F(x_{ij})$ практически отсутствует, а заключается только в величине Δt.

Отличие же прогностических и диагностических постановок задач заключается в концептуальной основе, в целевых установках их решения. В конечном итоге, всякая диагностика процесса ПП осуществляется, по существу, в целях прогноза. В общем виде решение прогностических задач в системе ПП включает решение одной или более диагностических задач. Прогностическим и диагностическим задачам соответствуют различные типы эмпирической валидности[1], т.е. различные критерии эффективности, отличающие пригодность конкретной задачи оценивания успешности деятельности выпускника по эксплуатации объектов ОВД. Диагностическим задачам соответствует конкурентная валидность. В этом случае успешность профессиональной деятельности выпускника может оцениваться на основе разделения значений измеряемых показателей на диагностически различные группы по результатам экспертного опроса. Прогностическим задачам соответствует предикативная валидность, при которой успешность профессиональной деятельности выпускника может оцениваться на основе синтезированного экспертами решающего правила, использующего опыт зависимости успешности профессиональной деятельности выпускников от характеристик процессов ПП, похожих на оцениваемый.

Педагогическая диагностика, одной из основных функций которой является определение прогнозов дальнейшего развития объектов системы ПП, должна решать на ос-

[1] **Валидность** (validity) - комплексная характеристика методики (теста), включающая сведения об области исследуемых явлений и репрезентативности диагностической процедуры по отношению к ним.

новании числовых значений единичных, групповых и интегральных показателей следующие квалиметрические задачи [4 - 5] :

1) при решении познавательных задач:

− определение уровня выработки умений, навыков и формирование личностных характеристик,

− определение эффективности процесса ПП и его компонент,

− определение целесообразных управляющих педагогических воздействий на обучающегося;

2) при решении преобразовательных задач:

− повышение эффективности процесса ПП,

− повышение эффективности процедур выработки умений, навыков и формирования личностных характеристик.

В зависимости от решаемых задач в рамках квалиметрии ПП можно выделить группы методов педагогической диагностики:

1. Методы сбора диагностической информации (значений показателей эффективности объектов и субъектов процесса ПП):

− наблюдение за ходом мероприятий ПП,

− опрос (устный – беседа, интервью и письменный – анкетирование, тестирование) руководителя ПП и обучающихся,

−анализ результатов моделирования функционирования организационной и дидактической подсистем СОУ ПП,

− педагогический эксперимент.

2. Методы обработки и анализа диагностической информации:

− шкалирование, т.е. приемы трансформации качественных характеристик объектов ПП в некоторые числовые значения,

− статистические (многомерной группировки, корреляционного и регрессионного анализа).

3. Методы представления и накопления результатов диагностики:

− фиксация уровней сформированности умений и навыков, достигнутые в ходе ПП,

− фиксация уровня личностного развития обучающихся,

− данные об уровне профессиональной подготовки обучающихся в точках контроля,

− накопление данных об эффективности функционирования элементов СОУ ПП.

4. Методы использования результатов диагностики:

− непосредственное педагогическое управляющее воздействие,

− опосредованное педагогическое воздействие,

− координация и планирование хода ПП,

− прогнозирование развития системы ПП.

Измерение эффективности объектов системы ПП предусматривает процедуру, при которой показатель эффективности объекта системы ПП сравнивается с некоторым эталоном и получает числовое значение в определенном масштабе или шкале. Для того, чтобы определить правила, в соответствии с которыми приписываются числа качественным признакам (свойствам) объектов системы ПП, необходимо определить их структуру и процесс функционирования, т.е. построить модели ОУ для объектов организационной и дидактической подсистем СОУ ПП.

Вопрос измерения эффективности процесса ПП тесно связан с другими вопросами, вытекающими из сущности категории эффективности:

1. Характеристики эффективности процесса ПП, как правило, изменяются в ходе взаимодействия объектов системы ПП. Динамика эффективности процесса ПП приводит к динамике его отдельных характеристик. Следовательно, применительно к проце-

дуре измерений показателей эффективности объектов системы ПП возникает необходимость проведения не единичных, а множественных измерений (мониторинга) одной и той же характеристики.

2. Эффективность процесса ПП рассматривается как иерархическая организация совокупности характеристик (свойств) составляющих его компонент, т.е. эффективность – это многоуровневая система. Применительно к задачам измерения показателей эффективности объектов системы ПП это означает, что если невозможно непосредственно измерить значение сложного показателя *i-го* уровня, то возможна его декомпозиция на более простые *(i - 1)-го* уровня, которые могут быть непосредственно измерены.

3. Эффективность объектов системы ПП всегда имеет определенную ценность для руководителя ПП и обучающихся. Эта ценность должна определяться количественно, но даже при полной невозможности количественного оценивания проявления какого-либо свойства конкретного объекта системы ПП, всегда можно провести его измерение по шкале двухуровневого типа «пригодно» - «непригодно».

4. Эффективность обладает как внутренней обусловленностью, формирующей его потенциальный характер, так и внешней, которая формирует его реальный характер в ходе процесса ПП. Для процедуры измерения показателя эффективности объекта системы ПП это означает, во-первых, установление типа и величины шкалы (границ измерений), во-вторых, позволяет измерить и оценить эффективность процесса ПП как меру соответствия потенциальной и реальной эффективности.

Измерение эффективности процесса ПП связано с развертыванием функции измерения в виде системы взаимосвязанных действий – на рисунке 1 в виде обобщенной схемы представлена методика определения числовых значений показателей эффективности объектов системы ПП.

Формулировка цели данного процесса должна отражать целевую функцию определения числовых значений показателей при ОУ процессом ПП. Цель определяет объект измерения, субъект измерения, отношение объекта и субъекта измерения.

В ходе выполнения классификационных действий определяются классы измерения их единичных свойств, подлежащих измерению, выявляются внешние индикаторы показателей эффективности проявления единичных свойств, определяется перечень методов «свертки» единичных свойств в групповые, групповых в интегральные и, наконец, дается классификация приемлемых измерительных шкал.

С использованием результатов классификации должны быть определены (выбраны) методы декомпозиции показателей эффективности (совокупности свойств) объектов процесса ПП и СОУ ПП. Применение этих методов должно обеспечить выделение групповых, а затем единичных свойств, которыми обладают реальные объекты процесса ПП и СОУ ПП. Информация о выделенных единичных, групповых и интегральных свойствах названных объектов должна быть преобразована в форму, удобную для дальнейшего анализа и интерпретации, для чего должны быть использованы соответствующие методы ее формализации.

Рис. 1. Обобщенная схема методики определения числовых значений показателей эффективности объектов системы практической подготовки

По определенному перечню единичных, групповых и интегральных свойств объектов процесса ПП и СОУ ПП необходимо, во-первых, осуществить выбор методик для формирования перечня показателей эффективности, покрывающих названные свойства. Во-вторых, сформировать перечень эталонов, удовлетворяющих требованиям надежности (определять только признаки свойств, планируемых к измерению, не рассматривая другие), точности (хорошая различимость степени выраженности признака измеряемого свойства), устойчивости (результаты повторных измерений должны совпадать с предыдущими). В-третьих, должно быть выполнено приведение показателей и эталонов к стандартному типу (нормирование). В-четвертых, должен быть осуществлен выбор типов шкал измерений с учетом особенностей каждого оцениваемого свойства.

На основании разработанной классификации, определенных методик декомпозиции эффективности и формирования совокупности показателей эффективности объектов процесса ПП и СОУ ПП должна быть построена методика определения числовых значений показателей эффективности объектов системы ПП.

Выбор методик и средств измерения играет важную роль, когда речь идет об оценивании и ОУ таким сложным объектом как эффективность системы (процесса ПП и СОУ ПП) ПП. При этом следует учитывать тот факт, что полная формализация показателей эффективности и процесса ПП вряд ли возможна из-за того, что в системе ПП есть две компоненты, реализующие интеллектуальную образовательную деятельность – это руководитель ПП и обучающийся. Вместе с тем следует признать тот факт, что самые сложные образовательные объекты и процессы могут быть квантифицированы и измерены в определенной шкале. Методы и средства измерений при ОУ ПП должны быть гомоморфными объекту измерений, т.е. определенным отношениям свойств измерительного эталона должны соответствовать такие же отношения свойств в измеряемом объекте.

Вывод: При оценивании эффективности ОУ ПП необходимо разработать методики агрегирования («свертки») частных (единичных и групповых) показателей в некоторые обобщенные (интегральные) показатели эффективности процесса ПП и СОУ ПП. Этот факт обусловлен, с одной стороны невозможностью получения оценок обобщенных показателей со сложной структурой непосредственным путем, а только путем оценивания составляющих их частных показателей, с другой стороны, - различным весом отдельных показателей в общей структуре оценивания эффективности ПП.

Литература:

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Основы квалиметрии, автоматизации и интеллектуализации систем организационного управления практической подготовкой в вузах МВД. / Наука, техника и образование. № 5 (35) Москва. изд. «Проблемы науки». 2017. С. 29-32.

2. Алексеев С.А., Стахно Р.Е. Вопросы организационного управления содержанием практической подготовки в вузах МВД. / Проблемы современной науки и образования № 19 (101). Москва. изд. «Проблемы науки». 2017.С. 19-22.

3. Алексеев С.А., Алексеева Е.К. Задача агрегирования частных показателей качества объектов в интегральный показатель качества системы тренажерной подготовки специалистов по судовождению / Журнал университета водных коммуникаций. № 3. – СПб.: ГУ МРФ им. адм. СО Макарова, 2013. – 198 с. С.109 – 115.

4. Барашков П.Н. Интенсификация учебно-воспитательного процесса в ВВУЗЕ: Проблемы управления, эффективности и пути их решения. – Л.: ВКАС им. С.М. Буденного, 1990. – 212 с.

5. Багрецов С.А. Квалиметрия групповой деятельности операторов сложных систем управления: под ред. Б.С. Алешина. – М.: Физматлит, 2006. – 384 с.: ил.

6. Квалиметрия и управление качеством. Инструменты управления качеством: Учеб. пособие / С.В. Пономарев и [др.] - Тамбов: Изд-во ТГТУ, 2005. - 79 с.: ил.

Суятин Б.Д., Евлампиев Н.В.
Кубанский государственный университет
Суятин Д.Б.
Лундский университет (Швеция)
Волков Л.В., Илюхин С.С.
НПП «Исток» им. Шокина

О ПРИМЕНЕНИИ КИРЛИАНОГРАФИИ В ОБРАЗОВАНИИ

Более 1000 серьезных медицинских, спортивных и исследовательских организаций в 63 странах мира работает, применяя метод метод газоразрядной визуализации (ГРВ).

Настало время для реализации новых идей и трансформации научного и общественного мировоззрения. И в решении этих актуальных задач, несомненно, свое веское слово скажет кирлианография. В этой связи 20-22 февраля 2018 года в Кубанском государственном университете прошла 1-ая Международная научно-практическая конференция «На пороге будущих открытий», посвященная 120-ой годовщине со дня рождения заслуженного изобретателя РСФСР С.Д. Кирлиана.

Организаторами конференции были: Кубанский государственный университет, Международный Центр Кирлианографии, Динской историко-краеведческий музей, Краснодарское региональное отделение Русского географического общества, НИИ культурного и природного наследия им. Д.С. Лихачёва, научно-образовательный центр «Цветные стекла» при КубГУ.

В конференции приняло участие более 170 человек. Наряду с Российскими учеными, в конференции приняли участие ученые из Англии, Голландии, Новой Зеландии, Украины (г. Днепропетровск), Донецкой народной республики (г. Донецк). Всего на конференции было заслушано 32 доклада. Кроме того представлено 8 стендовых докладов: из США профессором Марком Кринкером (2 доклада), врачем-исследователем Софией Бланк, профессором Демидовой М.И. из Петербургского госуниверситета, учеными из Калининградского университета Будиловским Г.Н., Фёдоровым А.С. (2 доклада), доцентом из г. Кургана Булатовой Т.Е., учеными-физиками из Краснодара Бурцевым В.А. и Онищук С.А.

Одним из перспективных электрографических методов исследования состояния и энергетики человека является ГРВ [1], основанный на известном эффекте Кирлиана. На основе метода ГРВ группой ученых под руководством профессора К.Г. Короткова (ИТМО, Санкт-Петербург) разработан программно-аппаратный комплекс «ГРВ-Камера». Комплекс прошел клинические испытания, внесен в государственный реестр медицинской техники и сертифицирован Минис-терством Здравоохранения РФ.

На конференции было представлено новейшее оборудование (10 приборов) производства ООО «Биотехпрогресс», а также была проведена презентация современного прибора «КРОУНОСКОП», работающего на основе метода Кирлиан ООО «Биоэнтек» (г. С.-Петербург).

Свечение объектов различной природы в электромагнитных полях высокой напряженности было обнаружено более 200 лет назад и с тех пор постоянно привлекало внимание исследователей [2, 3]. Большой вклад в развитие этого направления внесли Российские изобретатели супруги Кирлиан [4–6]. Однако только с созданием программно-аппаратных комплексов газоразрядной визуализации (ГРВ) в 1995 году исследование этих свечений получило статус научного направления. С тех пор были детально исследованы физические механизмы формирования свечений [7], налажено серийное производство приборов, созданы комплексы программ для приложений в медицине, биологии, исследовании материалов [8]. Было показано, что характеристики свечения поверхности кожного покрова чело-века зависят, в первую очередь, от активности вегетативной нервной системы с учетом системы адаптационных уровней [9].

В данной работе проведён анализ некоторых основополагающих докладов, касающихся, прежде всего, образовательного процесса, которые позволяют оценить возможности применения метода ГРВ в образовательной области.

Константин Георгиевич Коротков – д.т.н., профессор (г. С.-Петербург).

За последние годы метод ГРВ показал свою эффективность в ранней диагностике заболеваний, оценке тяжести их течения, эффективности лекарственной терапии, в спортивной медицине, а также в психотера-певтической практике. Проведенный анализ литературы показывает, что изменения ГРВ изображений тождественны изменениям в организме пациентов, верифицированным на основе клинической картины, данных ин-

струментальных и лабораторных методов диагностики, что свидетельствует о клинической информативности метода ГРВ, а также о перспективах использования этой методики в медицине. Диагностические возможности метода подтверждаются построенными на его основе решающими правилами и созданными автоматизи-рованными диагностическими системами. Такие преимущества ГРВ-биоэлектрографии как простота исполнения, неинвазивность, оперативность получения результатов, основанная на современных бурно развивающихся компьютерных технологиях, несомненно, должны привлечь исследователей в области биологии и медицины для решения многих проблем диагностики и мониторинга, при изучении механизмов действия лекарственных препаратов и методов лечения. Особенно перспективным представляется применение метода ГРВ в клинической практике и в образовательном процессе.

Метод ГРВ получает всё более широкое признание и наряду с другими биоэлектрографическими методами, используется в медицине, спорте, психологии и психофизиологии, а в последнее время и в образова-тельном процессе. Анализ результатов развития творческого наследия супругов Кирлиан, полученных за 40 лет, прошедших с конференции в Краснодаре в 1978 году посвященной 80-летию С.Д. Кирлиан, показывает, что направление эффекта Кирлиан активно развивается в мире. Произошел переход на новый класс компьютеризированных приборов, использующих последние достижения технологии и программного обеспечения, получен большой объем научных данных в медицине, психологии, исследовании сознания, воды и многих других областях. Одним словом – наследие супругов Кирлиан активно развивается в мире, интерес постоянно растет, тысячи специалистов используют эту технологию, и мы не сомневаемся, что нас ожидает еще множество волнующих открытий.

Марина Леонидовна Скуратовская – д.п.н., профессор (г. Ростов-на-Дону). Одной из важнейших задач профессиональной деятельности педагога-дефектолога является психолого-педагогическое изучение особенностей психофизического развития и образовательных возможностей лиц с ограниченными возможностями здоровья (далее с ОВЗ). В ходе обучения студенты должны овладеть способностью организовывать и осуществлять психолого-педагогическое обследование лиц с ОВЗ с целью уточнения структуры нарушения для выбора индивидуальной образовательной траектории, а также, осуществлять динамическое наблюдение за ходом коррекционно-развивающего воздействия с целью оценки его эффективности. Одним из современных методов, позволяющих решить эти задачи, является ГРВ-графия. Быстрота диагностики, высокая достоверность и информативность её результатов, характерные для метода ГРВ-графии, делают его очень перспективным в организации диагностики и мониторинга коррекционно-педагогической деятельности.

Тамара Евгеньевна Булатова – к.б.н., доцент (г. Курган).

Внедрение федеральных государственных образовательных стандартов второго поколения в системе образования требуют и соответствующего современного инструментария для полноценного мониторинга эффективности проводимых реформ. Системно-деятельностный подход, лежащий в основе разработки стандартов нового поколения, позволяет выделить основные результаты обучения и воспитания и создать навигацию проектирования универсальных учебных действий, которыми должны владеть обучающиеся. Важным направлением является формирование культуры здорового и безопасного образа жизни у детей.

Мониторинг психофизиологического состояния с использованием метода газоразрядной визуализации, совместный с детьми анализ полученных результатов включает их в деятельностный подход – освоение инструкции по правильному использованию своего организма. Метод ГРВ-графии позволяет дополнить систему условий, на которые опираются обучающиеся при формировании культуры здоровья по основным ви-

дам универсальных учебных действий: личностные (самоопределение – моё здоровье, смыслообразование – для чего мне нужно быть здоровым и действие нравственно-этического оценивания), регулятивные (целеобразование - быть здоровым (красивое, ровное свечение), планирование – вести здоровый образ жизни, контроль – всё ли выполняю правильно, коррекция – скорректировать отклонения, самооценка психофизического состояния, прогнозирование – надёжность моего организма), познавательные (общеучебные – новые знания, логические и знаково-символические) и коммуникативные - толерантность.

Проведение мониторинга психофизического здоровья обучающихся, учителей, родителей методом ГРВ-графии позволяет оценить их психофизическое состояние, разработать критерии оценки здоровьесберегающей деятельности в школе и в семье и как следствие создать обоснованный личностно-ориентированный подход к улучшению самочувствия каждого ребенка в рамках тесного сотрудничества ребёнка, семьи, школы и поликлиники [10 -16].

Сергей Георгиевич Джура – к.т.н., доцент (г.Донецк, ДНР).

В последние десятилетия дистанционное обучение получило широкое распространение, и его популярность неуклонно возрастает в связи с тем, что оно позволяет получить образование всем категориям населения – от людей с ограниченными возможностями до специалистов, желающих получить второе высшее образование. Помимо этого, дистанционное обучение помогает решить многие задачи, поставленные государством перед системой образования Украины, а именно: обеспечить реализацию принципа «образование в течение всей жизни», расширить возможности инклюзивного образования, решить задачу переподготовки кадров и т.д.

Однако дистанционное обучение, как и любая другая форма обучения, имеет ряд проблем, требующих своего решения, среди которых недостаточный непосредственный контакт преподавателя со студентами имеет наиболее важное значение в аспекте исследуемой проблемы. Существующим дистанционным системам обучения недостает возможности контроля со стороны преподавателя процесса понимания материала в ходе изложения нового материала. Насколько ученик или студент понял излагаемый материал, выясняется в результате тестирования в конце того или иного блока.

Эту проблему можно решить с помощью внедрения в процесс дистанционного обучения камеры газоразрядной визуализации (ГРВ-камеры), которая фиксирует реакцию обучаемого на восприятие изучаемого материала, что позволяет корректировать деятельность преподавателя, опираясь на полученные им данные.

Людмила Анатольевна Песоцкая - д.м.н., доцент (г. Днепропетровск, Украина).

Задачей образования является раскрытие природного потенциала учащегося. Для этого необходимо изучение типа мышления у них, психоэмоциональных особенностей. Используемые методы определения типа мышления и его степени развития основаны преимущественно на результатах различных психологических тестов (с использованием рисунка, числовых рядов, толкования пословиц, опросника Г.В. Резапкиной и др.). Однако, индивидуальные психоэмоциональные реакции организма в данный момент времени могут влиять на процессы мышления.

Заслуживают внимания методики оценки энергетического состояния организма в момент тестирования, которые фиксируют как кратковременные вегетативные реакции, так и стойкие рефлекторные изменения энергетического метаболизма в организме в целом. Сегодня достаточно широко в мире применяются методы, основанные на газоразрядной визуализации свечения терминальных точек пальцев рук и ног человека на фотоматериале, что известно, как эффект Кирлиан или кирлианография.

Ранее было установлено, что изображения газоразрядного свечения (ГРС) пальцев человека, основанные на эффекте Кирлиан содержат ряд информационных признаков,

которые коррелируют с его психологическим состоянием. Известны возможности кирлианографии пальцев рук на цветном фотоматериале для оценки психоэмоциональной активности и природных способностей человека.

Целью работы было выявить особенности газоразрядного свечения пальцев рук у студентов университета младших и старших курсов с различным типом мышления по результатам психологических тестов.

Обследовали студентов младших и старших курсов обучения в университете. У учащихся на основе психологических тестов были определены типы мышления: образное, логическое, интуитивное. Полученные результаты сопоставили с результатами анализа короны газоразрядного свечения вокруг пальцев рук обследуемых лиц на кирлиан-фотографиях после проведения каждого теста. Использовали экспериментальный прибор «РЕК 1», рентгеновскую и цветную пленку «Паляроид». Выявили различия в кирлиановских изображениях пальцев у студентов младших и старших курсов, при разных типах мышления. Наблюдали активацию разных реактивных систем организма в соответствии с возрастными физиологическими особенностями и длительностью обучения. Психоэмоциональную активность оценивали по соотношению компонентов цвета кирлиановского свечения пальцев на цветной фотопленке по данным компьютерной обработки полученных изображений.

Преимущество кирлианграфии, как биоэнергоинформационного, инновационного метода состоит в высокой чувствительности и возможности регистрации неспецифических изменений в организме на уровне предболезни при негативном влиянии на него факторов окружающей среды, выявлении уже начальных нарушений в системе компенсаторных реакций адаптации к ним. То есть, полученные результаты могут иметь прогностическое значение для своевременного проведения как экологических, так и оздоровительных мероприятий.

Рассмотрено несколько примеров практического применения кирлианграфии. В качестве критериев интерпретации короны излучений на кирлианограммах использовали диагностичесике карты доктора П. Мандела (1983, ФРГ), собственные наработки (Патенты Украины, методические рекомендации МЗ Украины). Исследования проводились на экспериментальном приборе «РЕК-1», с визуализацией кирлиан-свечения вокруг пальцев рук на рентгеновской пленке в условиях рентген-кабинета.

Обследовали 86 детей в возрасте от 8 до 15 лет из семей ликвидаторов последствий аварии на ЧАЭС или переселенцев с близлежащих территорий Украины (2002 г.) до и после санаторно-курортного лечения в санатории «Энергетик» в г. Ялта. На момент обследования дети были практически здоровы. Однако, на кирлиан-фотографиях у 99% детей были выявлены изменения в короне излучений вокруг пальцев рук, характерные для заболеваний в прошлом (хронические заболевания почек, щитовидной железы, желудочно-кишечного тракта, вегето-сосудистая дистония, воспалительные заболевания верхних дыхательных путей) или еще не проявившиеся клинически.

Метод классической кирлианографии использовали для экспресс-диагностики состояния здоровья работников на промышленных предприятиях во время профосмотров, что позволило разработать критерии оценки степени неблагоприятного воздействия на организм внешней среды, в том числе условий труда. Выявление дефектов в короне излучений превышало фактическое число проявившейся клинически заболеваемости со стороны органов респираторной сферы на 30%, что является резервом ее снижения при своевременном применении оздоровительных методов.

Применение кирлинографии совместно с цитогенетическим тестом биоиндикации экологического загрязнения окружающей среды по исследованию букального эпителия детей дошкольного возраста в разных регионах страны выявило в целом соответствие между ними, но в ряде случаев визуализировало неспецифические признаки формиро-

вания патологии при отсутствии генетических поломок, и наоборот, минимальные дефекты в короне сечения при их наличии, отражая адаптацию к неблагоприятным факторам в регионе.

Обследуя детей и взрослых, находящихся в одном и том же промышленном районе в динамике по годам методом кирлианграфии выявили соответствие изменений в состоянии их здоровья изменениям санитарно-гигиенических характеристик атмосферы и водных источников в районе. Исследования свечения разных проб воды позволили выявить критерии ее качества и предложить полезную модель оценки ее энергетического состояния.

Таким образом, применение метода кирлианографии может оптимизировать решение задач, связанных с экологической безопасностью человека в условиях растущего неблагополучия окружающей среды и производства, проводить массовую донозологическую диагностику населения с формированием государственной программы оздоровления населения, прежде всего детского, и проживающего или работающего в экологически загрязненных условиях.

Николай Константинович Игнатьев – к.б.н., директор научно-медицинского центра «Лимфосанация» (г. Новосибирск, Россия).

Разработаны и успешно применяются модификация метода Кирлиано-графии – метод Электробио-люминесцентного (ЭБЛ) исследования и диаг-ностический прибор «Кирлиан-биоэлектрограф». Согласно разработанному способу диагностики все изменения свечения пальцев рук и ног оцениваются по десятибальной шкале, что позволяет не только выявить нарушение, но и оценить степень и характер отклонений. Метод ЭБЛ-исследование позволяет оценить состояние 20 органов и систем, психоэмоциональное и энергетическое состояния, выявить и оценить степень эндотоксикоза. Доказанная чув-твительность обследования при медицинских испытаниях прибора составляла 85–90 %. Диагностический прибор «Кирлиан-биоэлектрограф» рекомендован Минздравом РФ для применения в медицинской практике для экспресс-диагностики функционального состояния организма.

Кирилл Борисович Марголин – директор ООО «Биоэнтек».

Стратегия здравоохранения будущего неразрывно связана с совершенствованием технологий для оценки состояния физического и психического здоровья человека, а также методов его коррекции. Важнейшую роль играет развитие методик, связанных с прогностическими аспектами технологий, способных оценить состояние здоровья на донозологическом уровне.

Одной из подобных перспективных технологий, обладающей высоким прогностическим потенциалом и привлекательностью, является метод кроуоноскопии. Кроуноскопия относится к семейству электрографических методов, анализирующих свойства объектов, с помощью использования коронных разрядов, формирующихся вокруг них в электромагнитном поле высокой напряженности.

Метод кроуноскопии – это сформировавшийся динамический подход к исследованию короноразрядных изображений объектов. Он является результатом развития методик по наблюдению и анализу феномена свечения объектов в электромагнитном поле высокой напряженности («эффекта Кирлиан», и в частности, компьютерного аналога ГРВ) от статических изображений к их динамическим характеристикам. Другими словами, это компьютерная визуализация и анализ динамики изменения «эффекта Кирлиан» исследуемых объектов.

Кроуноскопия – это метод исследования и коррекции энергетического, физиологического и психоэмоционального состояния человека. Кроуноскопия проводится с помощью прибора – кроуноскопа и специально разработанного пакета программ. Суть метода состоит в том, что с помощью кроуноскопа человек включается в контур

биообратной связи через компьютер. При этом на экран монитора выводится текущее коронное изображение (кроунграмма), отражающее его психофизиологическое состояние. Используя навыки саморегуляции, пациент учится управлять этим сигналом в нужном направлении. Другими словами, человек учится за компьютером самостоятельно приводить себя в состояние устойчивого спокойного бодрствования и комфорта, а затем переносит эту способность в реальную повседневную жизнь.

Способ исследования объектов методом кроуноскопии – принципиально динамический, основанный на анализе изменения коронного разряда объектов во времени в электромагнитном поле высокой напряженности.

Программно-аппаратный комплекс «Кроуноскоп» – это система, позволяющая визуализировать динамическое распределение энергетических потоков в пространстве, и, в частности, энергетическое поле человека, а также корректировать его на основе биообратной связи.

Таким образом, краткий обзор докладов, представленных на конференции, позволяет сделать вывод о возможности применения кирлиа – нографии в образовательном процессе. Особый интерес вызывают исследования доцента Т.Е. Булатовой из г. Кургана.

Проведение мониторинга психофизического здоровья обучающихся, учителей, родителей методом ГРВ-графии, позволяет оценить их психофизическое состояние, разработать критерии оценки здоровьесберегающей деятельности в школе, в семье и, как следствие, создать обоснованный лич-ностно-ориентированный подход к улучшению самочувствия каждого ребенка, семьи, школы и поликлиники.

Литература:

1. Коротков К.Г. Основы ГРВ – биоэлектрографии / СПб., 2001. – 358 с.
2. Коротков К.Г. Эффект Кирлиана. СПб., 1995, 218 с.
3. От эффекта Кирлиан к биоэлектрографии. Под ред. К.Г. Короткова СПб., 1998, 340 с.
4. Ананьева С.В. Эффект Кирлиан - величайшее открытие XX века. Сибирское Рериховское Общество. Издательский центр «Россазия». Новосибирск, 2018. 164 с.
5. Суятин Б.Д., Суятин Д.Б., Илюхин С.С. Кирлианография в образовательном процессе. // Проблемы и перспективы развития образования по физике: общеобразовательные учреждения, педагогические вузы: доклады научно-практической Конференции (г. Москва, 11-12 апреля 2018 г.) / Моск. гос. обл. ун-т, отв. ред. А.А. Синявина. – М.: ИИУ МГОУ, 2018. с. 43-50.
6. Коробова Е.Г. Открытие, опередившее время. Издательский дом, Краснодар, «Magala» - 2017. 102 с.
7. Коротков К.Г. Принципы анализа в ГРВ биоэлектрографии. СПб, Изд-во «Реноме», 2007, 286 с.
8. Петрова Е.Н., Коротков К.Г., и др. Принципы построения и структура автоматизированного программно-аппаратного комплекса оценки состояния здоровья // Изв. Вузов.Приборостроение. 2009. 52,(5). С.16 – 20.
9. Дроздов Д.А., Шацилло О.И. Анализ ГРВ - биоэлектрографических изображений с позиций вегетологии. Труды международной конференции «Наука. Информация. Сознание», СПб, 2005, с. 99-104.
10.Булатова Т.Е. Метод газоразрядной визуализации в оценке психофизического состояния гимназистов / Т.Е. Булатова, Л.И. Иванова // Инновационные процессы в образовании: Сб. научн. статей / Институт повышения квалификации и переподготовки работников образования Курганской области. – Курган, 2006. – с. 83 – 87.
11. Булатова Т.Е. Мониторинг психофизического состояния обучающихся с использованием метода ГРВ / Т.Е. Булатова, Т.В. Попова, М.Н. Тарасова, Л.И. Иванова // Наука. Информация. Сознание. Тезисы Международного научного конгресса по ГРВ

биоэлектрографии. - С.-Петербург, 2007. С. 35 – 37.

12. Булатова Т.Е. Оценка эффективности физических упражнений методом ГРВ / Т.Е. Булатова, Ю.В. Котов // Инновационные процессы в физическом воспитании: Мат. межрегион. пед. чтений (18 апреля 2007 г.) / Институт повышения квалификации и переподготовки работников образования Курганской области – Курган, 2007. – с. 410 – 411.

13. Булатова Т.Е. Оценка эффективности психофизической саморегуляции в сохранении здоровья учащихся / Т.Е. Булатова // XX съезд Физиологического общества им. И.П. Павлова. Тезисы докладов. – М.: Издательский дом «Русский врач», 2007. - с. 164.

14. Булатова Т.Е. Формирование ценности здорового образа Жизни для здоровья на основе ГРВ / Т.Е. Булатова. – Сб. материалов Всероссийской научно-практической крнференции «Здо-ровьесберегающие технологии в образовании». Новосибирск: Изд-во НИПК и ПРО, 2010. С. 29 – 31.

15. Булатова Т.Е. Мониторинг адаптации психофизиологических функций у детей к учебным нагрузкам / Т.Е. Булатова // Тезисы докладов 21 съезда физиологического общества им. И.П. Павлова. - М.-Калуга. 19 – 25 сентября. – Калуга: Бест-принт, 2010. с. 88.

16. Булатова Т.Е. Динамика показателей ГРВ-графии обучающихся в Курганской облаcи с 1 по 11 классы / Т.Е. Булатова // Наука. Информация. Сознание. Тезисы Международного научного конгресса по ГРВ биоэлектрографии. С.-Петербург, 2011 г.

Тарасенко А.В., Макоха А.Н.
Северо-Кавказский Федеральний университет

КОМПЬЮТЕРНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ ПОИСКА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ДЕРЕВЬЕВ И ИХ АНАЛИЗ

Поиск – одна из важнейших процедур обработки структурированной информации, она заключается в получении конкретного фрагмента или фрагментов информации из больших объемов ранее сохраненных данных.

Изучение алгоритмов поиска ведется уже давно и не теряет своей актуальности, ведь количество данных, требующих обработки, постоянно возрастает, возникают новые типы данных и новые проблемы, связанные с увеличением разнообразия платформ, общей глобализацией и интеграцией информационной среды человечества.

Для организации поиска в основной памяти особое значение имеет рассматриваемый в данной работе метод поиска, основанный на алгоритмах с использованием деревьев – это динамический метод, эффективный для быстрого доступа к ключу в таблице с упорядоченными данными и поддерживающий оперативное изменение структуры, в которой хранятся данные.

Анализ компьютерной реализации алгоритмов поиска позволяет представить результаты выполнения операций над деревьями в условиях, далеких от идеальных. Это может помочь с выбором оптимального алгоритма тем, кто будет искать оптимальную структуру для организации данных в своей системе, дополнив существующие теоретические выкладки. Благодаря проведенному изучению распределения времени, затрачиваемого на выполнение основных операций над данными, можно установить преимущества алгоритмов на практике для конкретных задач. Целью исследования было проанализировать распределение времени выполнения основных операций, реализуемых в рамках алгоритмов поиска информации с использованием деревьев, в зависимости от объема данных, и сравнить полученные результаты с прогнозируемыми при теоретическом изучении.

Для реализации и анализа были выбраны два алгоритма с древовидными структурами: бинарное дерево поиска и красно-черное дерево.

Бинарное (двоичное) дерево поиска – это двоичное дерево, для каждого узла которого выполняются два условия:

1) Потомками узла является не более 2 узлов, каждый из которых формирует двоичное поддерево.

2) Все узлы правого поддерева больше или равны ключу самого узла.

Для полного бинарного дерева (т.е. такого дерева, каждый узел которого кроме внешних узлов, имеет по два потомка) с n узлами эти операции выполняются, как заключил Д. Кнут, при работе с хорошо сбалансированным деревом примерно пропорционально $\Theta(\log(n))$, однако в случае вырожденного дерева время выполнения операций становится пропорциональным $\Theta(n)$. Среднее время поиска пропорционально $\Theta(\sqrt{n})$ [1]. Последнее значение должно давать примерную зависимость времени выполнения операций поиска, вставки и удаления от количества элементов в случайно сгенерированном бинарном дереве поиска без балансировки, если дерево не является вырожденным. На практике гарантировать полноту дерева при случайной вставке нельзя, а значит реальное затрачиваемое время окажется гораздо больше, в худшем случае длина пути поиска будет равна высоте дерева. Преимущество древовидной структуры будет потеряно. Существующие модификации деревьев, которые призваны гарантировать хорошее время выполнения основных операций в худшем случае, за счет балансировки и динамической реструктуризации дерева в процессе изменения его состава.

Основной подход к повышению степени сбалансированности в двоичных деревьях связан с периодическим явным выполнением их повторной балансировки [2].

Красно-чёрное дерево является особым видом двоичного дерева, используемым в информатике для организации сравнимых данных, таких как фрагменты текста или числа. Оно представляет собой одну из множества приближенно сбалансированных схем деревьев поиска. Реализация красно-черных деревьев предполагает для каждого узла поддержку следующих атрибутов: ключ, значение и цвет узла.

Красно-черные деревья обладают следующими свойствами:

1) Каждый узел окрашен либо в красный, либо в черный цвет.

2) Корень дерева является черным узлом.

3) Листья окрашены в черный цвет.

4) Если узел красный, то оба его потомка – черные. Нужно отметить, что у черного узла могут быть черные дочерние узлы, у красных - только черные.

5) Пути от узла к его листьям содержат одинаковое количество черных узлов (это черная высота).

Все эти свойства должны учитываться при вставке нового элемента и позволяют гарантировать время выполнения операций в таком дереве $\Theta(\lg(n))$ даже в худшем случае. Хотя вставка и удаление усложняются за счет перекрашивания вершин, их сложность остается близкой к логарифмической [1].

Выбор именно этих двух алгоритмов позволил:

3) использовать единообразно организованную функцию, реализующую операцию поиска в обоих деревьях;

4) оценить преимущества и недостатки поддержания баланса в дереве;

5) оценить эффективность дерева, имеющего сложный узел с дополнительным свойством;

Для выполнения компьютерной реализации рассматриваемых алгоритмов использована платформа .Net Framework и объектно-ориентированный язык программирова-

ния C#. Интерфейс построен с помощью технологии WPF, использующей аппаратное ускорение через DirectX, что снижает нагруженность процессора. В качестве структуры для хранения данных и осуществления свойств деревьев выбрана структура «двоичная куча». Это бинарное дерево, элементы которого представляют собой элементы массива, индексы которого определяют положение узла в дереве. Плюсом такой реализации является отсутствие необходимости хранить ссылки на левого и правого потомка в каждом узле, что экономит память [3]. При этом на основе кучи как структуры хранения может быть реализован любой из модифицированных алгоритмов двоичного дерева поиска. Наглядное сравнение того, как будут храниться данные при реализации массивом, представлено на рисунке 1.

Индекс	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Значение	32	17	18	16	9	12	7	10	3	3	7	2	5	1	2	4

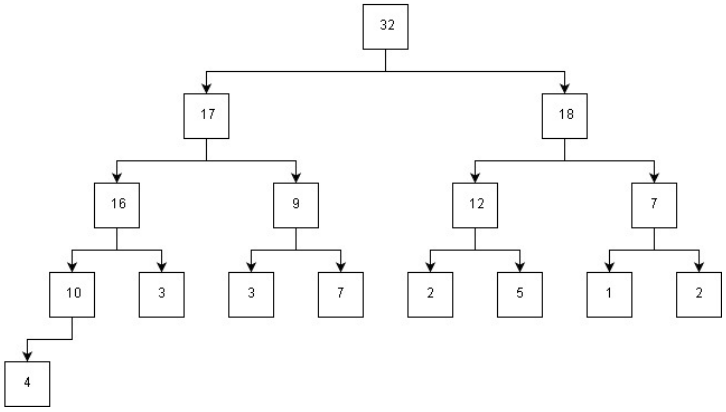


Рис. 1. Двоичная куча в виде массива и в виде дерева

Для быстрого поиска требуется предварительная подготовка – дерево, хранящее данные, надо построить специальным образом. Поэтому помимо поиска при работе с деревом имеют большое значение и другие операции: добавление в дерево, а также удаление из дерева узла. Именно эти три операции: поиск, вставка нового элемента и удаление элемента из дерева были выбраны для проведения анализа реализации алгоритмов. За основу брались соответствующие алгоритмы, представленные Т.Х. Корменом, адаптированные под выбранную структуру данных и язык программирования [4].

Для успешного выполнения анализа алгоритмов программа должна поддерживать:

1) Возможность выбора типа дерева для работы, каждый тип организован в виде отдельного класса.

2) Команды для основных операций над деревом: поиск, вставка, удаление элемента (причем вставка и поиск выполняются по значению элемента, а удаление – по индексу).

3) Поле для введения значения/индекса элемента, над которым будет проводиться операция.

4) Возможность генерировать некоторую случайную совокупность однотипных сравнимых данных с последующим формированием из них дерева заданного типа;

5) Поле, в которое выводится индекс узла – результат поиска.

6) Возможность оценить затраты времени на проведение операции – поле, в которое выводится время, затраченное на выполнение операции.

7) Опционально для проверки корректности выполнения возможна реализация вывода дерева.

Анализ проводился при помощи генерации деревьев с заданным числом элементов. Для каждой операции над каждым деревом проводилось пять попыток выполнения этой операции. Далее строился анализируемый график.

В таблице 1 приведены средние значения времени выполнения операций поиска, вставки и удаления, выполненные для случайно сгенерированных деревьев заданной размерности.

Таблица 1.

Время выполнения операций в бинарном дереве поиска (в $c \cdot 10^9$)

Кол-во элем. / Вид операции	4000	35000	460000	700000	1300000
Поиск	30280	30660	34060	34640	38420
Вставка	2180	2620	2380	2780	2920
Удаление	1800	2340	2800	2740	2900

По таблице заметно, что наибольшее время затрачивается на операцию поиска, что связанно со случайностью структуры сгенерированного дерева. Для операции вставки наблюдается скачок затрачиваемого времени, что, вероятно, связано с выбранным значением элемента для выполнения вставки, для которого понадобилось больше времени для помещения в дерево. Операция удаления имеет наибольший темп роста среди операций.

В таблице 2 приведены средние значения времени выполнения операций поиска, вставки и удаления, выполненные для случайно сгенерированных деревьев заданной размерности.

Значения размерности деревьев взяты поменьше, потому что рост количества элементов происходит быстрее, алгоритм выполняется медленнее и с большей нагрузкой на систему, величины выбирались с большим разбросом, чтобы позволить оценить соответствие полученного графика предполагаемому.

Таблица 2.

Время выполнения операций в красно-черном дереве (в $c \cdot 10^9$)

Кол-во элем. / Вид операции	1200	10000	200000	800000	2000000
Поиск	26520	34780	33740	35280	36960
Вставка	3260	3900	3610	4440	5360
Удаление	2600	2520	2340	3480	5340

По таблице заметно, что наибольшее время затрачивается на операцию поиска, что связанно со случайностью структуры сгенерированного дерева. Операции вставки и удаления выполняются со случайным разбросом времени, что связано с тем, как много элементов, для которых нарушены красно-черно свойства, окажется в итоге и, соответственно, как много действий по балансировке придется провести.

Сравнивая результаты, полученные в ходе анализа времени выполнения операции поиска в бинарном дереве (таблица 1) с аналогичными результаты в красно-черном дереве (таблица 2), на рисунке 2 можно заметить, что средние показатели довольно близки и не дают говорить о значительном преимуществе одного алгоритма над другим, однако операция поиска в среднем несколько быстрее выполнялась в красно-черном дереве.

Это связано с тем, что при генерации бинарного дерева поиска не возникло ситуации, когда полученная древовидная структура обладала значительной вырожденностью, то есть не был учтен худший случай по эффективности. По результатам исследования можно отметить, что колебания значений затраченного на поиск времени в рамках одного дерева меньше в случае с красно-черным алгоритмом, что говорит о повышенной стабильности выполнения операции, полученной благодаря поддержанию сбалансированности. График зависимости среднего времени выполнения операций поиска и удаления элементов в бинарном дереве поиска близок к графику вида $a \cdot \sqrt{x}$, что близко к среднему значению, предсказанному Кнутом [1] для несбалансированного дерева, но наблюдается скачок в одном из узлов.

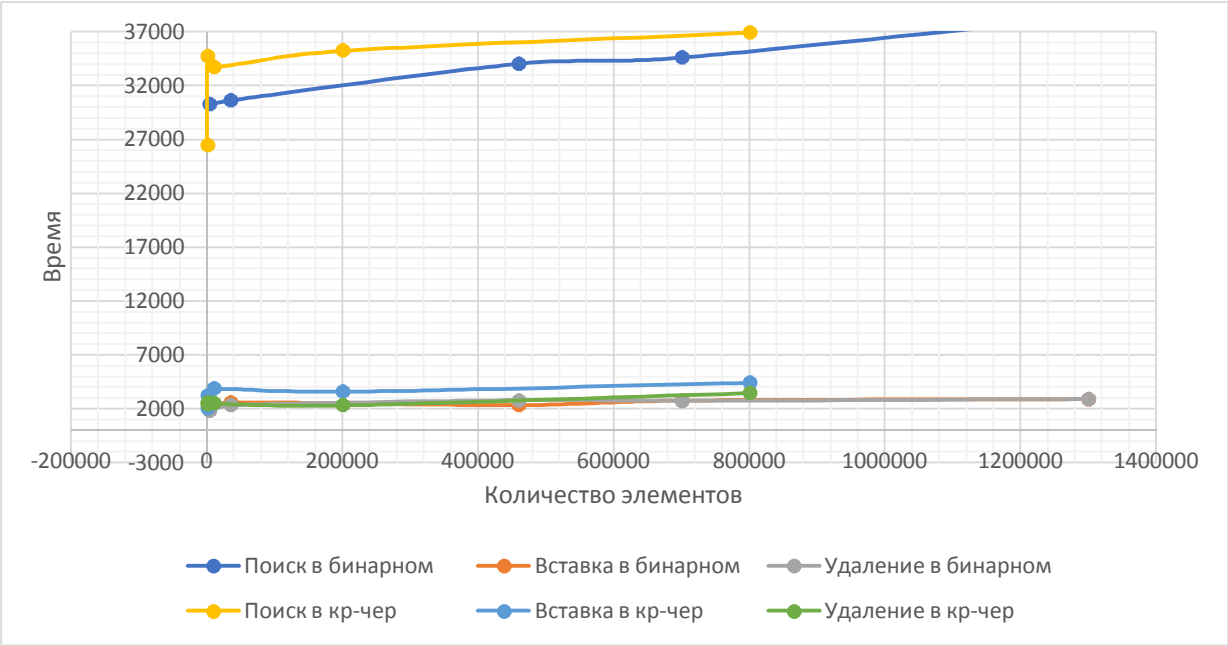


Рис. 2. Результаты выполнения операций поиска, вставки и удаления в алгоритмах

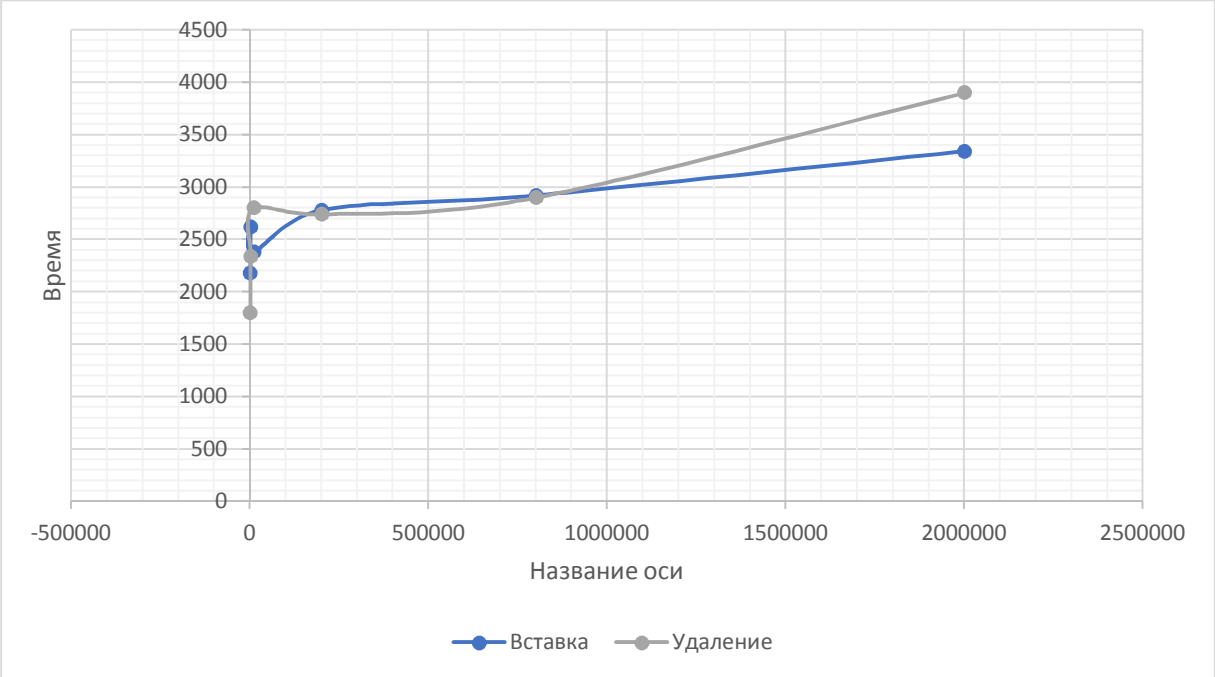


Рис. 3. Вставка и удаление в двоичном дереве поиска

График вставки (рисунок 3) в бинарном дереве поиска близок к логарифмическому графику, что подтверждает рассмотренную при анализе временную сложность. График удаления отклоняется от логарифмического вида при больших значениях количества элементов в дереве. Вероятно, это связано с дополнительными затратами времени в связи с особенностями выбранной структуры для хранения данных.

По графику вставки и удаления для черно-красного дерева (рисунок 4) можно заметить резкое возрастание затрачиваемого времени при возрастании количества элементов в дереве в начале и снижение темпов в дальнейшем.

Говоря об операциях вставки и удаления, можно сделать два заключения.

Во-первых, как и предполагалось при анализе, для красно-черного дерева операции выполняются дольше, за счет выполнения дополнительных шагов по восстановлению нарушенных свойств.

Во-вторых, общим моментом для обоих алгоритмов является то, что операция удаления в среднем тратит меньше времени, чем поиск и вставка. Это объясняется тем, что известен индекс удаляемого элемента, а значит, к нему не нужно спускаться от корня по дереву. Кроме того, в общем случае операция удаления просматривает и затрагивает только несколько элементов, находящемся рядом с удаляемым элементом, тогда как при поиске обходится всегда целая ветвь.

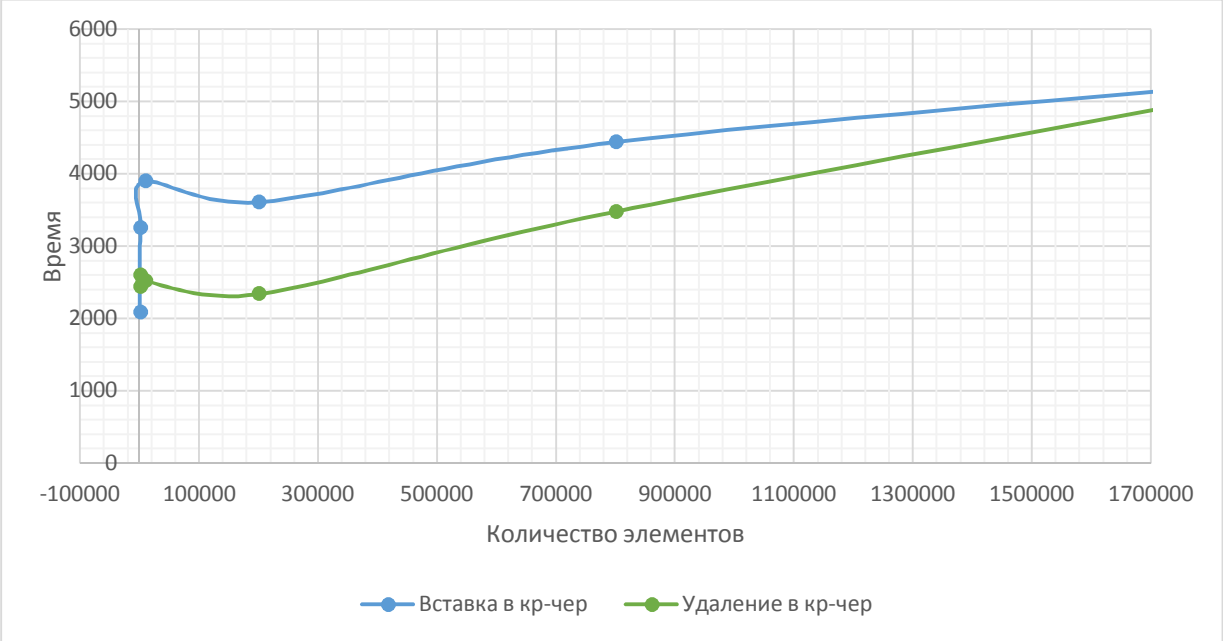


Рис. 4. Вставка и удаление в красно-черном дереве

Из проведенного анализа можно заключить, что сбалансированное дерево имеет реальное преимущество перед бинарным деревом поиска при больших объемах данных. В этом случае стабильность затрат времени на поиск элемента при любой случайной генерации дерева по эффективности сможет перевесить те потери, которые влекут за собой периодически выполняемые операции по восстановлению красно-черных свойств при вставке и удалении элементов. В противном случае вполне допустимо использование и несбалансированного дерева, особенно при необходимости частого изменения его структуры, благодаря быстрому выполнению операций вставки и удаления в нем.

Анализ графиков поиска и вставки для обоих алгоритмов позволяет говорить о совпадении с ожидаемой временной сложностью, рассмотренной в книге [1]. Затраты на удаление элементов оказались больше, чем прогнозируемые. Это может быть связано с усложнением алгоритма операции удаления элемента массива в случае, когда де-

рево хранится в массиве – куче, и при удалении необходимо выполнять дополнительные операции, направленные на поддержание зависимости положения элемента в массиве от положения его родительского и дочерних элементов.

Литература:

1. Кнут Д.Э. Искусство программирования / Д.Э. Кнут. 2 изд. - М.: И.Д. Вильямс, 2007. 832 с.

2. Новиков Ф.А. Дискретная математика: учебник для вузов / Ф.А. Новиков. 3 изд. - СПб.: Мир книг, 2011. 384 с.

3. Современные методы поиска информации // URL: http://poisk.swsu.ru/opis-poisk/problem/63-sovremen-metod.html (дата обращения: 01.05.2018).

4. Кормен Т.Х. Алгоритмы: построение и анализ / Т.Х. Кормен, Ч.И. Лейзерсон, Р.Л. Ривест, К. Штайн, 3 изд. - М: И.Д.Вильямс, 2013. 1328с.

Тимакина Ю.А.

Ростовский юридический институт МВД России

ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ С ИСПОЛЬЗОВАНИЕМ МЕТОДА KPI

Когда речь идет об эффективности управленческой деятельности, довольно трудно идентифицировать самые важные критерии, оценка которых привела бы к определению нужного вектора развития организации. Управленческая деятельность в органах внутренних дел, как и в любой другой организации, строится на базе системного использования функций управления, которые всегда присутствуют в ходе реализации внутриорганизационных мероприятий. Разнообразие набора функций управления в различных научных источниках предельно высоко. Однако наиболее часто встречаются следующие: информационно-аналитическая, функция планирования, организация, координация и контроль. Анализ докладов высшего руководства страны, ведомственной нормативно-правовой базы, прямых указаний руководства МВД России дает основание говорить о реально существующих проблемах в организации управленческой деятельности в органах внутренних дел.

Важными являются вопросы структурного и организационного построения органов внутренних дел разных уровней управления, а также существующих недочётов в организации работы подчинённых им подразделений и служб, какими являются:

- очевидное дублирование функций и задач в деятельности подразделений и служб;
- слабый уровень обмена информацией между подразделениями и службами;
- отсутствие слаженного механизма взаимодействия;
- нарушения учётно-регистрационной дисциплины, несоблюдение правил защиты государственной тайны;
- низкий кадровый потенциал; слабое использование имеющихся ресурсов аттестованных полицейских; не учитывается организация профессиональной подготовки и переподготовки работников, приводящая к высокой текучести кадров. Данная проблема связана также с авторитарным стилем управления и сложным характером руководителей при отсутствии личного авторитета и внимания к нуждам подчинённых;
- неэффективное использование финансовых и материальных ресурсов;
- слабая организация контрольной деятельности.

Таким образом, имеется блок недостатков, вызванных неэффективной организацией работы руководителей различных уровней и их подчинённых, которые необходи-

мо корректировать, используя инструментарий информационных технологий и другие эффективные научные методы, например метод ключевых показателей эффективности KPI(англ.- Key Performance Indicators (KPI)- ключевые показатели эффективности)[8].

Кроме того, необходимо сформировать основные требования к критериям оценки эффективности управленческой деятельности, которые позволят получить научно-обоснованную систему оценки. Можно полагать, что основными требованиями к критериям должны быть следующие:

- отражать в себе цели, задачи и функции управленческого воздействия;
- содержать результаты оцениваемой деятельности в количественной и качественной форме на базе показателей эффективности;
- характеризовать все аспекты управленческой деятельности объекта оценки;
- основываться на имеющейся в системе ОВД статистической, нормативной информации;
- избегать нерационально большого числа используемых критериев.

Сейчас объективно настала необходимость не только в разработке системы оценки эффективности управленческой деятельности в службах и подразделениях, но и в создании методики такой оценки. Необходимо учитывать, что разрабатываемая система оценки не может находиться в статическом состоянии, критерии и показатели должны и будут изменяться динамично вместе со служебными нормами или недостатками в органах внутренних дел.

Задачей каждой системы управления любой службы или подразделения является уменьшение неупорядоченности (энтропии) в управляемом объекте за счёт более существенного потребления информации. В формуле представлена функциональная зависимость энтропии (H) от информации (I) и от эластичности энтропии по отношению к увеличению информированности руководства органов внутренних дел ($\boldsymbol{s}$) [7]:

$$H = (1 - I)^S \qquad (1)$$

Анализ формулы (1) приводит нас к выводу, что чем выше информированность руководителей, больше знания закономерностей работы управляемого объекта, тем меньше энтропия процесса управления и больше его эффективность. Наглядно это представлено на рис 1. Использование гигантских объёмов структурированной информации при высоком уровне управляемости (высокой квалификации работников-управленцев, их умении обрабатывать информацию, превращать знания в реальные действия) позволяет уменьшить энтропию и с меньшими затратами достигать поставленных целей и задач. Знания становятся более эффективными, чем потребление информации для управления, потому что характеризуют процессы более высокого уровня, как это показано на рисунке 2.

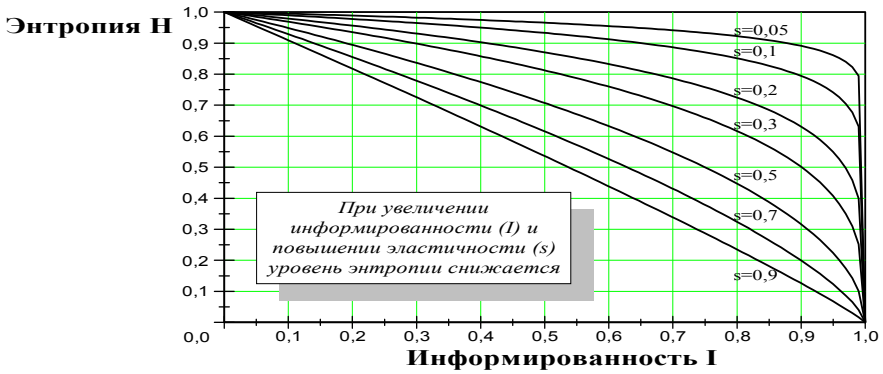


Рис. 1. Изолинии функции $H(I, s)$ при фиксированных значениях s

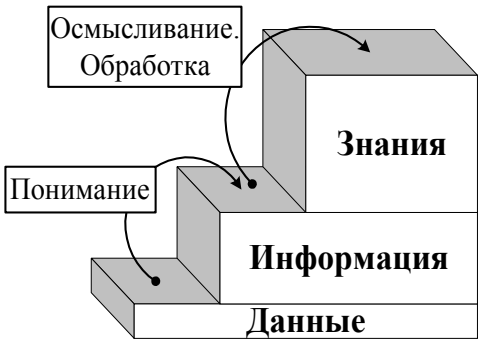


Рис. 2. Этапы представления информации и знаний

Тогда, можно сделать вывод, что использование знаний более эффективно, так как повышение информированности лиц, принимающих решение (ЛПР) или проводящих проверку приводит к снижению всех потерь организации. В [7] доказано, что информационную мощность организации, используя формулу А. Эйнштейна, можно рассмотреть в виде:

$$E = M \cdot C^2 \quad (2)$$

где М - семантическое содержание информации, ее ценность;

С - уровень подготовки персонала.

Для повышения Е и увеличения эффективности управления нужно изменять, повышая М и С. Такие качества будет иметь только активная, постоянно обновляемая информационная система на базе современных информационных технологий, которая может выявлять и учитывать закономерности на основе обработки информации и обнаружении связи между разными явлениями, базируясь при этом на современной вычислительной технике и информационных технологиях. Изучение получаемой информации приведёт к получению активной системы знаний, на базе которых она меняет своё состояние, строит модели поведения внешней и внутренней среды и прогнозирует ее действия.

Одним из перспективных методов оценки эффективности управления является метод KPI. Метод KPI (англ. - Key Performance Indicators (KPI) - ключевые показатели эффективности), так же, как и рейтинговый метод оценки, является одной из разновидностью квалиметрических методов, но позволяет не просто оценить деятельность сотрудников, но и оценить эффективность системы управления в целом [8]. В этом, на наш взгляд, несомненное преимущество метода KPI. Одним из существенных достижений системы KPI можно считать, с одной стороны, использование аналитики, которая выполняет роль инструмента планирования и отслеживания прогресса (регресса) системы управления на каждом этапе; с другой стороны, позволяет связать воедино интересы сотрудников и стратегию организации, что всегда было слабым звеном систем управления.

Использование подходов в теоретической квалиметрии делает возможным научно подойти к выбору и построению системы KPI (например, при оценке эффективности управления) и настроить измерительную систему с учётом стратегических целей органов внутренних дел.

Одним из способов определения значения показателя эффективности управленческой деятельности организации является нахождение аккумулируемых результатов его деятельности на единицу затраченных ресурсов. В квалиметрии существует подход, благодаря которому могут быть количественно оценены все экономические и неэкономические по своей сущности результаты и, таким образом, включены в рассмотрение при оценке эффективности управленческой деятельности или при получении различных видов обобщающей отчётности. Под ключевыми показателями эффективности в

нашей модели будем понимать количественно измеримый или качественный индикатор фактически достигнутых результатов в рамках выполнения поставленных целей, а также считать, что стратегические цели организации должны доводиться до уровня сотрудников и замеряться с помощью KPI

Предлагаемая модель системы KPI построена по нескольким основным направлениям (включает 10 ключевых показателей эффективности):

- затраты на управление;
- удельные затраты на управление организацией;
- численность работающих в организации (службе);
- стоимость основных производственных фондов подразделения;
- число преступлений против личности (за исключением случаев насилия в семье) на 100 000 человек;
- уровень преступлений против собственности на 100 000 человек;
- процентная доля часов, отведенных офицеру полиции для выполнения функций;
- скорость решения вопросов в подразделениях;
- оценка качества информации;
- уровень сотрудничества служб и подразделений с отделом управления персоналом.

Внедрение системы KPI необходимо совмещать с одновременным внедрением системы бюджетирования и управленческого учёта, которая является необходимым инструментом для поддержки реализации стратегии и позволяет предоставлять детальные данные о структуре затрат. Система бюджетирования и управленческого учёта должна включать следующие элементы: источники финансирования, управленческий план счетов, финансовая структура, централизованно управляемые проекты и сметы.

Для качественной оценкиэффективности управленческой деятельности в органах внутренних делнеобходимо качественное информационное обеспечение. Информационное обеспечение органов внутренних дел в настоящий момент является одной из самых важных и в то же время одной из самых непростых задач. Связано это с несколькими причинами. Во-первых, в последнее время отмечается тенденция увеличения потока как внешней, так и внутриотраслевой информации. Во-вторых, в связи с постоянной потребностью улучшения результативности управления, необходимо все более качественно обрабатывать информацию. Именно поэтому нужно искать новые способы организации обработки информационных потоков.

Получаемые сведения и данные накапливаются, обрабатываются, обобщаются, используются и становятся информационным ресурсом, который включается в общую информационную систему, а структура, накапливающие данные ресурсов – владельцем информационного ресурса. При этом появляются два ключевых вопроса: возможность поиска нужной информации, нужных данных и возникновение критической избыточности информации.

Информация, поступая в те или иные отделы, службы, подразделения, накапливается там, конкретным образом обрабатывается и систематизируется, создавая информационные ресурсы. Вследствие естественных объективных оснований ресурсы являются разделёнными, создаваясь в различных отделах и службах. Далее необходимо отметить, что при обработке часть информации остается в бумажном виде, часть переходит в электронный вид, некоторая доля особо важной информации имеется в обоих видах. Такими логически соединенными структурами информации выступают базы данных.

Подразделения, хранящие и обрабатывающие базы данных, обязательно должны обеспечивать актуальность информации, т.е. систематически ее обновлять и вносить поправки. Такие структуры называются источниками информационных ресурсов.

Косновным информационным ресурсам относятся, прежде всего, ИСОД (Единая система информационно-аналитического обеспечения деятельности МВД РФ) иинтер-

нет-порталы различных подразделений и служб. Для эффективной работы организации используются различные технические и информационные средства.

Процесс модернизации технологий оценки эффективности управленческих решений, ключевой элемент которых представляет собой стратегический выбор, базирующийся на сравнении собственного ресурсного потенциала организации с потенциальными возможностями и рисками внешней среды, в которой оно функционирует, это сложный и весьма трудоёмкий процесс. Процедура формирования решений и их продуктивность иллюстрируют ключевые показатели уровней и параметров эффективности системы принятия управленческих решений - рост уровня управляемости в общей сложности как следствие модернизации, развития, согласования функций планирования, регулирования, организации, координации, программирования, контроля, учёта и анализа, нацеленных на увеличение продуктивности текущей деятельности, перспективного и стратегического развития; повышение уровня управления, мобильность, гибкость, оперативность, оптимизация в текущем, среднесрочном и в стратегическом промежутке времени; экономическая эффективность.

Так, к примеру, улучшение технологии разработки управленческих решений в сфере организационной структуры позволит усовершенствовать нормы управляемости. Организационная структура большинства органов внутренних дел представляет собой линейно-функциональный вид. Рекомендации, связанные с подготовкой практических мер по модификации организационной структуры, делегирование доли полномочий и обязанностей на уровень среднего звена увеличит показатель управляемости.

Из большого числа вероятных признаков оценки результативности управления, являются максимально показательными два: нагрузочный и продуктивный.

Нагрузочный критерий оценки эффективности определяется параметром «сравнительная напряжённость деятельности», определяющим интенсивность труда сотрудников различных служб и подразделений.

Результативный критерий оценки результативности функционирования организаций ОВД содержит в себе несколько составляющих: финансовую эффективность, экономическую эффективность деятельности, продуктивность производственной деятельности.

Данную рекомендацию имеет смысл рассматривать и оценивать как эффективную по причине нулевых затрат. Подобное решение предполагает лишь пересмотр должностных полномочий и обязанностей, модификацию организационной структуры. Подготовка практических мер по осуществлению данного предложения увеличит показатель управляемости, снизит нагрузку на управляющий персонал, и при этом организация не понесёт материальных потерь.

Для улучшения оценки эффективности управления необходимо внедрить так называемую подсистемуинформационно-аналитической обработки и представления знаний и подсистему моделирования и прогнозирования.

Подсистема информационно-аналитической обработки и представления знаний это совокупность согласованных и взаимоувязанных информационных технологий, инструментов, средств и сервисов, способных реализовывать и поддерживать широкий класс аналитических приложений. В частности, такая подсистема должна обеспечивать решение таких задач как:

– создание регламентной (обязательной) отчётности;

– формирование в диалоговом режиме нерегламентной (неформальной) отчётности по параметризованным запросам лиц принимающих решения;

– проведение аналитических работ, включающих статистический анализ;

– представление данных в Internet на базе ИСОД.

Данная подсистема значительно упрощает процедуру информационно-

аналитической работы в учреждении, сокращает время ее выполнения, и позволяет получить максимально структурированную информацию для последующего применения в разработке управленческих решений.

Подсистема моделирования и прогнозированияэто комплекс логически, информационно-алгоритмически взаимосвязанных моделей, отражающих затратные, кадровые, результирующие, информационные, технологические процессы на всех уровнях организации. Средства реализации такой подсистемысмогут создаватьрасчётные цепочки из разрозненных моделей и знаний. Для этого необходимо имеющимися ресурсами произвести интеграцию входных параметров одних моделей с выходными параметрами других моделей.

Данная подсистема является следующим этапом информационно-аналитической работы в учреждениях внутренних дел. С ее помощью, используя полученную на предыдущем этапе структурированную информацию, имеется возможность смоделировать все возможные альтернативные решения имеющейся проблемы, а также произвести прогноз их последующих результатов. Это максимально упрощает процесс информационно-аналитической работы, а также способствует более точному и обоснованному принятию управленческого решения.

Для максимально эффективного решения проблемы, предлагается внедрить программное решение для автоматизации комплекса задач на web-технологиях, разработанные Научно-производственным объединением «Криста»[4]. Для внедрения подсистемы информационно-аналитической обработки и представления знаний, а также подсистемы моделирования и прогнозирования предлагается решение «Аналитический центр руководителя»[4].

Основной целью подсистемы является информационная поддержка процессов подготовки, принятия и контроля управленческих решений в органах внутренних дел.

Данные предложения позволят органам внутренних дел наиболее оперативно и эффективно производить процедуру информационно-аналитической работы, на основе имеющихся в хранилище данных сведений по необходимой проблеме получать обработанную и структурированную информацию, представлять её в различных видах и формах, а также иметь возможность смоделировать все возможные альтернативные решения имеющейся проблемы и произвести прогноз их последующих результатов. Данный спектр информационных технологий способствует более точному и обоснованному принятию управленческого решения, что в свою очередь приведёт к более успешному функционированию органов внутренних дел.

Литература:

1. Андреев, Б.В., Казарина, А.Х., Капинус, О.С. Оценка эффективности работы органов прокуратуры со стороны личности, общества, государства // Вестник Академии Генеральной прокуратуры Российской Федерации. [Текст]. -2013-№ 1.

2. Внедрение электронных архивов [Электронный ресурс]. –Режим доступа:http://efsol.ru/ (дата обращения: 10.05.2018).

3. Кардашевский, В.В. Организация и осуществление зонального, отраслевого и особого контроля оперативно-служебной деятельности органов внутренних дел (на примере ГУВД по г. Москве): Учеб. пособие. [Текст]. - М., 2009.

4. Программное решение «Аналитический центр руководителя» на сайте НПО «Криста» [Электронный ресурс]. – Режим доступа: https://www.krista.ru/products/imonitoring/

5. Электронные архивы. Создание электронных архивов документов и организация хранилищ корпоративной информации [Электронный ресурс]. – Режим доступа: http://www.korusecm.ru/solutions/elib/ (дата обращения: 10.05.2018).

6. Customerstory: MarkhamStouffvilleHospital [Электронный ресурс]. – Режим доступа:https://customers.microsoft.com/Pages/ CustomerStory.aspx? recid=13797(дата обращения: 10.12.2017).

7. Myerson, Judith M. EnterpriseSystemIntegration, SecondEdition (BestPractices) [Электронныйресурс]. – Режим доступа: https:/books.google.ru/books?id= D2h1eHFABk0C (дата обращения: 10.05.2018).

8. Strategic Analysis of the Role of Information Technology in Higher Education – A KPI-centric model. [Электронный ресурс]. –Режим доступа: // Jornal Communications of the IIMA //http://scholarworks.lib.csusb.edu/ciima/?utm_source=scholarworks.lib.csusb.edu%2Fciima%2Fvol15%2Fiss1%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages (дата обращения: 10.05.2018).

Тимофеев В.В., Надвоцкая В.В.
Барнаульский юридический институт МВД России

ПРИКЛАДНОЕ ПРИМЕНЕНИЕ БЕЗУСЛОВНОЙ ОПТИМИЗАЦИИ ФУНКЦИЙ ЧИСЛЕННЫМИ МЕТОДАМИ

В общем случае, любые технические, технологические, экономические, социальные и бизнес-процессы могут иметь определенную вариативность своей практической реализации. Вариативность процесса – характеристика процесса, определяющая степень его склонности к отклонениям от запланированного хода протекания. Чем ниже его степень вариативности, тем ближе рассматриваемый процесс к идеальному – при повторяющемся по заданной схеме процессе, на выходе процесса получается запланированный результат необходимого качества.

Степень общей эффективности реализации каждого из них можно оценить, например, как возможность достижения предполагаемого результата рассматриваемого процесса с привлечением минимального количества затрат. К ним следует отнести материалы, финансовые издержки, время, затраченное на подготовку и выполнение отдельных действий или этапов, составляющих единую цепочку рассматриваемого процесса. При этом эффективность реализации самого анализируемого процесса находится в непосредственной зависимости от эффективности реализации составляющих этого процесса.

Решение вопросов обеспечения непрерывной, надёжной и эффективной, в отношении производительности, радиосвязью подразделений и территориальных органов внутренних дел МВД России и оптимизация работы радиопередающей аппаратуры в условиях современной эфирной обстановки является безусловно актуальной задачей. В этой связи использование математических методов оптимизации функций в приложении к различным аспектам технической сферы, на сегодняшний день, также актуально [1].

Математический аппарат анализа представлен двумя группами методов: аналитическими и вычислительными – численными. Первая группа методов эффективна при анализе процессов, описанных известной функцией, в рамках известных граничных условий, т.е. имеющих математическую модель, адекватную реальному процессу. Существует целевая группа таких моделей – оптимизационные модели. Поэтому, основным недостатком аналитических методов, ограничивающих сферу их применения, является отсутствие математического описания анализируемого процесса, адекватного реальным условиям его протекания и неопределённость граничных условий его параметров.

Вторая группа методов – численные позволяет решить задачу оптимизации анализируемого процесса методами приближённого решения математических задач, путем выполнению конечного числа элементарных операций над числами. В качестве элемен-

тарных операций обычно применяются арифметические действия, выполняемые обычно с необходимой точностью, а также вспомогательные операции – например, записи промежуточных результатов, выборки из таблиц. При этом, числа задаются определённым набором цифр в некоторой позиционной системе счисления, обычно десятичной или двоичной. В ходе выполнения анализа процесса численными методами числовая прямая заменяется дискретной системой чисел – сеткой. Функция непрерывного аргумента заменяется таблицей её значений в сетке с выбранным шагом. Операции анализа, действующие над непрерывными функциями, заменяются алгебраическими операциями над значениями параметров функций в сетке. Положительными свойствами численных методов является возможность сведения решения математической задачи к вычислениям, которые могут быть выполнены как вручную, так и с помощью средств вычислительной техники [2].

В технической сфере существует множество задач, требующих оптимизации функций одной или нескольких переменных [3]. Типичным примером такой задачи может служить оптимизация функции настройки переменных компонентов автоматических согласующих устройств радиопередающих аппаратов различного назначения.

Является очевидным факт зависимости параметров согласования антенно-фидерного устройства (АФУ) от характеристик параметров выходного каскада радиопередающего аппарата (РПА), самой фидерной линии и входных электрических параметров антенны. Следует уточнить, что в общем случае, эффективное согласование радиопередающего аппарата с антенно-фидерным устройством осуществимо при одинаковом активном сопротивлении всех трёх перечисленных компонентов и его чисто активном характере. При этом реактивная составляющая входного сопротивления этих компонентов пренебрежительно мала, а в идеальном случае – равна нулю.

В математическом отношении рассматриваемые объекты находятся во взаимосвязи условиями необходимости и достаточности. Рассмотрим данное утверждение подробней.

В самом общем случае необходимое и достаточное условия – это определённые виды условий, логически связанные с определённым суждением. Отличие этих двух условий позволяет обозначать виды связи суждений и широко используется в алгебре логики и других разделах математики. Так, необходимыми условиями истинности утверждения А называются условия, при несоблюдении которых утверждение А принципиально не может быть истинным. Суждение Р является необходимым условием суждения Х, когда из истинности Х следует истинность Р. То есть, если Р ложно, то заведомо ложно и Х.

Достаточными называются такие условия, при соблюдении которых утверждение А является истинным. При этом, суждение Р является достаточным условием суждения Х, когда из истинности Р следует истинность Х, то есть в случае истинности Р проверять Х уже не требуется.

Иными словами условия эффективного согласования антенно-фидерного устройства с радиопередающим аппаратом можно сформулировать, как отсутствие реактивной составляющей входного сопротивления компонентов рассматриваемой системы, при равенстве их активных составляющих. Менее очевидны, но от того не менее значимы для качества согласования, внешние, по отношению к антенно-фидерной системе, факторы [4, 5]. В этой связи представляет существенный интерес определение границ рассматриваемой системы и связи её составляющих компонентов, которые можно выполнить методом системного анализа.

Задачей системного анализа, как научного метода познания, является последовательность действий по установлению структурных связей между элементами исследуемых сложных систем – технических, экономических и других. В свою очередь, он опи-

рается на комплекс общенаучных, экспериментальных, естественнонаучных, статистических, математических методов.

Целью системного анализа является упорядочение последовательности действий при решении проблем, основываясь на системном подходе. В системном анализе решение проблемы определяется как деятельность, которая сохраняет или улучшает характеристики системы. Приемы и методы системного анализа направлены на выдвижение альтернативных вариантов решения проблемы, выявление масштабов неопределенности по каждому варианту и сопоставление вариантов по их эффективности.

Результатом применения метода системного анализа для хорошо структурированных количественно выражаемых проблем используется известная методология исследования операций, которая состоит в построении адекватной математической модели (например, задачи линейного, нелинейного, динамического программирования, задачи теории массового обслуживания, теории игр и др.) и применении методов для отыскания оптимальной стратегии управления целенаправленными действиями по управлению процессом.

В отношении примера оптимизируемого алгоритма изменения параметров элементов настройки автоматического согласующего устройства, приведённого выше нет известной математической модели системы. Более того, сами границы системы являются весьма неочевидными. В анализируемую систему, несомненно, входят выходной каскад радиопередающего устройства, фидерная линия и антенна. Прочие же компоненты, явным образом влияющие на параметры согласования радиопередающего устройства с антенной, могут быть представлены совокупностью внешних факторов, включающих в себя: параметры установки антенны, электромагнитную обстановку в ближней зоне, климатическое воздействие на антенну, флуктуацию электрических параметров, обусловленную старением материалов и конструкции в целом, прочие причины. Таким образом, выявление элементов, оказывающих влияние на анализируемую систему, обнаружение взаимодействия и связей, непродуктивно, если при этом не вскрываются свойства целостности, существенные для решения задачи, ради которой формируется система. Фактически это и есть вопрос о границах системы. Если они оказываются слишком узкими, то не будет основы для получения необходимых для достижения целей исследования результатов, но и включение в систему элементов, изучение которых не способствует выявлению свойств целостности, может создать существенные технические препятствия для анализа из-за возрастания объема обрабатываемой информации, требующей сбора, обработки, осмысления, увеличение вычислительной нагрузки. Более того, неадекватное формирование системы часто направляет всю работу с ней по ложному пути, снижая её эффективность и общую результативность.

Одним из направлений оптимизации работы согласующих устройств автоматического типа, вне зависимости от их схемотехники высокочастотного (ВЧ) блока, является создание эффективной системы автоматического управления процессом согласования антенно-фидерного устройства с радиопередающим аппаратом. Основой для её создания является выработка достаточно эффективного алгоритма управления коммутацией элементов ВЧ блока.

Проблемные вопросы построения эффективной системы управления подобными устройствами затрагивают как схемотехнические, так и математические аспекты.

К схемотехническим можно отнести общую структурную схему построения ВЧ блока устройства, выбор между использованием в качестве настроечных элементов приборов с переменным значением электрического параметра C и L, либо наборов дискретных элементов; количество дискретных элементов и степень дискретизации варьируемого электрического параметра, закон изменения варьируемого электрического параметра при коммутации от элемента к элементу. Следует отметить, что электрические

параметры ёмкости *C,* индуктивности *L* и электрической прочности компонентов, находятся в непосредственной зависимости от выбранной структурной схемы устройства, а также от предполагаемых входных параметров согласуемых антенн и диапазона их разброса. Кроме этого необходимо учитывать уровень выходной мощности РПА.

К математическим аспектам построения и оптимизации подобных алгоритмов следует отнести оценку диапазона входных сопротивлений согласуемых антенн, выявление и оценку реактивной компоненты входного импеданса, возникающей в процессе согласования, оценку токовых нагрузок и электрической прочности используемых компонентов согласующего устройства. Указанные аспекты находятся в неразрывной взаимосвязи и взаимозависимости.

Решение задачи алгоритмизации процесса согласования вплотную связано с выбором эффективной последовательности операций изменения электрических параметров настроечных элементов устройства, либо коммутации их дискретных компонентов.

Решение задачи согласования способами последовательного перебора дискретных компонентов, либо перестройки величины номинала *C* и *L,* неэффективно по причине продолжительности этого процесса порядка десятков минут, при условии достаточной степени дискретности коммутируемых компонентов и приемлемой степени точности настройки, т.е. малой погрешности согласования. Кроме этого возникает необходимость хранить полученные значения контролируемого параметра и сравнивать их между собой в процессе настройки.

При алгоритмах, оценивающих изменение качества согласования по оценке убывания абсолютного значения коэффициента стоячей волны (КСВ) и осуществляющих поиск его минимума, возникает проблема неабсолютности этого минимума во всём рабочем диапазоне частот РПА и устройства его согласования с АФУ. Т.е. поскольку практически любая антенная система, а особенно многодиапазонная, является мультирезонансной, то и минимумов КСВ, в общем случае, может быть более одного. Задачей же эффективной реализации алгоритма согласования является поиск абсолютного минимума для используемой антенной системы. Только этот абсолютный минимум КСВ, со значением, стремящимся к единице, и будет истинным.

Недостатком алгоритма управления многих опубликованных разработок автоматических согласующих устройств является прекращение процесса согласования при достижении любого неабсолютного минимума КСВ. Кроме этого, поскольку по сложившейся традиции ВЧ блок согласующего устройства выполняется по Г-образной схеме, в процессе построения алгоритма работы системы автоматического управления, встаёт вопрос первоначальной коммутации конденсаторного блока устройства. Правильный выбор схемы подключения конденсаторного блока позволяет согласовать антенну уже при первой итерации алгоритма управления. В противном случае, при неправильной коммутации блока конденсаторов, согласования не произойдёт, а процедуру настройки придётся повторять с начала.

При невозможности предварительной оценки входных параметров согласуемой антенны представляется целесообразным последовательный перебор коммутации конденсаторного блока к выходу и входу блока индуктивностей. По оценке полученных значений КСВ производится выбор положения коммутации конденсаторного блока, обеспечивающего минимальное численное значение КСВ, либо иная оценка входного импеданса АФУ и дальнейшая оптимизация параметров согласования в полученной конфигурации ВЧ блока согласующего устройства.

Одним из основных и, наверное, наиболее эффективным способом получения решений многих технических и технологических задач является математическое моделирование процессов и явлений. Для успешного осуществления математического моделирования исследователю необходимо представлять себе имеющийся набор алгоритмов

вычислительной математики, а также иметь навыки их программной реализации на аппаратной базе ПЭВМ, в процессе исследований, и на базе микроконтроллеров, в процессе технической реализации устройства.

С точки зрения последующей реализации на микроконтроллерной базе наибольший интерес представляют собой элементарные методы безусловной минимизации функции одной и многих переменных.

Проведём сравнительный анализ имеющихся методов минимизации, сравним их преимущества и недостатки.

Хотя для решения рассматриваемой задачи необходимо нахождение минимума функции, не равного нулю, а стремящегося к единице, для случая рассмотрения КСВ, как величины, непосредственным образом зависящей от значения напряжения отражённой волны представляется возможным использовать методы, применяемые для решения трансцендентных уравнений вида:

$$f(x, p_1, p_2, \ldots, p_n) = 0 \qquad (1),$$

где *f*- заданная функция, *x*- неизвестная величина (аргумент функции), $p_1, p_2, \ldots, p_n$- параметры задачи.

При этом, обычно, исследователя интересует поведение функции в зависимости от параметров p_k. При каждом фиксированном наборе параметров p_k уравнение (1) может иметь либо конечное, либо бесконечное количество решений *x*, что соответствует определенному физическому смыслу конкретной задачи.

В рассматриваемом случае в качестве параметров p_k выступают частота колебаний выходного сигнала, поступающего из выходного каскада РПА в АФУ, геометрические параметры конструктивных элементов антенны и фидера, пространственное расположение конструктивных элементов антенны относительно внешних объектов. В качестве неизвестного *x* могут быть выбраны собственные частоты резонанса излучающих элементов антенны

Не нарушая общности задачи, можно поменять местами неизвестное *x* и любой из параметров p_k, т.е. решить уравнение (1) относительно другой неизвестной величины. При этом решениями или корнями уравнения (1) являются значения, которые при подстановке в уравнение обращают его в тождество.

К сожалению, только для простейших уравнений удаётся найти решение в аналитическом виде, т.е. записать формулу, выражающую искомую величину *x* в явном виде через параметры p_k

В большинстве же случаев приходится решать трансцендентные уравнения вида (1) численными методами.

Если функция является непрерывной на рассматриваемом интервале значений аргумента x, то график функции не обязательно строить, достаточно найти интервалы, на которых изменяется знак функции $f(x)$.

Одним из метода анализа функций является метод дихотомии, применяемый для определения корней уравнения. Метод дихотомии заключается в следующем. На рассматриваемом отрезке *ab* значений аргумента функции *x*, определяем середину отрезка $\bar{x} = (a+b)/2$ и вычисляем функцию $f(\bar{x})$. Далее делаем выбор, какую из двух частей отрезка взять для дальнейшего уточнения корня. Итерационный процесс будем продолжать до тех пор, пока интервал *ab* не станет меньше заданной погрешности *e*.

Следует учитывать, что функция $f(x)$ вычисляется с некоторой абсолютной погрешностью ε_1. Т.е при подходе к минимуму функции, особенно, если она имеет плавный характер изменения значений, её значения в соседних точках могут быть близкими друг другу по величине и сравнимыми с погрешностью её вычисления. Т.е. возникает полоса шумов шириной $2\varepsilon_1$. Дальнейшее уточнение минимума окажется невозможным.

Поэтому граничным условием прекращения итерационного процесса необходимо обозначить попадание значений функции в эту полосу шумов. Кроме этого необходимо учесть увеличение погрешности вычисления длины отрезка *ab* за счёт вычитания близких чисел *b-a*, при уменьшении интервала [*ab*]. Достоинством метода дихотомии является существенное уменьшение объема вычислений по сравнению с графическим методом.

Этот метод, в целом, приемлем и для подбора значений номиналов ёмкости и индуктивности согласующего Г-образного звена.

Другие методы (метод хорд, метод касательных, метод секущих) применяют более жесткие требования к точности построения графика функции. В то же время они обеспечивают и более высокую точность определения решений (корней) уравнения.

Следует отметить, что алгоритмы, использующие для решения поставленной задачи итерационные способы требуют значительных вычислительных затрат.

Кроме этого наибольший интерес с точки зрения возможности практической реализации представляют алгоритмы, выполняющие вычисления в целочисленной арифметике, что существенно упрощает их аппаратную реализацию.

Среди методов, непосредственно предназначенных для безусловной оптимизации функций следует рассматривать метод золотого сечения. Хотя, в общем случае, исследуемая функция может быть как непрерывной, так и разрывной в области поиска минимумов, рассматриваемые функции, отображающие входные характеристики согласуемых антенн в подавляющем большинстве непрерывны во всей рассматриваемой полосе частот (значений аргумента *x* в нашем случае).

Минимумы дифференцируемой функции $f(x)$ определяются из уравнения

$$f'(x)=0 \qquad (2)$$

для решения которого применимы вышерассмотренные и другие известные методы решения уравнений.

Известно, что корень уравнения x^* уравнения 2 является точкой минимума функции $f(x)$, если $f''(x)>0$, и точкой максимума, если $f''(x)<0$.

Следует отметить тот факт, что проведённые экспериментальные исследования по оценке влияние внешних воздействий на антенны проводились в отношении однодиапазонных антенн, имеющих выраженный резонанс в рабочем диапазоне, т.е. функции, описывающие зависимость КСВ и значение напряжения отражённой волны в согласованном фидере этих антенн носят заведомо унимодальный характер и дополнительных процедур деления на участки не требуют. Кроме этого в большинстве своём функции в области минимума достаточно гладкие и, в общем случае, могут быть представлены в виде параболы с достаточно малой погрешностью аппроксимации [1]. В случае достаточно широкого рабочего диапазона РПА, более трёх октав для диапазона декаметровых волн, неизбежно наличие нескольких (или многих) побочных резонансов в антенном устройстве.

В рассматриваемом приложении исследования функций невозможно получить аналитическую формулу для производной $f''(x)$. Её значение можно определить дифференцированием полинома, аппроксимирующего функцию $f(x)$. В случае если функция $f(x)$ недифференцируема или вычисление её значений для аппроксимации производной связано со значительными затратами времени, минимизацию осуществляют по следующим алгоритмам.

Поиск минимумов функции $f(x)$ разделяется на два этапа. На первом этапе выделяются интервалы аргумента *x*, в которых существует единственная точка x^*, где функция принимает экстремальное значение. Функции на каждом таком интервале называется унимодальной.

Первый этап минимизации по своей сути близок к задаче отделения корней трансцендентных уравнений и не поддаётся строгой алгоритмизации. При этом возможно использование графического представления минимизируемой функции, хотя оно связано с требованием достаточно точного построения графика с малым шагом изменения аргумента, для предотвращения пропуска возможного минимума функции [1].

На втором этапе осуществляется уточнение местоположения минимумов на интервале [*ab*] путем деления его в точке x_1 в отношении двух последовательных чисел Фибоначчи. Далее выбирается точка x_2, симметричная x_1 относительно середины отрезка. Учитывая унимодальность функций на рассматриваемых отрезках, если $x_1 < x_2$ и $f(x_1) > f(x_2)$, то в качестве следующего рассматриваемого интервала неопределённости следует выбрать отрезок $x_1 b$, что эквивалентно переносу точки a в точку x_1. Если $x_1 < x_2$ и $f(x_1) < f(x_2)$, то очередной интервал неопределённости будет $a x_2$. При $f(x_1) = f(x_2)$, минимум расположен в интервале $x_1\, x_2$. Метод золотого сечения зачастую сочетают с одним из методов аппроксимации минимизируемой функции, в которой область минимума обычно приближают параболой, минимум которой определяется по аналитической формуле.

Метод координатного спуска заключается в сведении многомерной задачи к последовательным одномерным задачам, которые решаются методами минимизации функции одной переменной, в частности, рассмотренным методом золотого сечения. Недостатком данного метода также является необходимость предварительного определения области предполагаемого минимума функции. В области, близкой к минимуму функция достаточно гладкая, то процесс спуска по координатам будет линейно сходиться к минимуму. Метод градиентного спуска основан на поиске направления спуска к минимуму в направлении, противоположном градиенту функции, направленному в сторону наискорейшего локального возрастания этой функции. При этом минимизируемая функция должна быть дифференцируема и ограничена снизу [1].

При проведении экспериментальных исследования частотных параметров выходного сигнала РПА, исследовании амплитудно-частотной характеристики его выходного сигнала и минимизации полосы, занимаемой выходным сигналом, возникла необходимость оценки степени влияния внешних воздействий, различного рода, на антенно-фидерное устройство РПА. В рассматриваемом случае эти воздействия являются параметрами p_k. Степень существенности этих воздействий была оценена как значимая для практической целесообразности учёта их влияния на работу АФУ в процессе штатной эксплуатации РПА широкого назначения [4, 5].

Результатом этого влияния является изменение электрических параметров антенны, непосредственно оказывающих влияние на качество согласования АФУ с РПА. Степень рассогласования АФУ с РПА, возникающая при этом, вполне достаточна для снижения качества согласования АФУ с выходным каскадом РПА ниже уровня, предусмотренного производителем РПА для данного типа аппаратуры, в качестве допустимого эксплуатационного.

Рассмотренные аспекты выбора математических методов безусловной оптимизации функций численными методами, рассмотренные, для примера, в приложении к выбору алгоритма оптимизации параметров элементов настройки устройств согласования РПУ с антенно-фидерными устройствами, позволяют считать их эффективными. Решение поставленной задачи невозможно без использования элементов метода системного анализа. Комплексное применение указанных методик является эффективным математическим инструментом решения слабо структурированных, или смешанных задач, которые содержат как известные компоненты, так и малоизвестные, неопределенные составляющие, которые имеют тенденцию доминировать [6].

Литература:

1. Зенков А.В. Численные методы : учеб. пособие / А.В. Зенков.— Екатеринбург : Изд-во Урал. университета, 2016. – 124 с.
2. Мудров А.Е. Численные методы для ПЭВМ на языках Бэйсик, Фортран и Паскаль. – Томск: МП «Раско » при издательстве «Радио и связь» 1992.
3. Сухарев А.Г., Тимохов А.В., Фёдоров В.В. Курс методов оптимизации. – М.:Наука. 1986.
4. Тимофеев В.В., Пронин С.П., Зрюмов Е.А. Влияние внешних факторов на качество согласования антенно-фидерного устройства с радиопередающим аппаратом. Измерение, контроль, информатизация: Материалы девятой международной научно-технической конференции./ Под. Ред. Л.И. Сучковой – Барнаул: АлтГТУ, 2008. – с. 230-234.
5. Тимофеев В.В. Влияние типичных внешних воздействий на качество согласования антенно-фидерного устройства с радиопередающим аппаратом. // Научная сессия ТУСУР-2008: Материалы докладов Всероссийской Научно-технической конференции студентов, аспирантов и молодых учёных. Ч. 1. – Томск: В-Спектр, 2008. – с. 128-130.
6. Тимофеев В.В., Пронин С.П., Зрюмов Е.А. Экспериментальная установка для исследования качества согласования антенно-фидерного устройства с радиопередающим аппаратом. В сборнике: Измерение, контроль, информатизация Материалы Девятой Международной научно-технической конференции. Барнаул, 2008. С. 228-230.

Трибунских О.А.
Военный учебно-научный центр Военно-воздушных сил
«Военно-воздушная академия имени профессора Н.Е. Жуковского
и Ю.А. Гагарина» (г. Воронеж)
Мачтаков С.Г.
Воронежский государственный университет инженерных технологий

КЛАССИФИКАЦИЯ УЧАСТНИКОВ ЭЛЕКТРОННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Электронное информационное взаимодействие стало предметом пристального внимания исследователей и разработчиков различных инфокоммуникационных систем уже достаточно давно. Связано это в первую очередь с бурным ростом количества физических и юридических лиц, подключенных к сетям связи и возможностью передачи значимой информации практически по всему миру. Несомненно, что исследование электронного информационного взаимодействия касается огромного комплекса самых разнообразных сторон: это могут быть вопросы самого разнообразного характера – технического, юридического, экономического, социального и т. д.

Рассматривая самые разнообразные признаки классификации электронного информационного взаимодействия [1], можно по аналогии построить классификацию на основе отношений между участниками взаимодействий, и позволяет предложить следующие типы:

1. Взаимодействие между сотрудниками одной организации – такое взаимодействие не требует выхода передаваемых данных за пределы сети организации. Даже при условии территориальной распределённости отдельных структурных подразделений организации информация не покидает сеть организации, формируется и передаётся в едином информационном пространстве. Такое взаимодействие в целом может обладать более низкими требованиями по обеспечению информационной безопасности, ограничению доступа к передаваемым данным, а также не требовать проведения дополнительных преобразований, передаваемых в электронном виде данных. Сотрудники орга-

низации могут иметь не только служебные, но и личные связи между собой, что позволяет переходить от делового стиля общения к межличностному для разрешения проблем и задач организации.

2. Взаимодействие между разными организациями – при таком подходе, должна соблюдаться технологическая нейтральность требований к передаваемой информации. Примерами реализации такой нейтральности для обмена официальными сведения является система межведомственного электронного информационного взаимодействия (СМЭВ). Можно отметить, что принцип технологической нейтральности также может быть реализован по-разному: если в СМЭВ второй версии каждая пара участников взаимодействия «договаривались» по поводу алгоритма передачи и формы представления данных, что, конечно, предоставляло участникам создавать «удобные» для них правила и процедуры, то в новой третьей версии СМЭВ, взаимодействие осуществляется по единым правилам для всех участников. Каждая заинтересованная организация предоставляет информацию посредством своего сервиса, а сам сервис имеет общую архитектуру для всех участников электронного взаимодействия.

3. Взаимодействие между физическими лицами – крайне обширная тема исследования, связанная как с использованием социальных сетей, мессенджеров, форумов, так и простой пересылкой писем по электронной почте. Здесь сами пользователи, не выступают в роли разработчиков, диктующих условия, алгоритмы и формы представления данных. Здесь пользователи только пользуются уже предлагаемыми третьими лицами (сторонними организациями) программными средствами. На первый план при данном виде взаимодействия выходят обеспечение тайны переписки, сохранение личных и персональных данных.

4. Взаимодействие между физическими лицами и организациями – аналогично предыдущему виду взаимодействия физические лица используют программные и технические средства для осуществления электронного информационного взаимодействия. Чаще всего такое взаимодействие связано либо с удовлетворением требований граждан на предоставление той или иной информации (например, правил приема в образовательную организацию, количестве вакантных мест для трудоустройства, ознакомления с графиком работы, ознакомлением с характеристиками продаваемых товаров и услуг и т.д.), либо с использованием разделяемых ресурсов для удовлетворения своих личных, научных или деловых интересов (например, использование облачных технологий и сервисов для хранения своих данных, разработки своих приложений, осуществление видеоконференцсвязи близких родственников или друзей, покупка билетов и т.д.). Одной из важных черт такого взаимодействия является официальность предоставляемых организациями сведений, имеющими как правило значимый характер, и возможная полная анонимность физических лиц.

Предлагаемая классификация позволяет определить направления работы правоохранительных организаций в целях контроля передаваемых сведений, проведения превентивных мер по предупреждению и раскрытию преступлений, своевременного реагирования на часто появляющиеся в последнее время фейковые новости компрометирующего характера. В то же время можно отметить, что приводимые типы отношений могут быть рассмотрены как процессы, с описанием возможных переходов участников взаимодействий между различными этапами взаимодействий. Такие процессы в свою очередь легко поддаются описательному анализу и составлению математических моделей в виде сетей Петри [2].

Литература:

1. Пьянков О.В. Оптимизация электронного взаимодействия в органах внутренних дел / О.В. Пьянков, И.Н. Шаповал // Математические методы и информационно-технические средства: материалы XIII Всероссийской научно-практической конферен-

ции (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 237-239.

2. Мачтаков С.Г. Математическое моделирование информационных процессов на этапе преддоговорной работы / С.Г. Мачтаков, Д.О. Смышников // Математические методы и информационно-технические средства: материалы XIII Всероссийской научно-практической конференции (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. – С. 187-189.

Трофимец Е.Н.
Санкт-Петербургский университет
государственной противопожарной службы МЧС России

МОДЕЛИРОВАНИЕ ЛОГИСТИЧЕСКИХ ОПЕРАЦИЙ В СИСТЕМЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ МЧС РОССИИ

Основной задачей системы материально-технического обеспечения (МТО) МЧС России является обеспечение всех структурных подразделений Министерства материальными средствами, необходимыми для выполнения задач по предназначению. К таким материальным средствам относятся: вооружение, военная, специальная и медицинская техника, пожарно-техническая продукция и продукция общепромышленного применения, запасные части, продовольствие, горюче-смазочные материалы, специальные жидкости, средства по обеспечению ремонта.

Многообразие номенклатуры и существенный рост звенности товаропроводящей сети, по мнению специалистов тыла МЧС, существенно усложнил задачи планирования логистических операций. Оптимальное решение таких задач, в зависимости от вида выбранной целевой функции, позволяет существенно снизить временные или стоимостные затраты на проведение таких операций.

Проведенный анализ нормативно-правовых документов позволил обосновать выбор методического аппарата планирования доставки материальных ресурсов подразделениям МЧС.

Нормативно-правовые основы базируются на двух основных документах: План строительства и развития сил и средств МЧС России на 2016 - 2020 годы и Приказ МЧС России от 18.09. 2012 г. №555 «Об организации материально-технического обеспечения системы МЧС России».

Организационные основы планирования базируются на общих методах логистики с учетом их специфики в деятельности МЧС:

- распределение ресурсов и определение потребности в средствах снабжения, исходя из критериев значимости для заданного района с учетом прогнозируемых рисков;
- координацию эффективного управления поставками и перевозками в условиях ЧС;
- регулирование и формирование запасов продукции как для обеспечения текущей деятельности, так и для функциональной работы системы РСЧС в особых режимах;
- анализ потребности в перевозках продукции, их направлениях и объемах, передвижения продукции через региональные и промежуточные склады;
- размещение, развитие и организацию базовых складов.

Система МТО МЧС обеспечивает выполнение различных логистических функций. В рамках данной статьи границы исследования охватывают подсистему транспортных перевозок материальных средств. В этой подсистеме в качестве поставщиков (или исходных пунктов) выступают или склады хранения МЧС, или официальные дилеры, зарегистрированные в реестре поставщиков продукции для государственных

нужд МЧС или определенные решением конкурсной комиссии. В качестве потребителей (пунктов назначения) выступают структурные подразделения Министерства.

Отправной точкой планирования доставки материальных ресурсов подразделениям МЧС послужила классификационная схема моделей управления цепями поставок.

Фокус внимания смещен на аналитические модели, а именно, на модели исследования операций, в более узких границах – на модели математического программирования. По степени определенности были рассмотрены детерминированные модели, однако эти границы могут быть расширены и на стохастические модели. В этом случае необходимо осуществить преобразование детерминированной постановки задачи к её стохастическому (или вероятностному) виду. Обычно преобразование осуществляется к одной из двух наиболее распространенных стохастических постановок, получивших соответственно названия *M*-постановки и *P*-постановки.

Если, для простоты, речь вести только о стохастической природе целевой функции, то в *M*-постановке задача будет формулироваться как максимизация (или минимизация) математического ожидания целевой функции, а в *P*-постановке – как максимизация вероятности получения максимального (или минимального) значения целевой функции.

По виду целевой функции и системы ограничений рассмотренные задачи относятся к классу линейных, однако опять же границы могут быть расширены и на класс нелинейных задач. Но в этом случае для отыскания оптимального решения необходимо использовать методы решения задач нелинейного программирования, например, градиентные методы.

По математическим свойствам рассмотренные задачи относятся к классу статистических задач принятия решений. Переменные могут быть как непрерывными (например, объем перевозимого топлива), так и целочисленными (например, число перевозимых контейнеров). С точки зрения содержания логистических операций они относятся к задачам транспортного типа [1].

Их содержательная постановка обычно связана с распределением некоторого груза в некоторой транспортной системе. Вместе с тем встречаются и другие постановки, связанные с логистикой в энергетических, информационных, финансовых и других системах.

В математической постановке транспортные задачи представляют, как и большинство задач, математического программирования, оптимизационные модели, включающие в свою структуру целевую функцию и систему ограничений. Большинство таких моделей являются задачами линейного программирования специального вида, наиболее простой из которых является классическая транспортная задача.

Так как транспортные задачи относятся к классу задач линейного программирования, то они могут быть решены с использованием симплекс-метода. Однако из-за наличия особенностей в системе ограничений этих задач для их решения были разработаны специальные методы. Так для построения опорного плана наиболее известными является метод северо-западного угла, метод наименьшей стоимости, метод Фогеля. Для улучшения опорного плана до оптимального обычно используется распределительный метод или метод потенциалов.

Вместе с тем, следует заметить, что решение любой реальной транспортной задачи немыслимо без применения компьютерных технологий. Поэтому, наряду с изучением существа самих методов, важным является овладение технологиями компьютерного моделирования реальных практических ситуаций.

Для решения транспортной задачи были разработаны два программных решения: программа TransportEmercom, разработанная в среде Delphi, и комплекс компьютерных ситуационных моделей в среде Excel [2, 3].

В программе TransportEmercom для нахождения опорного плана реализован метод северо-западного угла, а для его улучшения до оптимального – метод потенциалов.

В программе реализованы два способа ввода исходных данных. Первый способ предполагает заполнение табличной формы. Второй способ предполагает заполнение графической формы.

Главным достоинством разработанной программы является простота её использования, от пользователя не требуется знаний математического программирования. Вместе с тем, в процессе опытной эксплуатации программы был выявлен существенный недостаток – невозможность перенастройки программы под различные нестандартные практические ситуации, встречающиеся в транспортной логистике. Каждая новая ситуация требует доработки программы, что снижает её практическую ценность.

Кроме того, в «ФКУ ЦУКС СЗРЦ» сотрудники центра в качестве инструмента обработки информации в основном используют табличный процессор MS Excel. Отсюда возникла задача, разработки комплекса компьютерных моделей (шаблонов), позволяющих решить оптимизационные задачи планирования перевозок. При этом фокус внимания был смещен, именно, на моделирование различных практических ситуаций, встречающихся в деятельности МЧС.

Для нахождение оптимального решения использовалась программная надстройка MS Excel «Поиск решения». При этом отпадает необходимость написания программного кода для реализации того или иного математического метода, а фокус внимания смещается, именно, на моделировании практических ситуаций.

На базе шаблона сбалансированной транспортной задачи, разработаны шаблоны для двух вариантов несбалансированной задачи – дефицитной и профицитной; для задачи блокирования перевозки грузов по указанным маршрутам; для задачи перевозки грузов по заключенным договорам; для задачи перевозки грузов с учетом неприкосновенных запасов; для задачи обеспечения ресурсами с учетом приоритетов; модель пропорционального распределения ресурсов в условиях дефицита.

Масштабность модели может быть легко расширена за счет добавления строк (складов) и столбцов (пожарно-спасательных частей).

В рамках транспортной логистики системы МТО МЧС разработанные модели используются для перевозки грузов с учетом грузоподъемности транспортных средств, многопродуктовых перевозок, перевозки с организацией промежуточных пунктов и другие.

Литература:

1. Развитие экономико-математического инструментария решения управленческих задач в оборонно-промышленном комплексе / Батьковский А.М., Трофимец В.Я., Трофимец Е.Н. Радиопромышленность. 2016. № 2. С. 129-142.

2. Совершенствование управления оборонно-промышленным комплексом / Батьковский А.М., Фомина А.В., Батьковский М.А., Калачихин П.А., Клочков В.В., Леонов А.В., Пронин А.Ю., Семенова Е.Г., Стяжкин А.Н., Тельнов Ю.Ф., Трофимец В.Я., Трофимец Е.Н.. Под редакцией А.М. Батьковского, А.В. Фоминой. Центральный научно-исследовательский институт экономики, систем управления и информации "Электроника". Москва, 2016.

3. Информационно-аналитические технологии в системе подготовки специалистов для силовых структур и обороннопромышленного комплекса / Батьковский А.М., Крюкова М.С., Трофимец Е.Н.. Радиопромышленность. 2016. № 1. С. 117-126.

Трофимец Е.Н., Лебедев А.Ю., Крупкин А.А., Шилов А.Г.
Санкт-Петербургский университет
государственной противопожарной службы МЧС России

ДИСТАНЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ИЗУЧЕНИИ ДИСЦИПЛИН МАТЕМАТИЧЕСКОГО ЦИКЛА САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА ГПС МЧС РОССИИ

Одним из важных результатов применения информационно-коммуникационных технологий (ИКТ) в сфере образования является дистанционное обучение.

Под дистанционными образовательными технологиями (ДОТ) понимаются образовательные технологии, реализуемые в основном с применением информационных и телекоммуникационных технологий при опосредованном (на расстоянии) или не полностью опосредованном взаимодействии обучающегося и педагогического работника.

Одним из самых актуальных и перспективных направлений при подготовке к вступительным испытаниям в вузы МЧС России в век информационных технологий является дистанционное обучение. Использование в образовании дистанционных технологий предполагает заочное обучение абитуриентов, удаленных территориально от местонахождения учебного заведения и обучающихся с использованием телекоммуникационных технологий через интернет.

Целью использования ДОТ образовательным учреждением является предоставление обучающимся возможности освоения образовательных программ непосредственно по месту жительства обучающегося или его временного пребывания (нахождения).

Появлению технологии дистанционного обучения способствовало развитие различных средств передачи информации на расстоянии. Основоположником данной педагогической технологии принято считать англичанина Исаака Питмана, который в 1840 году начал обучать студентов стенографии с помощью почтовых отправлений.

Основными задачами ДОТ являются:

- удовлетворение потребностей общества и государства в квалифицированных специалистах с высшим и средним профессиональным образованием;
- удовлетворение потребности личности в получении образования;
- повышение качества образования путем внедрения современных технологий, при которых целенаправленное опосредованное или не полностью опосредованное взаимодействие обучающегося и преподавателя осуществляется независимо от места их нахождения и распределения во времени на основе использования средств телекоммуникации.

Преимущества использования ДОТ:

- качественное образование на основе современных информационных технологий;
- возможность повышать образовательный уровень по месту жительства;
- доступность образовательных услуг и информационных ресурсов в любом месте (в т.ч. по месту жительства) и в любое время;
- самостоятельный выбор интенсивности обучения;
- постоянная связь с преподавателем, индивидуальное консультирование;
- техническая поддержка при работе с компьютерным оборудованием.

Основные виды дистанционных образовательных технологий можно разделить на три группы: кейсовая технология, сетевые технологии, телекоммуникационная (информационно-спутниковая) технология [1, 2].

Кейсовая технология – дистанционная образовательная технология, основанная на предоставлении обучающимся информационных образовательных ресурсов в виде специализированных наборов учебно-методических комплексов, предназначенных для самостоятельного изучения с использованием различных видов носителей информации.

Сетевые технологии – дистанционная образовательная технология, основанная на предоставлении обучающимся информационных образовательных ресурсов в виде специализированных наборов учебно-методических комплексов, предназначенных для самостоятельного изучения с использованием различных видов носителей информации.

Телекоммуникационная (информационно-спутниковая) технология – дистанционная образовательная технология, основанная на использовании преимущественно космических спутниковых средств передачи данных и телевещания, а также глобальных и локальных сетей для обеспечения доступа обучающихся к информационным образовательным ресурсам, представленным в виде цифровых библиотек, видеолекций и других средств обучения.

ДОТ позволяют создать ряд методов адаптации обучения к потребностям трудовой деятельности обучаемых. Преимущества подготовительных курсов в формате online для абитуриентов заключается в возможности выбрать удобное время и место для обучения, а также собственный темп освоения курса; возможность готовиться к поступлению с преподавателями университета.

На подготовительных курсах в формате online абитуриент развивает необходимые навыки самообучения, что служит дополнительным критерием для принятия его на образовательную программу.

В Санкт-Петербургском университете ГПС МЧС России на базе лаборатории электронного обучения и дистанционных образовательных технологий разрабатываются и создаются открытые онлайн-курсы. О важности и перспективности данного направления работы уже давно говорится на всех уровнях государственной власти.

С целью апробации технологии массового обучения предлагается проект подготовительных курсов по высшей математики и математики в формате онлайн.

На подготовительном этапе была проведена работа по опросу потенциальных абитуриентов о необходимости проведения подготовительных курсов. Опрос проводился посредствам групп в социальных сетях, официального сайта университета и сайта представительства в г. Тюмень. Также эта работа велась в формате телефонных консультаций абитуриентов.

В ходе опроса были заданы три основных вопроса:

1. «Какое образование планирует получать абитуриент – первое или второе высшее?». 77% опрошенных планируют получать первое высшее образование;

2. «Предпочтительный формат обучения на подготовительных курсах?». 60% респондентов предпочитают онлайн-обучение взамен классического.

3. «Актуальные дисциплины на online курсах?». Для поступающих на первое высшее образование приоритетными дисциплинами являются Математика, Физика, Русский язык. Для абитуриентов поступающих на второе – Высшая математика.

В Санкт-Петербургском университете ГПС МЧС России дисциплины «Высшая математика» и «Математика» являются профилирующими экзаменами на вступительных испытаниях при подготовке технических, экономических, психологических кадров МЧС России.

Реализация данного проекта позволяет повысить уровень общеобразовательной подготовки абитуриентов, а также, в целом, повысить эффективность довузовской работы в Университете.

Для успешного внедрения дистанционного обучения следует учитывать три интегративных фактора:

- технологический, который определяется информационными технологиями, используемыми для разработки, доставки, поддержки учебных курсов;

- педагогический, который определяется набором методов и приемов, используемых в ходе учебного процесса;

- организационный, характеризующий специфику организационной структуры образовательного учреждения, использующего дистанционное обучение.

Актуальность высшей математики и математики связана с оперативной оценкой обстановки и предупреждением чрезвычайных ситуаций, в условиях риска и неопределенности; с вопросами принятия объективных и взвешенных решений.

Прогнозирование и изучение опасных техногенных и природных событий требуют от специалиста МЧС России знаний инструментальных методов высшей математики. Они являются средствами предельно четкой формулировки понятий и проблем в области предупреждения и ликвидации последствий природных и техногенных катастроф на территории РФ с учетом поставленных целей и задач МЧС России.

С точки зрения нормативного обеспечения, Университет обладает всеми необходимыми правами и локальными актами для реализации подготовительных курсов.

Во-первых: это Лицензия на осуществление образовательной деятельности, где в приложении 1.2. в разделе Дополнительное образование, указано право реализации Дополнительного образования детей и взрослых.

Во-вторых: это Устав Санкт-Петербургского университета ГПС МЧС России, где во втором разделе «Цели и виды деятельности» в пп. 2.4. указано, что Учреждение в установленном порядке осуществляет по договорам с Ю и Ф лицами на возмездной основе следующие, приносящие доход виды деятельности, не являющиеся основными – предоставление дополнительных образовательных услуг (обучение по дополнительным образовательным программам, обучение на подготовительных отделениях).

Таким образом, соблюдаются все требования законодательства в области реализации подготовительных курсов.

Для регламентирования порядка работы подготовительных курсов подготовлены два локальных акта:

1. Стандарт организации – Положение о подготовительных курсах;

2. Дополнительные общеразвивающие программы (ДОП) по Высшей математике и Математике.

Главная цель реализации программ заключается в восстановлении и формировании систематизированных знаний, умений и навыков в области высшей математики и математики, необходимых для сдачи вступительных экзаменов.

Принципы построения (ДОП):

- применение современных образовательных технологий, инновационных методов обучения на основе массовых онлайн-курсов;

- возможность формирования индивидуальной траектории обучения;

- использование информационных и коммуникационных технологий, в том числе современных систем технологической поддержки процесса обучения, обеспечивающих комфортные условия для обучающихся, преподавателей;

- применение электронных образовательных ресурсов (дистанционное, электронное, комбинированное обучение).

Порядок реализации образовательных услуг определен на условиях публичной оферты.

Почему возникла необходимость использования публичной оферты в рамках данного проекта?

В соответствии со ст. 437-438 Гражданского кодекса публичная оферта или предложение позволяет исключить такие трудо- и время затратные этапы договорной работы, как подписание, согласование, финансовая и юридическая экспертиза, а также почтовая рассылка копий договора.

Таким образом, минимизируются трудозатраты на заключение договоров и потребитель образовательной услуги после регистрации и оплаты может в кратчайшее время приступить к обучению.

Какова же схема заключения договоров на условиях публичной оферты?

1. Ознакомившись с качеством образовательной услуги и заполнив регистрационную форму на сайте, пользователь принимает условия опубликованной оферты.

2. На втором этапе пользователю предлагается оплатить выбранную образовательную услугу путем безналичного платежа на расчетный счет Университета.

В соответствии с указанными статьями Гражданского кодекса выполнение первых двух условий со стороны Заказчика является Акцептом публичной оферты, или иными словами процедурой подписания договора.

С момента акцепта Заказчиком настоящей оферты данная оферта считается «классическим» Договором об оказании платных образовательных услуг.

3. После регистрации и оплаты выбранного курса, на электронную почту Заказчика отправляется приглашение на курс и пользователь получает образовательную услугу.

Со стартовой страницы электронной информационно-образовательной среды Санкт-Петербургского университета ГПС МЧС России или по ссылке с информационных источников (соцсети, реклама), абитуриент переходит в раздел подготовительных курсов. На странице подготовительных курсов представлены их цели и задачи, преимущества формата онлайн-обучения, а также порядок записи на курс.

Каталог подготовительных курсов реализован в формате витрины курсов с указанием основной информации по стоимости и направлению подготовки, а также возможностью просмотра рекламного промовидео курса.

При переходе по ссылке «Подробная информация», абитуриент попадает на страницу выбранного подготовительного курса, где может ознакомиться с полной информацией о курсе, а также с качеством и форматом обучения, о чем говорилось ранее.

Аннотация курса включает в себя вступительное слово преподавателя в рамках которого, преподаватель знакомит потенциальных слушателей с порядком обучения на курсе.

Если после знакомства с курсом у абитуриента остались вопросы, он всегда может заказать звонок сотрудника университета для подробных разъяснений.

В случае, если пользователя устраивает качество предоставляемой услуги, ему предлагается заполнить регистрационную форму записи на курс.

При заполнении регистрационной формы необходимо внести сведения о Заказчике и Обучающемся, а также принять необходимые и обязательные условия.

В данном случае, это:

- Заказчику исполнилось 18 лет и более;
- Заказчик ознакомлен и согласен с условиями публичной оферты.

После принятия условий пользователю предлагается подать заявку и оплатить выбранный курс.

Оплата производится с помощью сервиса онлайн-оплаты Университета.

После получения заявки и денежных средств на расчетный счет Университета, издается приказ о зачислении и слушателю отправляется приглашение на курс для обучения.

Курс включает в себя основные разделы дисциплины «Высшая математика» для подготовки письменного вступительного экзамена в магистратуру.

Курс представляет собой структурированный набор видеолекций и конспектов с кратким изложением теоретических вопросов и подробным рассмотрением решения типовых практических примеров (Plus usus sine doctrina, quam citra usum doctrina valet / Практика без теории ценнее, чем теория без практики).

Нормативная трудоемкость обучения по программе, включая самостоятельную работу слушателей – 36 академических часов; длительность – 4 недели; недельная нагрузка – 9 часов.

Форма обучения – заочная с применением электронного обучения, дистанционных образовательных технологий в объеме, предусмотренном учебно-тематическим планом.

В результате обучения слушатели восстанавливают основные понятия, методы и теоремы курса высшей математики для решения тестовых заданий на вступительном экзамене. Восполняют основные знания по высшей математики для освоения магистерской программы по направлениям подготовки 27.04.03 «Системный анализ и управление», 20.04.01 «Техносферная безопасность».

Курс позволяет слушателям восполнить некоторые компетенции: способность обладать математической культурой, как частью профессиональной и общечеловеческой культуры; способность проводить доказательства утверждений, как составляющей когнитивной и коммуникативной функции; способность анализировать, интерпретировать и представлять результаты исследований; способность использовать аппарат высшей математики для описания моделей различных явлений и процессов в области пожарной безопасности; способность использовать аппарат высшей математики при выборе методов (систем) защиты человека и среды обитания, ликвидации чрезвычайных ситуаций применительно к конкретным условиям.

Возможные направления ДОТ: мультимедиа-лекции и лабораторные практикумы; электронные мультимедийные учебники; компьютерные обучающие и тестирующие системы; имитационные модели и компьютерные тренажеры; консультации и тесты с использованием телекоммуникационных средств; видеоконференции; видео-лекции.

Дистанционное обучение является перспективным направлением и его развитие в системе образования продолжается.

Данный способ очень удобен для людей с ограниченными возможностями, не имеющих возможность покинуть место жительства или службы (работы).

Литература:

1. Ибрагимов И.М. Информационные технологии и средства дистанционного обучения / И.М. Ибрагимов – М.: «Академия», 2007. – 336 с.

2. Информационно-аналитические технологии в системе подготовки специалистов для силовых структур и обороннопромышленного комплекса / Батьковский А.М., Крюкова М.С., Трофимец Е.Н.. Радиопромышленность. 2016. № 1. С. 117-126

Фадеенко Д.В., Филипенко И.В.
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

ЭЛЕКТРОННОЕ ОБУЧЕНИЕ КАК ВАЖНЕЙШАЯ СОСТАВЛЯЮЩАЯ СОВРЕМЕННОГО ОБРАЗОВАНИЯ

Особенностью современного общества является значительная роль информационных технологий во всех сферах жизни. Не исключение и сфера образования. Возникает потребность получения информации в различных видах, в любое время и в любом месте. Происходят существенные изменения в методиках обучения как при изучении теоретического материала, так и при проведении практических занятий [1].

Особое внимание уделяется переходу образовательного процесса от обычных форм к электронному обучению. Под электронным обучением, согласно [2], понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и

обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников.

Интернет-образование на сегодняшний день можно отнести к одной из самых динамически развивающихся областей образования, об этом свидетельствуют многочисленные международные и национальные образовательные программы [3].

Реализуется электронное обучение на базе так называемой электронной среды или платформы, представляющей собой персональную страницу, с которой пользователь получает доступ к учебным материалам и заданиям [4].

К достоинствам внедрения таких систем можно отнести следующее [5]:

– материалы курса находятся в постоянном доступе (выкладываются лекции, литература, интерактивные презентации, ссылки на электронные ресурсы, кроме того могут создаваться видеолекции, задания в виде тестов и др.);

– возможность создания различных интерактивных форм обучения, представление информации тяжелой для понимания в более наглядном и привычном виде, все это позволяет повысить интерес обучающихся;

– возможность самостоятельной работы обучающихся, при этом могут устанавливаться сроки выполнения задания, автоматически выполняться проверка и ставиться оценка;

– проведение промежуточной оценки знаний обучающихся в виде тестов и/или заданий;

– легкое и быстрое обновление теоретической информации и внесение изменений в задания;

– возможность настройки процесса обучения под свои запросы и нужды;

– при использовании электронных технологий снижается роль стрессовых факторов в процессе выполнения заданий, сдачи зачетов и экзаменов, повышается уровень психологического комфорта;

– возможность учитывать индивидуальные особенности каждого обучающегося, данный вид обучения подходит для людей с ограниченными возможностями;

– экономия на оснащении и содержании учебных помещений.

Благодаря современным информационным технологиям электронное обучение является удобным, гибким и насыщенным информацией различного формата процессом передачи знаний. При этом процесс обучения может проходить 24 часа в сутки и 365 дней в году без каких-либо ограничений, требуется только выход в интернет.

Кроме достоинств применения таких систем в сфере образования, стоит отметить и их недостатки. Сюда можно отнести отсутствие у обучающихся группового взаимодействия, нет возможности обмениваться мнениями и точками зрения. Однако этот недостаток может быть устранен путем реализации разнообразных групповых учебных проектов и применением в них таких видов деятельности, как обсуждение на форуме, чате, в социальных сетях, проведение видеоконференций и т.п.

Еще одной проблемой может стать мотивация обучающихся, ведь электронное обучение по большей части рассчитано на самостоятельное изучение материала. В данной проблеме существенную роль играет преподаватель, который должен преподносить знания таким образом, чтобы это было информативно и интересно для обучающихся.

По моему мнению, в настоящее время даже самые ярые противники и критики электронного обучения не смогут не отрицать пользы внедрения таких систем в качестве дополнительного или самостоятельного инструмента обучения.

Электронное обучение пока не может являться эталоном, но за счет своих достоинств, возможности постоянного развития и совершенствования, уже сейчас способно улучшить процесс обучения, сделать его интересней, наглядней, информативней и принести больше знаний.

Литература:

1. Алексахина Н.В., Бойцова Е.Г., Чичев Е.М., Организация образовательного процесса средствами сетевых технологий // Управление качеством образования. – 2014. – № 3. – С. 58-67.

2. Федеральный закон «Об образовании в Российской Федерации» [Текст]. – М.: Омега – Л., 2014. – 134 с.

3. Наумова И.М., Поначугин А.В. Сравнительный анализ эффективности традиционных и дистанционных образовательных технологий. Сборник «Учиться и жить вместе: современные стратегии образования лиц с ограниченными возможностями здоровья». Международная научно-практическая конференция ЮНЕСКО / Под редакцией Н.М. Прусс, Ф.Г. Мухаметзяновой. – 2014. – С. 97-101

4. Кошелев Д.А., Частиков А.П., Дейкун Д.Г., Шевцова К.Г., Полусмак В.И., Бородовицина Т.К., Арутюнян Т.В., Программно–аппаратное обеспечение обучающихся и самообучающихся нейросетей / Международный научно-исследовательский журнал «Успехи современной науки». – 2016. –№8.– С. 21-23

5. Карманов М.В., Малахова О.А. Электронное обучение как благо современного общества // Проблемы современного образования. – 2015. – № 3. – С. 122-127

Халиуллин А.И.
Научно-исследовательский институт
Университета прокуратуры Российской Федерации

ОКАЗАНИЕ УСЛУГ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИМИ ОРГАНИЗАЦИЯМИ УЧАСТНИКАМ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Развитие информационных технологий привело к их широкому вовлечению в орбиту уголовно-правовых отношений. В условиях опережающего развития способов совершения преступлений в сфере компьютерной информации по отношению к механизмам обеспечения информационной безопасности уровень развития отечественного законодательства не в полной мере соответствует угрозам, о чем, в частности, свидетельствует высокий уровень латентности названой категории преступлений.

Угрозу соблюдению прав человека в сети «Интернет» представляют, как мы полагаем, не согласованные действия правоохранительных органов различных государств и коммерческих компаний в сфере информационной безопасности по борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий. В этой хаотичной борьбе с преступностью в сети «Интернет» страдают не только отдельные люди, но так и целые коммерческие компании. Например, введен запрет на использование антивируса Касперского в США и Великобритании из-за того, что он по версии государственных органов данных стран использовались в целях несанкционированного сбора информации на их территории спецслужбами Российской Федерации. В подобных условиях стремясь избежать участия в качестве «третьей стороны» в информационных конфликтах между различными государствами коммерческие технологические компании однозначно декларируют основой собственной деятельности безопасность и стабильность сетевого пространства и единство подходов в обеспечении защиты прав человека при оказании услуг по всему миру.

Российская Федерация осуществляет активное участие в международном правотворческом процессе, обобщенная позиция Российской Федерации основывается на уважении «цифрового» суверенитета и защите прав человека в сети Интернет. Вместе с тем, даже в законодательстве Российской Федерации вопрос предоставления услуг коммерческими компаниями в сфере информационной безопасности параллельно уголовному судопроизводству остается не урегулированным.

В ряде регионов России возможность проведения компьютерно-технических экспертиз носит ограниченный характер по объективным причинам – высокая загруженность, недостаточное количество экспертов и отсутствие необходимых технических средств для производства экспертиз отдельных видов технических устройств. Изменчивость как свойство компьютерной информации определяет необходимость обеспечения законности и своевременности производства необходимых процессуальных действий, направленных на исследование фактов в ходе осуществлении проверки сообщений о компьютерном преступлении, не допуская нарушения принципа разумности уголовного судопроизводства. В целях преодоления сложившейся ситуации для производства экспертных исследований привлекаются представители научных и образовательных учреждений.

Вместе с тем в большинстве регионов России не рассматриваются все возможные варианты при назначении и проведении компьютерно-технических судебных экспертиз (исследований), например, существует возможность использования экспертных компетенций сотрудников Торгово-промышленной палаты Российской Федерации и ее территориальных подразделений; Центра реагирования на компьютерные инциденты в органах государственной власти России и его региональных представительств; Центра мониторинга реагирования на компьютерные атаки в финансовой сфере (Fin-cert) Центрального банка Российской Федерации и его региональных представительств; коммерческих центров реагирования на компьютерные атаки (лаборатория Касперского, Group-Ib, Positive Technologies и другие).

Привлечение негосударственных экспертных учреждений либо специалистов коммерческих организаций в сфере информационной безопасности к производству судебных экспертиз (исследований) с одной стороны требует в соответствии с частью 2 статьи 195 УПК РФ подтверждения наличия специальных знаний, с другой стороны по своему содержанию и применяемому исследовательскому инструментарию может находиться в пограничной зоне между судебной экспертизой (исследованием) и одновременно обладать некоторыми признаками оперативно-розыскных мероприятий (например, получение компьютерной информации).

Характерный пример, согласно информации официального сайта компании специалистами Group-IB оказывает на возмездной основе следующие категории услуг в сфере информационной безопасности: компьютерно-техническая экспертиза; криминалистические исследования; сбор цифровых доказательств; исследование вредоносных программ; аутсорсинг и независимая экспертиза; взаимодействие с правоохранительными органами.

В настоящее время специализированный нормативный акт, регулирующий деятельность компаний в сфере информационной безопасности отсутствует и их деятельность в анализируемой сфере не лицензируется, тем не менее последствия оказания ими информационно-поисковых, аналитических, экспертных и других услуг могут привести к утрате либо модификации компьютерной информации (в том числе хранящейся на электронных носителях за границей), имеющей значение для решения вопроса о возбуждении уголовного дела.

Кроме того, оказание «информационно-поисковых услуг» либо «предоставление сведений» представителями интернет-сервисов, с помощью которых осуществляется

передача электронных сообщений (mail.ru, rambler.ru, google.ru и другие), также не может быть признано законными.

К примеру, в постановлении Конституционного суда Российской Федерации от 26.10.2017 указано, что «не может рассматриваться как наделяющее правообладателя интернет-сервиса, с помощью которого осуществляются передача электронных сообщений и хранение информации, статусом обладателя информации в отношении сведений, содержащихся в сообщениях, получаемых или отправляемых пользователями по электронной почте, или в отношении информации, которую пользователи хранят с помощью данного интернет-сервиса».

Негативные последствия получения подобным образом сведений на стадии возбуждения уголовного дела могут иметь место в последующем при его расследовании, так как доказательства по делу будут признаны недопустимыми в случае их получения в нарушение положений процессуального законодательства Российской Федерации, так и в случае их получения с нарушением Конвенции или Протоколов к ней в толковании Европейского Суда, прямо запрещающих необоснованное ограничение права на тайну телефонных и иных переговоров.

Необходимо отметить, что в соответствии с п. 7 ст. 3 Закона Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации»[2]: «сбор сведений по уголовным делам на договорной основе с участниками процесса. В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом лицо, производящее дознание, следователя или суд, в чьем производстве находится уголовное дело».

В этой связи полагаем, что необходимо дополнить УПК РФ статьей 21^2, указав, что «в случае, если потерпевший, свидетель, подозреваемый, обвиняемый, подсудимый, их законные представители или защитники (адвокаты) привлекают лиц для поиска, сбора либо анализа информации, имеющей отношение к разрешаемому органами предварительного расследования сообщению о преступлении либо расследуемому уголовному делу, осуществляемой в том числе с использованием информационных поисковых технологий, должны об этом незамедлительно в письменной форме уведомить лицо, производящее дознание, предварительное расследование или суд, в чьем производстве находится уголовное дело».

Литература:

1. DHS Statement on the Issuance of Binding Operational Directive 17-01 // https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01 (дата доступа 02.01.2018).

2. UK spying fears spark Russian software ban. // https://www.ft.com/content/d323c458-d6a4-11e7-8c9a-d9c0a5c8d5c9 (дата доступа 02.01.2018).

3. Временный регламент передачи данных участниками информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (версия 2.0) // URL: http://www.cbr.ru (Дата обращения 01.02.2018).

4. Выступление Заместителя Секретаря Совета Безопасности Российской Федерации на конференции ОБСЕ по кибербезопасности, 03.11.2017 // http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2938933 (дата доступа 02.01.2018).

[2] Расследование высокотехнологичных преступлений Group-Ib // URL: https://www.group-ib.ru/investigation.html (Дата обращения 01.02.2018).

5. Закон Российской Федерации от 11.03.1992 № 2487-1 (ред. от 05.12.2017) «О частной детективной и охранной деятельности в Российской Федерации» // СПС «Гарант».

6. Заявление о ценностях, бизнесе, решениях и сервисах Лаборатории Касперского: // https://media.kaspersky.com/ru/about/Kaspersky_Lab_Profile.pdf (дата доступа 02.01.2018).

7. Постановление Конституционного суда Российской Федерации от 26.01.2017 по делу «О проверки конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // СПС «Гарант».

8. Постановление Пленума Верховного Суда Российской Федерации от 27.06.2013 № 21 «О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 04.11.1950 и Протоколов к ней» // Бюллетень Верховного Суда РФ. № 8. 2013.

9. Расследование высокотехнологичных преступлений Group-Ib // URL: https://www.group-ib.ru/investigation.html (Дата обращения 01.02.2018).

10. Резолюция о деятельности Microsoft по обеспечению соблюдения прав человека // https://www.microsoft.com/en-us/about/corporate-responsibility/CMSFiles/Microsoft-Global-Human-Rights-Statement-ru-ru.pdf?version=f7ae53ff-5df0-0c78-6d7e-5546d85be9a9 (дата доступа 02.01.2018).

11. Указ Президента Российской Федерации о 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СПС «Гарант».

12. Указание Генерального прокурора Российской Федерации от 25.06.2009 № 212/20 «Об организации исполнения соглашения о сотрудничестве между Генеральной прокуратурой Российской Федерации и торгово-промышленной палатой Российской Федерации».

Харченко А.В.
Кубанский государственный университет

ДИСТАНЦИОННЫЙ КОМПОНЕНТ КУРСА ОБУЧЕНИЯ ПРОГРАММИРОВАНИЮ БАКАЛАВРОВ ПРИКЛАДНОЙ МАТЕМАТИКИ

Современный молодой человек – первокурсник – постоянно находится в окружении инновационных информационных технологий, технологий мобильных устройств, автоматизированного поиска информации. Студенты прикладной математики в особенности, в силу профессиональной специфики, имеют навыки использования электронной почты, организации форумов и чатов различных форматов, работы с поисковыми системами. Подобные навыки необходимо использовать в процессе обучения. С одной стороны, изучая основы программирования, студенты-первокурсники будут совершенствовать компетенции общей компьютерной и информационной грамотности, находясь в привычной им среде. С другой стороны, введение дистанционного компонента в курс обучения программированию позволит расширить дидактические возможности изучаемой дисциплины [1].

Таким образом, актуальность работы определяется необходимостью внедрения дистанционного компонента в курс обучения программированию для расширения дидактических возможностей дисциплины.

Цель статьи состоит в раскрытии функций дистанционного компонента в курсе обучения программированию на примере конкретного учебного раздела.

Учебный курс "Основы программирования" предназначенный для бакалавров первого года обучения включает ряд основных разделов. Рассмотрим методику введения дистанционного компонента на примере раздела "Операторы цикла". Предварительно на лекционном занятии студентам предлагается ознакомиться с базовыми операторами цикла: циклом с предусловием, циклом с постусловием, циклом с заранее известным числом итераций. Приводятся примеры работы операторов, указываются их особенности. Далее по учебному материалу раздела проводится лабораторное занятие [2, 3].

Структура лабораторного занятия следующая. Отметим, что в содержании лабораторной работы учебный материал излагается в справочном формате, основной акцент делается на особенности применения операторов при решении задач.

Лабораторная работа №3. Операторы циклов

Цель работы:

- Изучить синтаксис и семантику оператора цикла с параметром, оператора цикла с предусловием, оператора цикла с постусловием.
- Выявить особенности применения этих операторов.
- Приобрести навыки использования операторов при решении задач.

Содержание лабораторной работы:

Оператор цикла с параметром имеет следующий синтаксис:

For i:=<начальное значение> to <конечное значение> do <оператор>

Оператор используется в том случае, когда количество итераций цикла заранее известно.

Пример 1. Дано целое число. Найти сумму его делителей.

```
Var a, s, i : integer;
Begin
Writeln(‘Введите число’);
Readln(a);
S:=0;
For i:=1 to a do
If a mod i =0 then s:=s+ i;
Writeln(s);
End.
```

Пример 2. Вычислить $\sum_{i=1}^{N} \frac{(-1)^i x^{2i+1}}{i!}$.

```
Var n, x, i, z, p, f : integer;
s:real;
Begin
Writeln(‘Введите числа n и x’);
Readln(n, x);
s:=0; z:=1; p:=x; f:=1;
For i:=1 to n do
begin
z:=z*(-1);
p:=p*x*x*x;
f:=f*i;
s:=s+(z*p)/f;
end;
Writeln(s);
```

End.

Оператор цикла с предусловием имеет следующий синтаксис:

While <условие> do <оператор>

Оператор используется в том случае, когда число итераций цикла заранее неизвестно. В этом операторе сначала проверяется истинность условия и, если условие истинно, выполняются операторы тела цикла.

Пример 3. Дано целое число. Найти сумму его цифр.

```
Var a, s : integer;
Begin
Writeln('Введите число');
Readln(a);
S:=0;
While a<>0 do
begin
s:=s+ a mod 10;
a:= a div 10;
end;
Writeln(s);
End.
```

Другим циклом с неизвестным заранее числом итераций является цикл с постусловием. Его синтаксис следующий.

Repeat <операторы> until <условие>

Этот цикл выполняется по крайней мере один раз и только после выполнения операторов тела цикла определяется истинность условия. Если условие истинно, выполняется завершение оператора цикла.

Пример 4. Дано целое число. Найти первую его цифру.

```
Var a : integer;
Begin
Writeln('Введите число');
Readln(a);
repeat
a:= a div 10;
until a < 10;
Writeln(a);
End.
```

Задания для самостоятельной работы в аудитории.

1. Даны числа x и y. Вычислить x^y.
2. Дано число. Верно ли, что у числа больше двух нечетных делителя (исключая 1 и само число)?
3. Определить является ли заданное число простым.
4. Построить N-е число Фибоначчи.
5. Дано целое число. Найти количество его цифр.
6. Дано целое число. Найти сумму его четных цифр.
7. Дано целое число. Найти произведение цифр «2» и «5», встречающихся в его записи.
8. Дано целое число. Является ли оно числом Фибоначчи.
9. Дано целое число. Верно ли, что в его записи нет нулей (использовать цикл с постусловием).

Домашние задания

1. Дано целое число. Вычислить его факториал.

2. Дано целое число. Найти произведение его делителей, делящихся на 3.
3. Определить является ли заданное число совершенным.
4. Дано два целых числа. Определить, являются ли они дружественными.
5. Дано целое число. Верно ли, что в числе нет двоек и троек?
6. Дано целое число. Верно ли, что в числе все цифры одинаковые?
7. Дано число. Найти сумму его нечетных цифр.
8. Дано целое число. Найти количество заданной цифры в числе (использовать цикл с постусловием).
9. Даны целых числа x и y. Вычислить x^y (для решения использовать цикл с предусловием и с постусловием).

Задания для самостоятельной работы выполняются студентом непосредственно на лабораторном занятии в компьютерном классе. Домашние задания относятся к самостоятельной внеаудиторной деятельности бакалавров.

На этом этапе изучения раздела дисциплины подключается дистанционный компонент курса. Студенты работают со Средой модульного дистанционного обучения КубГУ (www.moodle.kubsu.ru). Дисциплина составляет контент среды. Выбрав текущий раздел, студент может ознакомиться с дополнительными примерами использования операторов, загрузить выполненные домашние задания и получить дополнительную консультацию преподавателя. В Среде модульного дистанционного обучения КубГУ в рамках изучаемой дисциплины организован форум, на котором студенты могут задавать вопросы по учебному материалу, обсуждать решения и алгоритмы, как с преподавателем, так и между собой. Домашние задания оцениваются, кроме того существует функция обратной связи, т.е. преподаватель может оставить комментарий к решению, а студент имеет возможность изменить ответ, дополнив его или исправив.

Современные бакалавры не ограничены строгими часами консультации преподавателей. С помощью электронной почты работы студентов отправляются на поверку, в чатах социальных сетей, таких как ВК идет дополнительное обсуждение вопросов программирования.

Включение дистанционного компонента в курс обучения программированию существенно расширяет рамки дисциплины, предоставляя возможность студентам ознакомиться с дополнительным набором примеров алгоритмов, получить практическую консультацию преподавателя, обсудить решения на форуме. Общаясь посредством компьютерных технологий, в том числе и мобильных, студент находится в привычной ему среде, что снимает тревожность в общении с преподавателями, стресс при сдаче задания. Партнерские отношения студент-студент и студент-преподаватель, заложенные на первом году обучения, являются крепкой основой для будущих совместных творческих IT-проектов.

Литература:

1. Добровольская Н.Ю., Харченко А.В. Изучение программирования в программе бакалавриата на основе технологии конструирования учебных задач. // Современные технологии в образовательных системах: теория и передовой опыт.- 2016.- С. 185-187.

2. Добровольская Н.Ю., Харченко А.В. Применение информационных технологий в обучении. // Актуальные проблемы информационно-правового пространства.- 2017. - С. 28-31.

3. Добровольская Н.Ю. Формирование умения формального исполнения алгоритма как основы алгоритмических навыков учащихся. // Преподавание математики и информатики в школе и вузе.- 2017. - С. 56-58.

Швец Н.А., Майлатов И.С., Васин О.И, Щербаков В.А.
Краснодарское высшее военное училище
имени генерала армии С.М.Штеменко

ОБ ОДНОМ ИЗ СПОСОБОВ ПОВЫШЕНИЯ ТОЧНОСТИ ОПРЕДЕЛЕНИЯ КООРДИНАТ ОБЪЕКТОВ ГНСС ГЛОНАСС ПУТЕМ СКРЫТОЙ ПЕРЕДАЧИ КОРРЕКТИРУЮЩИХ СИГНАЛОВ

Глобальная навигационная спутниковая система (ГНСС) ГЛОНАСС необходима, в первую очередь, для оперативной навигации приземных подвижных объектов (сухопутных, морских, воздушных и низкоорбитальных космических). Она состоит из трех сегментов:

- орбитальной группировки (ОГ) навигационных космических аппаратов (НКА);
- наземного комплекса управления (НКУ);
- навигационной аппаратуры потребителей (НАП).

Данная система позволяет подвижному объекту посредством навигационной аппаратуры потребителей в любой точке приземного пространства определить свои координаты (три координаты) и скорость движения (три составляющих вектора скорости).

Орбитальная группировка системы ГЛОНАСС состоит из трех круговых геоцентрических орбит с высотой ~20000 км над поверхностью земли. На каждой из этих орбит располагается по 8 НКА (рисунок 1) [1].

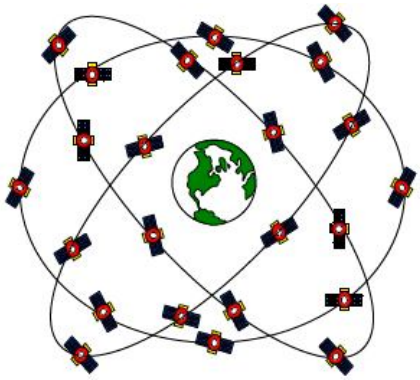


Рис. 1. Орбитальная группировка СРНС ГЛОНАСС

В НАП на подвижном объекте в сеансе навигации принимаются радиосигналы не менее чем от четырех видимых НКА и используются для измерения псевдодальностей и псевдоскоростей объекта. Результаты измерений и эфемеридная информация, принятых от каждого НКА, позволяют определить три координаты и три составляющие вектора скорости подвижного объекта. Благодаря использованию атомных стандартов частоты на НКА передается время атомных часов спутника, что позволяет определить смещение шкалы времени движущегося объекта относительно шкалы времени системы [2].

В связи с тем, что НКА только посылает радиосигналы на Землю, а отклика не получает, число пользователей не ограничено, т.е. одновременно принимать радиосигналы с навигационного космического аппарата может любое количество НАП.

Развитие глобальных навигационных спутниковых систем (ГНСС) привело к быстрому развитию новых спутниковых геодезических технологий. Все более совершенное спутниковое оборудование и средства связи, предлагаемые фирмами – производителями, позволили создать основу для развития новой технологии координатных определений, основанную на использовании сетей опорных (базовых) станций – технологию систем точного позиционирования (СТП).

Основой наземной инфраструктуры систем точного определения пространственных координат (позиционирования) с помощью ГНСС являются постоянно действующие базовые станции ГНСС. Постоянно действующие базовые станции устанавливаются в виде одиночных станций (рисунок 2) или нескольких базовых станций ГНСС, образующих сеть [3].

Рис. 2. Постоянно действующая базовая станция ГНСС.

Сеть, состоящая из большого числа постоянно действующих базовых станций, будет обеспечивать определение координат местоположения и скорости движущегося объекта на большой территории, с точностью от одного метра до нескольких сантиметров. Для этого ему необходимо принять дифференциальные поправки с базовой станции (или с сервера сети) и на месте вычислить координаты текущего местоположения. Такой способ спутниковых наблюдений называется измерением в режиме реального времени. При этом поправки можно получать по радиоканалу, каналам мобильной связи и через Интернет.

Любая постоянно действующая базовая станция включает в себя приемник ГНСС, управление работой которого осуществляется компьютером, расположенным на удалении от приемника. «Сырые» данные кодовых или фазовых спутниковых измерений передаются в память компьютера и записываются в файлы определенной длины. В зависимости от типа прикладной задачи длина файла может быть задана любым требуемым значением, от нескольких минут до часов или даже суток.

Специализированное программное обеспечение компьютера передает файлы по каналам связи на FTP сервер для обеспечения пользователям простого к ним доступа через Интернет. Такое программное обеспечение базовой станции может обрабатывать данные приемника ГНСС и предоставлять пользователю дифференциальные поправки в различных форматах (например, RTCM) с передатчика базовой станции по радиоканалам, высокоскоростным беспроводным сетям (GSM, GPRS, CDMA и др.) или через Интернет. Для определения координат и скоростей движущегося объекта в режиме реального времени с сантиметровой точностью расстояние от базовой станции до пользователя не должно превышать 25–30 км. В таком режиме работы одной базовой станции достаточно. Однако чтобы обеспечить необходимую точность получения пространственных координат на больших площадях и территориях может потребоваться целая сеть постоянно действующих базовых станций (рисунок 3).

Такая сеть состоит из нескольких постоянно действующих приемников ГНСС, подключенных к центру управления сетью по каналам связи, в качестве которых могут использоваться компьютерные сети, телефонные проводные линии, сотовая связь или глобальная сеть Интернет. Сервер с программным обеспечением для работы с базовыми станциями может управлять всей сетью базовых станций, включающей несколько сотен приемников ГНСС, при этом для каждого приемника отдельный компьютер не требуется. Он, как правило, размещается в едином вычислительном центре.

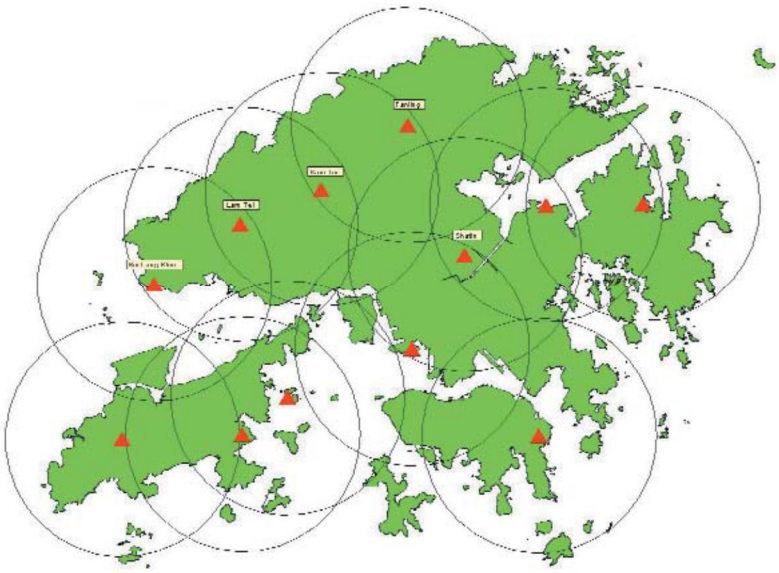


Рис. 3. Сеть постоянно действующих базовых станций на территории Гонконга.

Программное обеспечение базовой станции управляет спутниковым приемником, направляет данные для их последующей обработки, формирует RTK и DGPS поправки, которые передаются пользователям подвижных приемников. Сеть базовых станций, являющаяся основой системы точного позиционирования, включает следующие каналы связи:

– между спутниковыми приемниками базовых станций и компьютером (сервером) центра управления;

– между сервером центра управления и подвижными приемниками пользователей для работы в поле в режиме реального времени;

– между сервером центра управления и персональными компьютерами пользователей для приема и передачи данных, которые необходимы для постобработки.

Каждый из указанных каналов связи может быть создан на основе различных типов соединений:

1. Напрямую, с помощью кабеля, посредством последовательного интерфейса RS232.

2. По локальной компьютерной сети с использованием протокола TCP/IP.

3. По сети Интернет с использованием протокола TCP/IP.

4. С помощью различных типов модемов – радио, GSM, CDMA и т. п.

Но, как показывает практика, для большинства задач, требующих точного определения пространственных координат и скоростей движущегося объекта целесообразно использовать сеть Internet (рисунок 4). Это, в свою очередь, накладывает определенные ограничения и требует принятия дополнительных мер защиты. Например, для решения военных задач пользователи должны быть уверены в том, что информация, передаваемая по Internet через зарубежные сервера, не будет перехвачена и изменена.

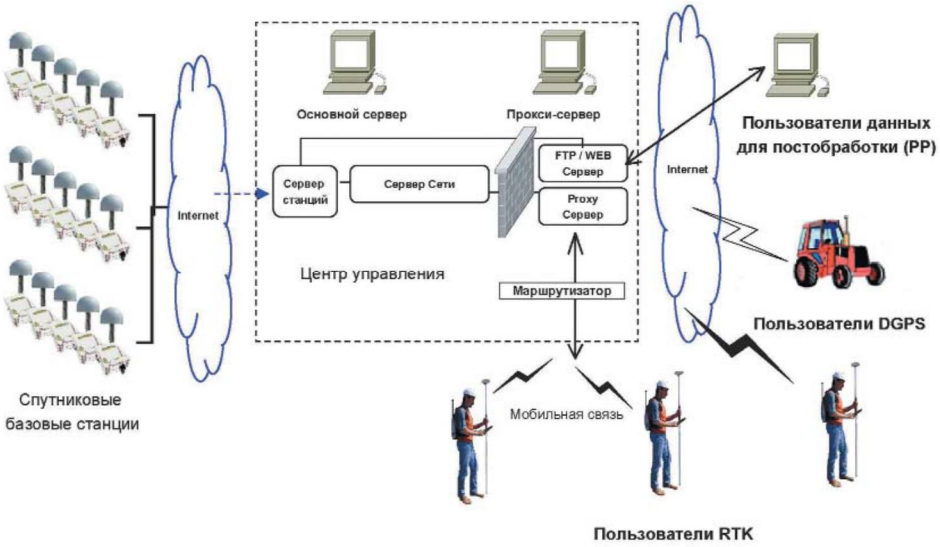


Рис. 4. Сервер и система коммуникации в сети спутниковых базовых станций.

Для решения этой проблемы предлагается использовать криптозащищенные туннели. Туннель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений. То есть, со стороны отправителя и получателя устанавливаются криптомаршрутизаторы, они позволяют шифровать данные перед отправкой, и расшифровывать их непосредственно только у получателя, а так же оповещать пользователя о подмене данных, если таковая имела место быть [4].

Для доставки конфиденциальных данных из одной точки в другую через сети общего пользования используются различные протоколы, отличающиеся степенью защиты. Такие протоколы как L2TP, PPTP, IPSec и т.п.

Рассмотренные протоколы возможно использовать при защищенном сеансе связи. Каждый из них предоставляет различный уровень информационной безопасности. Протокол L2TP поверх IPSec является наиболее предпочтительным. Система IPSec прочно занимает лидирующие позиции в наборе стандартов для создания VPN. Этому способствует ее открытое построение, способное включать все новые достижения в области криптографии. IPSec позволяет защитить сеть от большинства сетевых атак, «сбрасывая» чужие пакеты еще до того, как они достигнут уровня IP на принимающем компьютере. В защищаемый компьютер или сеть могут войти только пакеты от зарегистрированных партнеров по взаимодействию. Благодаря использованию IPSec в режиме туннелирования, осуществляется шифрование всего пакета, включая заголовок сетевого уровня. Данный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Таким образом, в результате использования базовых станций и скрытой передачи корректирующих сигналов движущийся объект, любого назначения, способен определить свои координаты и скорость с точностью до нескольких сантиметров, не опасаясь при этом, что данные будут подменены или получены сторонними пользователями.

Литература:

1. Навигационная аппаратура потребителя спутниковых радионавигационных систем: Учеб. пособие для вузов связи / В. К. Снежко, С. А. Якушенко, А. Д. Мальцев, С. А. Бондаренко. – СПб.: ВАС, 2011. – 216 с.

2. Навигационная аппаратура потребителей ГЛОНАСС/GPS: учебное пособие / В.С. Бахолдин, И.С. Герасименко, В.А. Добриков, В.Ф. Иванов, И.В. Сахно, Е.А. Ткачев. - СПб.: ВКА имени А.Ф. Можайского, 2016. - 98 с.

3. Наземная инфраструктура ГНСС для точного позиционирования. О.В. Евстафьев / Под ред. В.В. Грошева. – М.: ООО «Издательство «Проспект», 2009. – 48 с.

4. Система обмена информацией в электронном виде вооруженных сил российской федерации. Часть 1. Общие положения по построению системы обмена информацией в электронном виде вооруженных сил Российской федерации: Учеб. пособие / Под ред. О. В. Рисмана. – СПб.: ВАС, 2011. – 3108 с.: ил.

Швец Н.А., Майлатов И.С., Васин О.И., Щербаков В.А.
Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

ОПРЕДЕЛЕНИЕ МЕСТА ПОДВЕСА ОКСН НА ОПОРАХ ЛЭП

ОКСН - оптический самонесущий неметаллический кабель. Он представляет собой стеклопластиковый стержень (1) в центре, вокруг которого, переплетаясь между собой, вьются оптические волокна (2) (рисунок 1). Эти волокна находятся под несколькими слоями защиты, а именно: модуль из полибутилентерефталата или полиамида (3), гидрофобный гель (4), полимерная оболочка (5), армирующие элементы (6).[1]

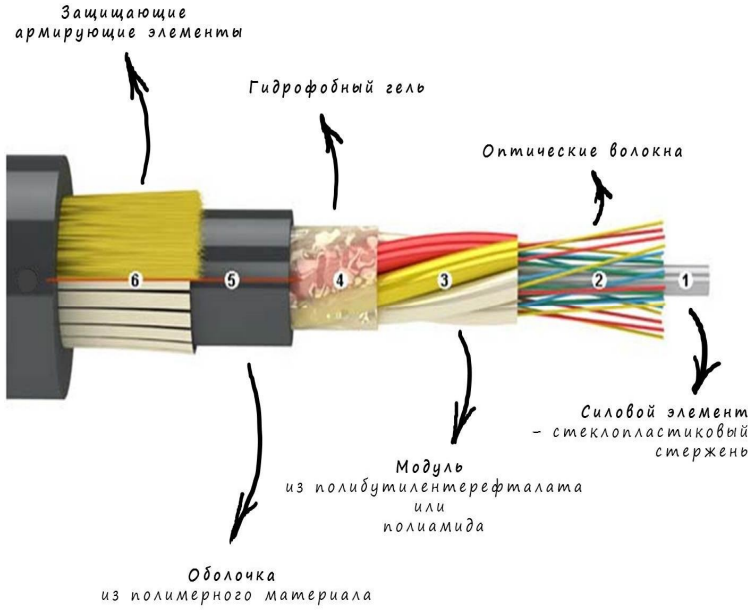


Рис. 1. Структура ОКСН

Такая структура оптоволоконного кабеля позволяет подвешивать его на опорах воздушных линий электропередач, но в соответствии с п.2.5.197 из [2], место крепления ОКСН на опоре с учетом его вытяжки в процессе эксплуатации определяется, исходя из условий:

- стойкости оболочки к воздействию электрического поля;
- обеспечения наименьшего расстояния до поверхности земли не менее 5 метров независимо от напряжения ВЛ и вида местности;

- обеспечения расстояний от ОКСН до фазных проводов на опоре не менее 0,6 м для ВЛ до 35 кВ; 1 м - 110 кВ; 1,5 м - 150 кВ; 2 м - 220 кВ; 2,5 м - 330 кВ; 3,5 м - 500 кВ; 5 м - 750 кВ при отсутствии гололеда и ветра.

С учетом указанных условий ОКСН может размещаться как выше фазных проводов, так и между фазами или ниже фазных проводов.

Связано это с тем, что в результате воздействия электрического поля ВЛ на оболочку ОКСН возникают скользящие по загрязненной поверхности диэлектрической оболочки электрические разряды (трекинговые токи). Они возникают под действием разности потенциалов (рисунок 2) между заземленной точкой крепления оптического кабеля на опоре и его частью в пролете. Протекание тока по поверхности ОКСН приводит к нагреву оболочки и в дальнейшем к возникновению трещин, обрывов линии связи.

Допустимая величина потенциала электрического поля согласно [4] составляет 12 - 25 кВ.

Таким образом, возникает потребность в расчете электрического поля вокруг проводов ЛЭП для определения величины наводимого потенциала, которая будет влиять на место подвеса ОКСН. Существует определенная упрощенная методика проведения таких расчетов.

Упрощенная методика определения места подвеса оптоволоконного кабеля заключается в расчете полей электрических потенциалов вокруг проводов ЛЭП в середине пролета и у опоры. Это связано с тем, что провода имеют провис, который в свою очередь влияет на картину поля и, в конечном итоге, на место подвеса ОКСН.

При определении места подвеса оптоволоконного кабеля на опорах ЛЭП по упрощенной методике вводится ряд некоторых допущений, а именно:

- не учитывается влияние опор;

- провода задаются в виде тонкой нити, поскольку расстояние от провода до места расчета гораздо больше размеров самого провода.

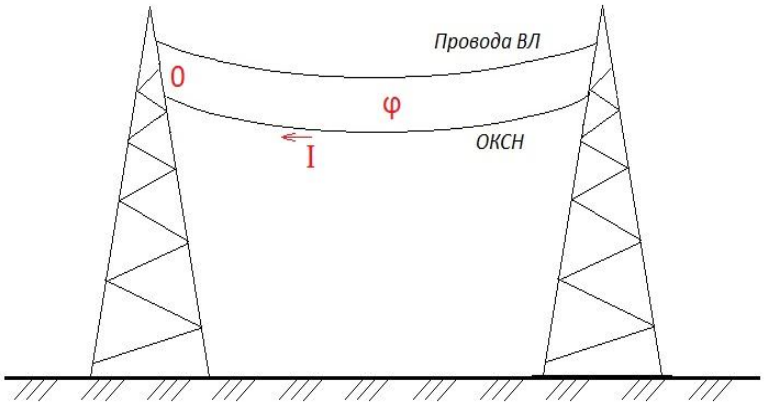


Рис. 2. Протекание тока по ОКСН под действием наведенного потенциала

Расчет обычно производится численным методом в одном из нескольких программных пакетов - *Elcut, Comsol, Ansys*. Но может производиться и вручную.

В результате расчета получают картины электрического поля, по которым определяют зону, где потенциал соответствует нормируемому (12 - 25 кВ) и у опоры, и в пролете.

Но, как показывает практика, существуют случаи, когда такая методика расчета неудобна или не подходит для того, чтобы корректно определить место подвеса оптоволоконного кабеля. Как правило, возникновение таких случаев связано с конструктивными особенностями воздушных линий электропередачи, которые вносят неравномер-

ность в распределение электрического поля (цепи одной линии выполнены разными проводами, пересечения линий, отпайки и т.п.).

Например, рассмотрим такую ситуацию: на двухцепной опоре цепи выполнены разными проводами. Такая конструкция вносит некоторые особенности в расчет, поскольку у разных проводов провис и диаметр отличаются.

Левая цепь исследуемой линии 110 кВ на опорах П6М (рисунок 3) содержит провод АС-185, правая цепь - провод АС-120.

Исходные данные:

Класс напряжения - 110 кВ

Величина наибольшего рабочего напряжения согласно ГОСТ 721-77:

$U_{нр}$= 126 кВ

Величина наибольшего рабочего фазного напряжения:

$$U_{нрф}=U_{нр}\times\frac{\sqrt{2}}{\sqrt{3}}=126\times10^{3}\times\frac{\sqrt{2}}{\sqrt{3}}=\ 103\ \text{кВ} \qquad (1)$$

Длина гирлянды и сцепной арматуры:

Lг=1.665 м.

Расчетный диаметр провода АС-120:

$d_{АС\text{-}120}$=15.2 мм

Расчетный диаметр провода АС-185:

$d_{АС\text{-}185}$=18.9 мм.

Стрела провиса для АС-120:

$f_{АС\text{-}120}$=9.1 м.

Стрела провиса для АС-185:

$f_{АС\text{-}185}$=7.1 м.

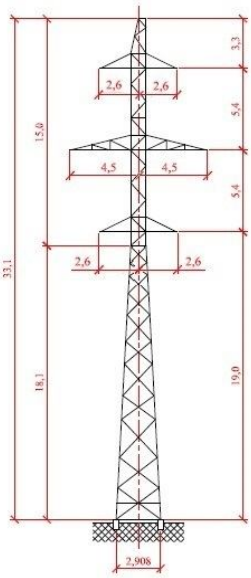


Рис. 3. Эскиз опоры П6М

Высоты подвеса проводов у опоры равняются высоте соответствующей траверсы за вычетом длины гирлянды и сцепной арматуры. Высоты подвеса проводов на опоре П6М представлены в таблице 1.

Проведем моделирование этой ситуации в программном пакете *Elcut*. Поскольку необходимо рассчитать электрическое поле вблизи фазных проводов, то ограничим область расчета по горизонтали (в поперечном направлении относительно оси ВЛ) от -25 м до 25 м относительно оси опоры. Провода смоделируем в виде окружностей соответствующего радиуса на высотах рассчитанных ранее. Для удобства построения сетки область расчета можно ограничить полусферой, что и было сделано.

Таблица 1.

Высоты подвеса проводов на опоре П6М

	Высота подвеса провода на опоре, м	
	АС-185	АС-120
Фаза А	28.135	28.135
Фаза В	22.735	22.735
Фаза С	17.335	17.335

Далее необходимо задать свойства модели. Каждому из проводов присвоим потенциал равный наибольшему рабочему фазному напряжению (103 кВ) и угол смещения фазы. Потенциал равный нулю присвоим линии (модель земли), которая ограничивает область расчета снизу и совпадает с осью *x*. Пространству, заключенному внутри смоделированной полусферы, задается значение диэлектрической проницаемости (Ɛ), равное единице. Построим сетку и произведем расчет. Картина поля, полученная в результате расчета, с выделенной зоной, где потенциал не превышает нормируемое значение, т.е. 25 кВ, представлена на рисунке 4, а.

Теперь, согласно упрощенной методике определения места подвеса ОКСН на опорах ЛЭП, необходимо произвести аналогичный расчет электрического поля в середине пролета, чтобы оценить влияние провиса проводов на картину поля вокруг проводов воздушной линии электропередачи.

Рассчитаем высоты, на которых будут находится фазные проводники в середине пролета:

- фазы левой цепи, содержащие провод АС-185:

$h_{A1пролет} = h_{A1} - f_{AC-185} = 28.135$ м - 7.1 м = 21.035 м

$h_{B1пролет} = h_{B1} - f_{AC-185} = 22.735$ м - 7.1 м = 15.635 м

$h_{C1пролет} = h_{C1} - f_{AC-185} = 17.335$ м - 7.1 м = 10.235 м

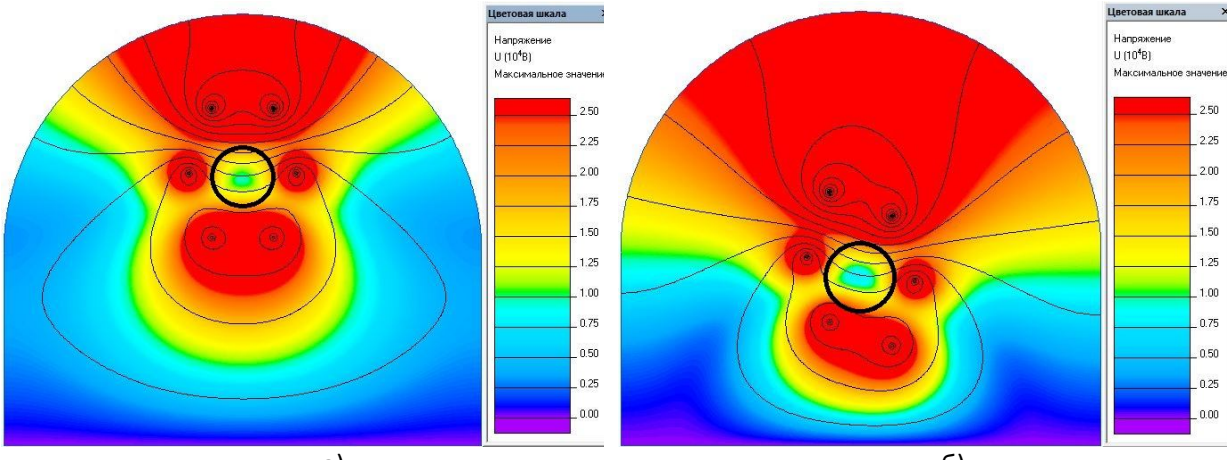
- фазы левой цепи, содержащие провод АС-120:

$h_{A2пролет} = h_{A2} - f_{AC-120} = 28.135$ м - 9.1 м = 19.035 м

$h_{B2пролет} = h_{B2} - f_{AC-120} = 22.735$ м - 9.1 м = 13.635 м

$h_{C2пролет} = h_{C2} - f_{AC-120} = 17.335$ м - 9.1 м = 8.235 м

Произведем построение геометрической модели двухцепной воздушной линии в середине пролета, провода которой будут находится на высотах, рассчитанных выше, а остальные параметры будут аналогичны расчету у опоры. Результат расчета с выделенной зоной, где потенциал не превышает нормируемое значение - на рисунке 4, б.



а) б)

Рис. 4. Картина электрического поля с выделенными зонами, где потенциал не превышает норму: а) у опоры; б) в середине пролета.

Для того чтобы точно определить высоты зоны, где потенциал не превышает нормируемый, построим график распределения потенциала вдоль вертикальной линии, совпадающей с осью ординат от 0 до 35 метров. График распределения потенциала у опоры представлен на рисунке 5, а в середине пролета - на рисунке 6.

По графикам распределения потенциала видно, что зона подвеса ОКСН у опоры по вертикали находится в диапазоне от 18 м до 26 м, а в середине пролета в диапазоне от 11 м до 17 м. Следовательно, оптоволоконный кабель необходимо подвесить на опоре на высоте 20 - 22 метров со стрелой провеса 7-8 метров.

Но, на сегодняшний день существуют такие программные пакеты (Comsol, Ansys), которые позволяют производить полное трехмерное моделирование пролета линии электропередачи и, в результате всего одного простого расчета, получать наиболее точную информацию о месте подвеса ОКСН на опорах этой ЛЭП.

Результат такого моделирования пролета линии электропередачи на опорах П6М, цепи которой выполнены проводами АС-185 и АС-120, представлен на рисунке 7.

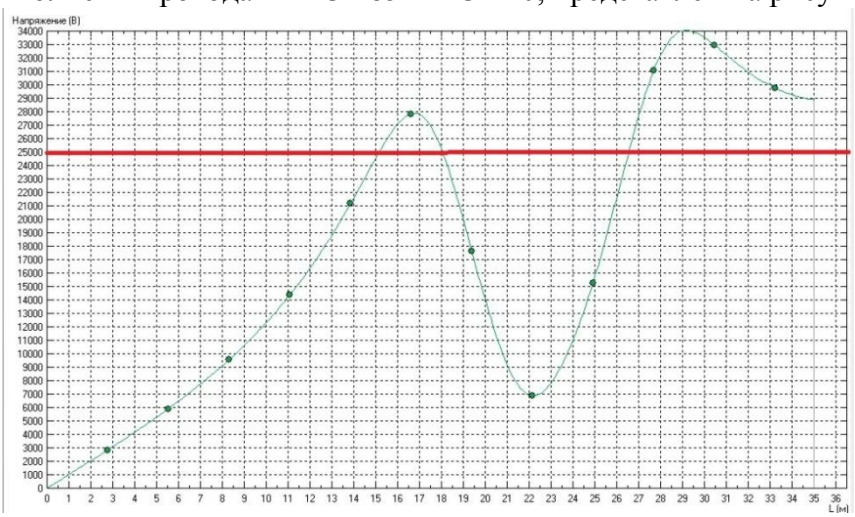


Рис. 5. График распределения потенциала вдоль вертикальной оси у опоры

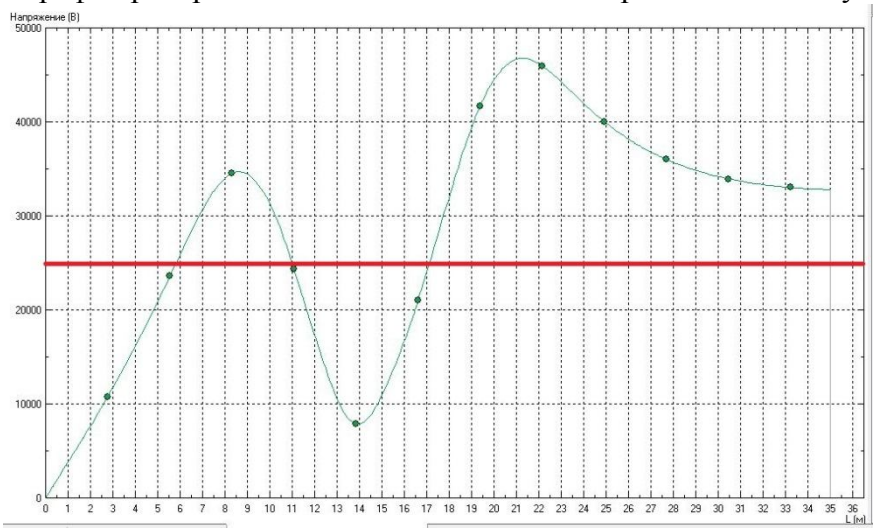


Рис. 6. График распределения потенциала вдоль вертикальной оси в середине пролета

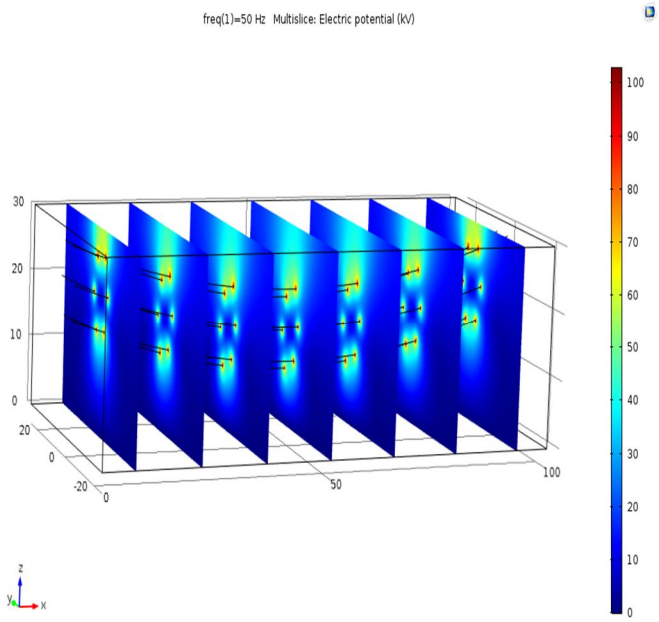
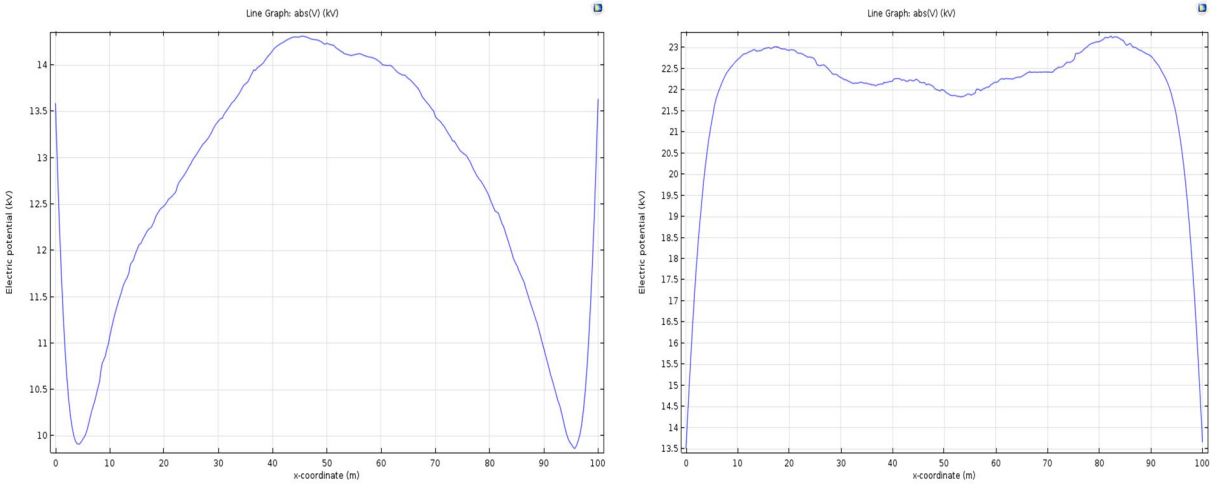


Рис. 7. Трехмерная картина электрического поля пролета линии на опорах П6М, левая цепь которой выполнена проводом АС-185, а правая цепь проводом АС-120

На рисунке 7 видно, что существует зона потенциала, где можно подвесить ОКСН «безопасно» для него, соблюдая определенную стрелу провеса. Для точного определения методом подбора была построена линия на высоте 20 метров со стрелой провеса 7 и 8 метров. График изображенный на рисунке 8, а показывает распределение потенциала вдоль этой линии со стрелой провеса 7 метров, а на рисунке 8, б - со стрелой провеса 8 метров.



а) б)

Рис. 8. График распределения потенциала вдоль построенной линии на высоте 20 метров со стрелой провеса: а) 7 метров; б) 8 метров.

Сравнив полученные графики, видно, что наиболее благоприятной для ОКСН будет стрела провеса равная 7 метрам.

Теперь необходимо определить точнее высоту крепления ОКСН на опоре. Стрелу провеса принимаем 7 метров и оставляем неизменной. Построим график распределения потенциала вдоль линий, подвешенных на высотах 19, 20, 21 метр (рисунок 9).

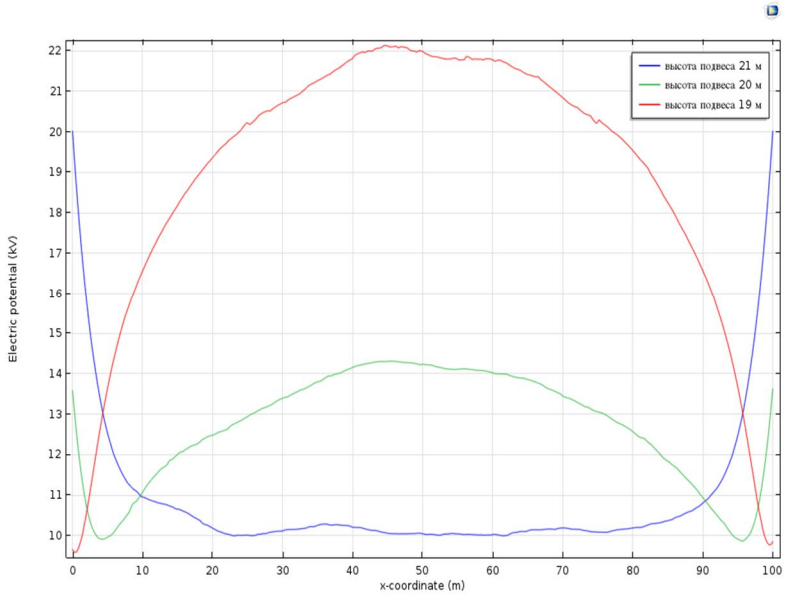


Рис. 9. График распределения потенциала вдоль построенной линии на высотах 19, 20, 21 метров со стрелой провеса 7 метров

Данный график подтверждает, что ОКСН должен крепиться на опоре на высоте 20 метров, и стрела провеса оптического кабеля должна соответствовать 7 метрам.

По результатам расчета можно сделать вывод о том, что полное трехмерное моделирование, по сравнению с моделированием по упрощенной методике позволяет затратить меньше времени на расчет и более точно определить место крепления ОКСН на опоре и его натяжение, соблюдая условие по наводимому потенциалу на поверхность оптоволоконного кабеля.

Литература:

1. Оптические сети и коммуникации. ОКСН. Что? Где? Когда? [Электронный ресурс] – 2012. – Режим доступа: http://www.vols-vl.ru/node/57. – Загл. с экрана.

2. Правила устройства электроустановок (ПУЭ), изд. 7, 2001 - 2004 г.

3. В.Г. Беляков. Особенности технических решений при проектировании ВОЛС-ВЛ [Электронный ресурс] / В.Г. Беляков, В.Д. Москалев, И.А. Исаева // startbase. – 2012. -https://www.startbase.ru/knowledge/articles/37/. – Загл. с экрана.

4. РД 153-34.0-48.518-98. Правила проектирования, строительства и эксплуатации волоконно-оптических линий связи на воздушных линиях электропередачи напряжением 110 кВ и выше. – Введ. 1999-02-07. – Москва: 1999.

5. Пример расчета эл. полей ЛЭП [Электронный ресурс] / ООО “Инкаб”. – Режим доступа: http://incab.ru/project/calculation_electric_fields/. – Загл. с экрана.

6. СТО 56947007- 33.180.10.172-2014. Технологическая связь. Правила проектирования, строительства и эксплуатации ВОЛС на воздушных линиях электропередачи напряжением 35 кВ и выше. – Введ. 2014.21.05. – Москва: ОАО «СОЮЗТЕХЭНЕРГО», 2014. – 250 с.

7. Руководства Comsol. Основы постобработки и визуализации в Comsol Multiphysics [Электронный ресурс] // Режим доступа: https://www.comsol.ru/sc/resources/pdf-offers/COMSOL_HANDBOOK_SERIES_Essentials_of_Postprocessing_and_Visualization-50_RUS_high.pdf - Загл. с экрана.

8. Ton´ci Modri´c. 3D Computation of the Power Lines Magnetic Field. / Ton´ci Modri´c, Slavko Vujevi´c, Dino Lovri´. - Progress In Electromagnetics Research M, Vol. 41, 1–9, 2015.

Содержание

Научное издание

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XIV Всероссийской научно-практической конференции
(15 июня 2018 г.)

В авторской редакции
Компьютерная верстка *Н. А. Никитиной*

ISBN 978-5-9266-1370-1

Подписано в печать 29.11.2018. Формат 60х84 1/8.
Усл. печ. л. 40,0. Тираж 60 экз. Заказ 737.

Краснодарский университет МВД России.
350005, Краснодар, у. Ярославская, 128.