Краснодарский университет МВД России

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XVII Всероссийской научно-практической конференции
(18 июня 2021 г.)

Краснодар
2021

УДК 004+51+53
ББК 22.1+32.81
М340

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. В. Еськов, доктор технических наук, профессор;
А. А. Хромых, кандидат физико-математических наук;
М. В. Шарпан, кандидат физико-математических наук;
К. И. Руденко, кандидат социологических наук

М340 **Математические методы и информационно-технические средства** : материалы XVII Всерос. науч.-практ. конф. (18 июня 2021 г.) / редкол.: И. Н. Старостенко, Е. В. Михайленко, А. В. Еськов и др. – Краснодар : Краснодарский университет МВД России, 2021. – 140 с.

ISBN 978-5-9266-1729-7

В сборнике содержатся материалы XVII Всероссийской научно-практической конференции, состоявшейся в Краснодарском университете МВД России 18 июня 2021 г., посвященной математическим методам и моделированию, программному обеспечению и информационно-техническим средствам, информационным технологиям в борьбе с экстремизмом, терроризмом и организованной преступностью, проблемам информационной безопасности, информационным технологиям в образовании.

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

УДК 004+51+53
ББК 22.1+32.81

ISBN 978-5-9266-1729-7

© Краснодарский университет
МВД России, 2021

Акапьев Виктор Львович,
Прокопенко Алексей Николаевич,
Савотченко Сергей Евгеньевич

МАТЕМАТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ СИСТЕМ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ

В условиях повсеместного внедрения дистанционного обучения все острее встает вопрос объективной оценки работы обучающихся - чем дальше от глаз экзаменатора, тем больше возможностей скрыть свое незнание. Основным условием успешной сдачи обучающимися итоговой аттестации является систематическая работа на лекциях, семинарах, практических занятиях, а также самостоятельная работа.

Дистанционная форма проведения экзаменов или зачетов принципиально не отличается от традиционной. Мероприятия могут быть проведены как устно, так и письменно, либо в форме теста. Главное в этом процессе – определить средство коммуникации между педагогом и обучающимся, а также контроль самостоятельности выполнения заданий.

Существует несколько вариантов контроля знаний обучающихся при дистанционном обучении.

Вариант 1. Для проведения устной формы контролирующих мероприятий используется платформа для видеоконференцсвязи (далее – ВКС), которая позволит наблюдать за ходом процесса. Чаще всего такая форма контроля используется для проведения промежуточной аттестации – экзамена или зачета.

Изначально необходимо довести до сведения обучающихся правила проведения контролирующих мероприятий (сколько времени на подготовку, чем можно пользоваться, критерии оценивания, какие могут быть «штрафные санкции» и т.д.).

Перед началом мероприятия следует проверить наличие подключившихся обучающихся, наличие и качество связи. Затем разделить группу экзаменуемых на небольшие подгруппы по 3-5 человек.

Распределить билеты между сдающими, для чего можно воспользоваться, например, генератором случайных чисел и демонстрацией экрана. Сообщить номер билета сдающему, вопросы из билета, зафиксировав время начала и окончания мероприятия.

По мере готовности, создав микрогруппу, обучающиеся начинают отвечать на вопросы по видеосвязи. Кроме того, рекомендуется включать сдающим режим «демонстрация экрана» для исключения чтения с экрана.

Для контроля за остальными сдающими достаточно не допускать ожидающими отключения видеосвязи.

Вариант 2. Письменная форма контролирующего мероприятия предполагает выполнение некоторой работы в письменном виде (эссе, расчетная работа, отчет и др.) и проверку ее преподавателем. Ее также можно провести, используя различные платформы для видеоконференций. Данная форма контроля используется для текущего контроля в конце практических занятий и семинаров, а также самостоятельной работы.

Темы раздаются любым удобным способом (почта, чат конференции и др.). Обучающиеся обязательно должны подтвердить получение и правильность понимания задания.

Далее необходимо установить сроки сдачи и объем письменной работы. Объем письменной работы должен быть заключен от 0,5 до 1 стр. По истечении времени обучающиеся должны предоставить результат работы установленным ранее способом (почта, чат конференции и др.).

При необходимости проверка высланных работ может быть проведена с использованием системы Антиплагиат.

Вариант 3. Тестирование. На настоящий момент чаще всего в качестве контроля знаний используется тестирование, поэтому этот вариант контроля знаний необходимо рассмотреть более подробно.

Основные количественные показатели систем тестирования.

Количественное значение уровня обученности получается тогда, когда оценку понимают (и определяют) как соотношение между фактически усвоенными знаниями, умениями и общим объемом этих знаний, умений, предложенным для усвоения. Показатель усвоения (продуктивности обучения) вычисляется из соотношения:

$$О = Ф / П,$$

где О – оценка успеваемости (обученности, продуктивности); Ф – фактический объем усвоенных знаний, умений; П – полный объем знаний, умений, предложенных для усвоения. Как видно, показатель усвоения (оценка) здесь колеблется между 1 – полное усвоение информации и 0 – полное отсутствие такового.

Для определения оценки по этому критерию необходимо научиться измерять объемы усвоенной и предложенной информации. Одной из технологий, позволяющей осуществлять такие измерения, является тестовый контроль.

Также тестирование должно быть измерением качества усвоения знаний, умений и навыков, поэтому в качестве элемента контроля уровня знаний нами предложено компьютерное тестирование. Педагогические тесты - единственный инструмент, позволяющий не только измерить обученность, но и умение использовать знания.

Смысл теста и его отличие от любого другого варианта контроля знаний может легко быть понят из его символической формулы:

Тест = Задание + Эталон.

Формулировка задания и наличие эталона (то есть полного и правильного решения теста, в котором выделены существенные операции теста), составляет основную специфику теста как средства объективного контроля качества знаний обучающихся.

Статистическая обработка результатов. Рассчитываются показатели трудности, валидности, надежности.

Мера трудности определяется отношением: $Q = 100\frac{W}{N}$,

где W – количество неправильных ответов;

N – общее число тестируемых.

Если трудность задания меньше 20 и больше 80, то такое задание необходимо переформулировать или убрать из теста.

Валидность характеризует тест с позиции адекватности, проверяемых знаний, умений, навыков. Она отражает тот факт, что тест действительно измеряет тот параметр, который по замыслу создателя должен измерять. Для создания валидного теста необходимо тщательно проанализировать понятия, структуру знаний, умений, навыков по курсу. Показателем валидности является различающая способность тестовых заданий (РСЗ). Измерить ее можно следующим образом: группу слушателей по результатам тестирования разделяют на «лучшую» и «худшую» подгруппы, выбирают по 30% в первой подгруппе «самых лучших» и во - второй подгруппе – «самых худших».

Тогда $РСЗ = \frac{P_л - P_х}{N}$, где $Р_л$ - доля правильных ответов «лучших слушателей», $Р_х$ - доля правильных ответов худших, N - общее число тестируемых.

Если РСЗ = 0, это означает, что «тест не работает». Чем выше показатель РСЗ, тем качество теста выше.

Требование надежности заключается в обеспечении устойчивости результатов тестирования испытуемого. При определении критерия надежности качества теста можно

использовать следующую формулу: $K = \frac{P_1}{P_2}$, где P_1 - количество правильно выполненных заданий в процессе тестирования, P_2 - общее количество заданий в тесте.

Оценка надежности качества теста представлена в таблице 1.

Таблица 1

Оценка надежности качества теста

Значение коэффициента надежности	Качество теста
0,000 – 0,599	Плохое
0,600 – 0,699	Неудовлетворительное
0,700 – 0,799	Удовлетворительное
0,800 – 0,899	Хорошее
0,900 – 0,949	Очень хорошее
0,950 – выше	Отличное

При контроле знаний обучающихся с применением тестов можно обеспечить любую наперед заданную надежность суждения о качестве усвоения. Для этого тесты каждого уровня объединяют в батареи, содержащие несколько тестов одного и того же уровня. От суммарного числа операций в батарее тестов зависит надежность контроля.

На рис. 1 показана кривая надежности батареи тестов при различном числе существенных операций в нем. Представляется, что оптимальным вариантом является разработка тестов с семьюдесятью существенными операциями.

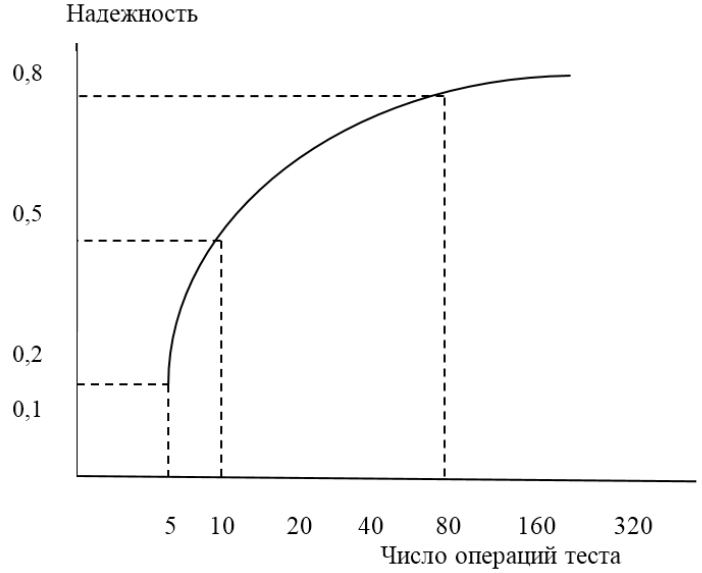


Рис. 1. Кривая надежности батареи тестов.

Классификация тестовых заданий.

По форме тестовые задания представляют собой сообщения, сформулированные в форме утверждений, которые в зависимости от ответов испытуемых могут интерпретироваться как в истинные или ложные высказывания. Кроме сообщений в виде наборов символов задания могут быть оформлены в виде графических объектов или их совокупности.

В таблице 2 представлены перечень и характеристики тестовых заданий в зависимости от уровня усвоения и сложности.

Виды заданий в таблице 2 сгруппированы по формам – закрытая и открытая. В зависимости от уровня усвоения материала закрытая форма заданий обеспечивает представление об изучаемом предмете. Открытая форма заданий обеспечивает уровни воспроизведение суждений, понятий, умений и навыков владения предметом изучения и уровень творчества, когда слушатель может не только решать задачи на понимание и воспроизведение материала, но и самостоятельно формировать решения в нетипичных ситуациях.

Таблица 2

Виды тестовых заданий

Виды тестовых заданий	Характеристика	Уровни усвоения
Закрытая форма: 1. Задания на «выбор» (альтернативный или множественный выбор). 2. Задания на «соответствие». 3. Задания на «установление правильной последовательности» (ранжирование).	На этом уровне слушатель способен узнавать изученные объекты, процессы, явления, способы действия, если они представлены в материальном виде или даны их описание, изображение и характеристика.	I уровень - уровень представления (знакомства)
Открытая форма: 4. Задания открытой формы (подстановка, типовое задание).	На этом уровне слушатель может воспроизводить изученную информацию, повторять усвоенные действия (операции), решать типовые задачи. Он обладает знанием – копией.	II уровень - уровень воспроизведения
5. Задания на «ситуацию» (нетиповое задание).	На этом уровне различают две разновидности усвоения: - умение, когда слушатель выполняет действия после довольно продолжительного предварительного продумывания последовательности и способов их осуществления; - навык, когда слушатель выполняет действие автоматически.	III уровень - уровень умений и навыков
6. Проблемные задания.	На этом уровне слушатель способен творчески использовать знания, умения и навыки в новых, нетипичных ситуациях, создавая оригинальные способы их решения.	IV уровень - уровень творчества

Из представленных в таблице 2 видов наибольшее распространение в педагогической практике образовательных учреждений получили первые четыре вида тестовых заданий – «на выбор», «на соответствие», «на правильную последовательность действий (алгоритм)» и «на подстановку».

В зависимости от вида контроля тест может включать задания различного уровня (таблица 3).

Таблица 3

Подбор уровней для различных видов контроля

Вид контроля	Характеристика	Контролируемый уровень усвоения
Входной	Контроль знаний и умений в начале обучения.	I
Текущий	Контроль уровня усвоения знаний и умений на лекциях, лабораторно-практических занятиях.	I-II
Рубежный	Контроль знаний и умений по окончанию изучения темы (раздела), модуля.	II-III
Итоговый	Контроль знаний, умений, навыков по окончанию обучения.	I-IV

Входной и текущий контроль применяется для организации управления учебным процессом в пределах одного сеанса работы слушателя (оперативное управление учебным процессом).

Рубежный контроль организуется для обеспечения принятия решения на продолжение процесса обучения (подготовки) слушателя.

Итоговый контроль предназначен для формирования квалификационной оценки – «Годен / Не годен», «Зачет / Незачет», «Допуск / Недопуск» и т.д.

Рассмотрим виды тестовых заданий по уровням усвоения.

I уровень:

Тестовые задания на «выбор» характеризуется тем, что в задании наряду с вопросом предоставляются готовые ответы, один (или несколько) из которых является правильным (правильными). В первом случае тестовое задание предполагает альтернативный выбор (выбор одного из многих), во втором – множественный (выбор многих из многих).

Алгоритмы формирования результата тестирования.

В практике автоматизированного контроля применяются различные алгоритмы формирования результата:

как сумма баллов: $R = \sum_{i=1}^{n} r_i$,

как разность между максимально возможным результатом и суммой штрафных баллов

$$R = R_{\max} - \sum_{i=1}^{n} \overline{r_i} .$$

Для определения эффективности усвоения по результатам тестирования можно использовать следующую формулу:

$$K_{оц} = 2{,}5 + 10\left(\frac{P}{N} - 0{,}7\right),$$

где P – число правильных ответов обучаемого; N – число вопросов теста.

Причем 2,51<K<3,49 соответствует оценке «удовлетворительно»; 3,51<K<4,49 – оценке «хорошо» и 4,51<K – оценке «отлично».

Инновационные формы заданий составляют наиболее перспективное направление развития компьютерного тестирования. Предъявление теста на компьютере позволяет разработчикам заданий использовать некоторые из особенностей компьютера и его функциональных преимуществ, потенциально предлагая новые и лучшие формы аттестации. Сам термин инновационные формы заданий для компьютерного тестирования используется для того, чтобы соотнести расширенные возможности заданий при ис-

пользовании компьютера. Аспекты рассмотрения инновационных форм заданий для компьютерного тестирования включают в себя: потенциальные преимущества, направления инноваций при разработке тестовых заданий и влияние сложности (комплексности) задачи (проблемы) (рис. 2).

Потенциальные преимущества от применения инновационных форм заданий для компьютерного тестирования. Формы заданий для компьютерного тестирования могут отличаться от традиционного, дискретного, основанного на тексте, альтернативного формата (с выбором ответа) заданий для бланкового тестирования многими способами.

Такие задания могут включить такие особенности или функции, которые нелегко, а иногда и невозможно обеспечить при бланковом тестировании. Имеется в виду включение видео, аудио или графики в задание, или вариант ответа. Экзаменующиеся, отвечая на такие задания, могут «Кликнуть» или перемещать экранный графический символ, вводить свободный (конструируемый) ответ, подсвечивать текст или совершать многие другие действия, невозможные на бумаге.

Рис. 2. Аспекты исследования инновационных форм заданий

Другие отличия касаются способности компьютера интерактивно взаимодействовать с экзаменующимися и вести подсчет сложных (комплексных) ответов.

Основная цель разработки инновационных типов заданий состоит в том, чтобы улучшить педагогическое измерение через повышение качества существующих, традиционных методов или через расширение измерительных технологий.

Другими словами, инновационные типы заданий дают возможность нам измерить кое-что лучше или измерять кое-что по большему количеству параметров. Инновационные типы заданий могут предложить улучшенное качество педагогического измерения за счет сокращения влияния угадывания или совершенствования процедур измерения. Инновационные типы заданий также могут улучшить педагогическое измерение, разворачивая тестовый экзамен на новые области содержания или на новые познавательные процессы испытуемых.

Рис. 3. Основные направления (тенденции) инноваций при разработке тестовых заданий

Новшества в компьютерных заданиях могут быть категоризированы в терминах пяти направлений. Хотя эти направления инноваций не полностью независимы, любое данное задание является обычно инновационным только в одном или двух смыслах. Эти пять направлений новшеств в компьютерных заданиях: формат задания, действия

испытуемого при ответе, включение медиатехнологий, повышение уровня интерактивности и совершенствование методов подсчета баллов.

Формат задания определяет вид ответа, получаемого от экзаменующегося, причем главные категории формата задания – с выбором варианта ответа и созданный (конструируемый) самим экзаменующимся ответ. Действия испытуемого при ответе относятся к тем средствам (способам), которыми экзаменующиеся обеспечивают ответы на вопросы при тестировании.

Включение медиатехнологий охватывает добавление нетекстовых элементов в задания – графику, звук, анимацию и видео. Уровень интерактивности определяется степенью, до которой тип задания реагирует или отвечает на ввод того или иного сигнала от экзаменующегося. Эта степень может варьироваться от полного отсутствия интерактивности до сложных многошаговых заданий с разветвлением алгоритма ответа. Наконец, различные методы подсчета баллов описывают каким образом ответы экзаменующегося преобразуются (конвертируются) в количественное множество на той или иной шкале.

При дистанционном обучении без использования тестов не обойтись как на этапе получения знаний, так и на этапе проверки полученных знаний, а также на этапе проверки умения применять эти знания к решению задач.

На современном этапе развития образовательных структур в условиях пандемии многие традиционные методы преподавания и контроля знаний стали отходить на задний план, уступая место новым методикам. Одно из ключевых мест здесь занимают системы компьютерного тестирования, позволяющие повысить объективность оценки уровня знаний.

Инновационные типы компьютерных заданий охватывают очень широкий диапазон сложности задач (не путать с уровнем трудности задания). Сложность задачи определяется числом и типом взаимодействий экзаменующегося в пределах данного задания. Уровень сложности задачи имеет значения для разработки задания, так же как для методов предъявления всего теста.

Задания с низкой сложностью задачи (поставленной проблемы) подобны традиционным, основанным на тексте задания с множественным выбором. Скромные различия между этими заданиями с низкой сложностью и более традиционными (бланковыми) типами заданий подразумевают, что задания с низкой сложностью поставленной проблемы могут быть легко включены в существующую структуру компьютерного теста.

Задания с высокой сложностью задачи требуют гораздо большего количества времени для ответов экзаменующегося, так как они основаны либо на использовании интерактивной подсказки в каком-либо эссе, либо на компьютеризированном моделировании задачи на основе выполнения некоторой лабораторной работы, или другой практической деятельности. Аттестация на основе заданий с высокой сложности задачи часто разрабатывается для определенной программы экзамена, чтобы удовлетворить специфические потребности в охвате большой области содержания знаний и познавательных навыков испытуемых.

Задачи (задания) высокой сложности часто предъявляются автономным способом, т.е. не включаются в существующее тестовое испытание. Большинство научно-исследовательских работ посвящено этим двум крайностям в уровне сложности задач.

Проблемы в связи с внедрением задач повышенной сложности в компьютерное тестирование могут лежать в разных плоскостях. Применение новых форматов заданий может требовать значительных усилий по совершенствованию методов их разработки и оценке соответствующих алгоритмов подсчета тестовых баллов. Наконец, тестовые испытания, в которых представлены исключительно задания высокой сложности, могут иметь проблемы с запоминанием, непониманием испытуемыми специфики задачи, скрытыми дефектами таких заданий.

Литература

1. Акапьев В.Л. Формирование информационно-технологической компетентности сотрудников ОВД: монография / В. Л. Акапьев. – Белгород: БелЮИ МВД России, 2015. – 132 с.
2. Методические рекомендации о преподавании дисциплин естественно-научного направления по всем видам занятий в системе дистанционного обучения в образовательных организациях МВД России. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2021. – 41 с.
3. Частные методики образовательных технологий формирования информационно-технологической компетентности сотрудников правоохранительных органов: учебно-методическое пособие / С.Е. Савотченко [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2017. – 68 с.

Сведения об авторах

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: akapevvl@yandex.ru.

Прокопенко Алексей Николаевич, кандидат технических наук, доцент начальник кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: aprokopenko11@mvd.ru.

Савотченко Сергей Евгеньевич, доктор физико-математических наук, доцент, профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: savotchenko@hotbox.ru.

Аршинов Георгий Александрович

СОВЕРШЕНСТВОВАНИЕ АКУСТИЧЕСКИХ МЕТОДОВ ОПРЕДЕЛЕНИЯ ДЕФЕКТОВ В ЭЛЕМЕНТАХ КОНСТРУКЦИЙ

Диагностика прочности изделий неразрушающими методами – актуальное направление обеспечения эксплуатационной и экономической эффективности сооружений.

Акустический метод контроля микродефектов – эффективный и относительно простой способ обнаружения скрытых повреждений материала, вблизи которых может начаться процесс разрушения. Ультразвук хорошо проникает вглубь материала, поэтому акустический метод во многих случаях обладает значительными преимуществами перед другими приемами исследований на наличие повреждений.

Способность с достаточной информативностью выявлять дефекты разных типов и размера в различных материалах приводит к широкому применению акустических приемов исследования металлов.

Проведем исследование динамики деформирования бесконечного стержня, выполненного из материала с реологическими нелинейными физико-механическими свойствами, для получения более точных значений скорости деформации, важных для совершенствования акустической диагностики микроповреждений изделий.

Допустим, что на стержень не действует внешняя нагрузка. Введем функции

$$u_1 = u(x,t);\ u_2 = -\nu y u_x;\ u_3 = -\nu z u_x,$$

задающие компоненты перемещений точек стержня: u_1 – по оси x, совпадающей с его осью, u_2 – по оси y и u_3 – по оси z (рис. 1).

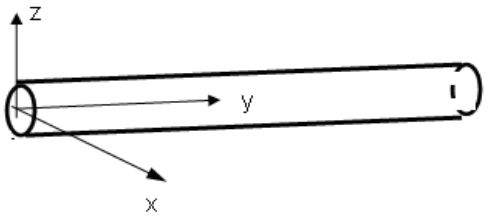


Рис. 1. Система координат в неограниченном стержне

Нелинейные компоненты деформации зададим в виде:

$$\varepsilon_{ij} = \frac{1}{2}(u_{i,j} + u_{j,i} + u_{k,i}u_{k,j}).$$

Реологические свойства материала стержня опишем уравнениями наследственной теории вязкоупругости:

$$s_{ij}(t) = 2\mu[e_{ij}(t) - \alpha\int_{-\infty}^{t} e^{-\beta(t-\tau)}e_{ij}(\tau)]d\tau .$$

$$\sigma(t) = K\theta(t)$$

Представим функции $f(\tau) = e_{ij}(\tau)$ степенными рядами по степеням $(t-\tau)$ и, заменяя интегральный оператор дифференциальными, получим связь между напряжениями и деформациями в виде

$$\sigma_{ij} = \tilde{\lambda}\theta\delta_{ij} + 2\tilde{\mu}\varepsilon_{ij}, \qquad (1)$$

В соотношениях (1) $\tilde{\lambda} = \lambda - \frac{2\mu}{3}$, $2\tilde{\mu} = 2\mu(1+p)$.

Применение оператора $p = \frac{\alpha}{\beta^2}\frac{\partial}{\partial t} - \frac{\alpha}{\beta}$ к $f(t)$ дает $pf = \frac{\alpha}{\beta^2}f_t - \frac{\alpha}{\beta}f$.

Вычислим компоненты девиатора деформации с помощью формул

$$e_{11} = \frac{2(1+\nu)}{3}u_x + \frac{1}{3}(1-\nu^2)u_x^2 + \frac{\nu^2 r^2}{3}u_{xx}^2;$$

$$e_{22} = -\frac{1}{3}(1+\nu)u_x - \frac{1}{6}(1-\nu^2)u_x^2 - \frac{\nu^2 r^2}{6}u_{xx}^2;$$

$$e_{12} = -\frac{\nu y}{2}u_{xx} + \frac{\nu^2 y}{2}u_x u_{xx},\ e_{13} = -\frac{\nu z}{2}u_{xx} + \frac{\nu^2 z}{2}u_x u_{xx},$$

в которых $r^2 = z^2 + y^2$.

Найдем вариации компонент тензора деформаций и представим их через дифференциальные операторы:

$$\delta\varepsilon_{11} = [-\frac{\partial}{\partial x} - u_x\frac{\partial}{\partial x} + \nu^2 r^2 u_{xx}\frac{\partial^2}{\partial x^2}]\delta u;$$

$$\delta\varepsilon_{22} = \delta\varepsilon_{33} = [\nu\frac{\partial}{\partial x} - \nu^2 u_x\frac{\partial}{\partial x}]\delta u;$$

$$\delta\varepsilon_{12} = [-\frac{\nu y}{2}\frac{\partial^2}{\partial x^2} - \frac{\nu^2 y}{2}u_{xx}\frac{\partial}{\partial x} + \frac{\nu^2 y}{2}u_x\frac{\partial^2}{\partial x^2}]\delta u;$$

$$\delta\varepsilon_{13} = [-\frac{\nu z}{2}\frac{\partial^2}{\partial x^2} - \frac{\nu^2 z}{2}u_{xx}\frac{\partial}{\partial x} + \frac{\nu^2 z}{2}u_x\frac{\partial^2}{\partial x^2}]\delta u.$$

Определяя вариацию внутренней энергии стержня

$$\delta W = \{-[\tilde{\lambda}(1-2\nu) + 2\tilde{\mu} - 2\nu(1-2\nu)\tilde{\lambda} - 2\tilde{\mu}\nu)]u_{xx} + \tilde{\mu}\nu^2 r^2 u_{xxxx} -$$

$$-(B_1+2A_1-2\nu B_2+4\nu^2A_2)u_xu_{xx}-[\tilde{\lambda}+2\tilde{\mu}-2\nu\tilde{\lambda}-2\tilde{\mu}\nu]\nu^2r^2u_{xx}u_{xxxx}+$$
$$+\nu^2r^2(A_1-2\tilde{\mu}\nu)(u_xu_{xx})_{xx}-(\frac{3B_1}{2}+3\nu^2B_2)u_x^2u_{xx}-\frac{1}{2}\nu^2r^2[(\tilde{\lambda}+2\tilde{\mu})+$$
$$+2\nu^2\tilde{\lambda}+2\tilde{\mu}\nu^2](u_xu_{xx}^2)_x+\frac{\nu^2r^2}{2}(B_1+2\tilde{\mu}\nu^2)(u_x^2u_{xx})_{xx}+\frac{\nu^4r^4}{2}(\tilde{\lambda}+2\tilde{\mu})(u_{xx}^3)_{xx}\}\delta u,$$

где $A_1=a(2\nu^3-\nu+1)$; $B_1=a\nu(2\nu-2\nu^2+1)$; $A_2=a\nu^2(1-\nu)$;

$B_2=a\nu^3$; $a=\dfrac{1}{2(1+\nu)(1-2\nu)}$; $r^2=z^2+y^2$,

и по принципу виртуальных перемещений приходим к уравнению движения стержня в перемещениях

$$\rho(-u_{tt}+\nu^2r^2u_{ttxx})+N_1u_{xx}-\tilde{\mu}\nu^2r^2u_{xxxx}+N_2u_xu_{xx}+$$
$$+\nu^2r^2N_3u_{xx}u_{xxx}-\nu^2r^2N_4(u_xu_{xx})_{xx}+N_5u_x^2u_{xx}+ \qquad (2)$$
$$+\frac{1}{2}\nu^2r^2N_6(u_xu_{xx}^2)_x-\frac{1}{2}\nu^2r^2N_7(u_x^2u_{xx})_{xx}-\frac{1}{2}\nu^4r^4N_8((u_{xx})^3)_{xx}=0.$$

Здесь введены переменные

$$N_1=\tilde{\lambda}(1-2\nu)^2+2\tilde{\mu}(1+2\nu^2);\ N_2=3(1-2\nu)(1+2\nu^2)\tilde{\lambda}+6\tilde{\mu}(1-2\nu^3);$$
$$N_3=(1-2\nu)\tilde{\lambda}+2\tilde{\mu}(1-\nu);\ N_4=\tilde{\lambda}(1-2\nu)+2\tilde{\mu}(1-2\nu);$$
$$N_5=\frac{3}{2}\tilde{\lambda}(1+2\nu^2)^2+3\tilde{\mu}(1-2\nu^4);\ N_6=(1+2\nu^2)\tilde{\lambda}+2\tilde{\mu}(1+\nu^2);$$
$$N_7=(1+2\nu^2)\tilde{\lambda}+2\tilde{\mu}(1+\nu^2);\ N_8=\tilde{\lambda}+2\tilde{\mu}.$$

Запишем (2) в безразмерных переменных

$$\xi=\frac{x}{L}-\frac{c}{L}t;\quad \tau=\varepsilon\frac{c}{L}t;\quad u^*=\frac{u}{A}.$$

Пусть L – длина волны деформации, A – ее амплитудная характеристика и параметр $\varepsilon=A/L<<1$. Допустим, что справедливы отношения порядков

$$\frac{\alpha c}{\beta^2L}=O(\varepsilon);\quad \frac{d}{L}=O(\sqrt{\varepsilon}).$$

Представим перемещение u асимптотическим разложением

$$u=u_0+\varepsilon u_1+\varepsilon^2u_2+\ldots. \qquad (3)$$

С учетом (3) получаем уравнение движения точек стержня

$$\frac{\rho c^2}{E}[-u_{\xi\xi}+2\varepsilon u_{\xi\tau}-\varepsilon^2u_{\tau\tau}+\varepsilon\nu^2I(u_{\xi\xi\xi\xi}-2\varepsilon u_{\xi\xi\xi\tau}+\varepsilon^2u_{\xi\xi\tau\tau})]+$$
$$+(1-\frac{\alpha a_0}{\beta})u_{\xi\xi}-\frac{\varepsilon\nu^2I}{2(1+\nu)}(1-\frac{\alpha}{\beta})u_{\xi\xi\xi\xi}+\varepsilon(3-\frac{\alpha a_3}{\beta})u_\xi u_{\xi\xi}+$$
$$+\frac{\alpha c}{\beta^2l}(\varepsilon\frac{\partial}{\partial\tau}-\frac{\partial}{\partial\xi})\cdot[a_0u_{\xi\xi}-\frac{\varepsilon\nu^2I}{2(1+\nu)}u_{\xi\xi\xi\xi}+\varepsilon a_3u_\xi u_{\xi\xi}]=0.$$

Анализируя нулевое приближение в (3), имеем равенство

$$\left[-\frac{\rho c^2}{E}+\left(1-\frac{\alpha a_1}{\beta}\right)\right]u_{0\xi\xi}=0. \qquad (4)$$

Здесь $a_1=\dfrac{2}{3}(1+\nu)$. Поскольку имеет место неравенство $u_{0\xi\xi}\neq0$, то из равенства

(4) для вычисления скорости волны деформации в стержне получаем формулу

$$c = \sqrt{\frac{E}{\rho}[1-\frac{2\alpha(1+\nu)}{3\beta}]}.$$

Анализ первого приближения в асимптотическом разложении (3) приводит к эволюционной модели

$$\psi_\tau + b_1\psi\psi_\xi + b_2\psi_{\xi\xi} + b_3\psi_{\xi\xi\xi} = 0, \qquad (5)$$

являющейся уравнением Кортевега де Вриза – Бюргерса (КДВ).

В (5) введены обозначения:

$$\psi = u_{0\xi}; \qquad b_1 = \frac{E(3\beta-\alpha a_2)}{2\rho c^2\beta}; \quad b_2 = -\frac{E\alpha a_1}{2\rho c\beta^2 l\varepsilon};$$

$$a_2 = 2(1-\nu^2); \qquad b_3 = \nu^2 I[\frac{1}{2} - \frac{E(\beta-\alpha)}{4\rho c^2\beta(1+\nu)}].$$

Физико-механические свойства нелинейного стержня при линейно-упругих объемных деформациях опишем уравнениями теории ползучести в виде

$$\sigma_{ij}(t) = \lambda\theta\delta_{ij} + 2\mu\varepsilon_{ij} - 2\mu\alpha\int_{-\infty}^{t} e^{-\beta(t-\tau)}[1+\gamma\varepsilon_u^2(\tau)]e_{ij}(\tau)d\tau, \qquad (6)$$

Для упрощения (6) применим разложение в ряды Тейлора функций $[1+\gamma\varepsilon_u^2(\tau)]e_{ij}(\tau)$ по степеням $(t-\tau)$, получим закон состояния в виде

$$\sigma_{ij} = \tilde{\lambda}\theta\delta_{ij} + 2\tilde{\mu}\varepsilon_{ij} + 2\gamma\mu p(\varepsilon_u^2 e_{ij}),$$

где $\tilde{\lambda} = \lambda - \frac{2\mu}{3}p; \quad \tilde{\mu} = \mu(1+p); \qquad p = \frac{\alpha}{\beta^2}\frac{\partial}{\partial t} - \frac{\alpha}{\beta}.$

Вычислим линейную

$$\delta W_л = \{-[\tilde{\lambda}(1-2\nu) + 2\tilde{\mu} - 2\nu((1-2\nu)\tilde{\lambda} - 2\mu\nu)]u_{xx} + 2\tilde{\mu}\frac{\nu^2 r^2}{2}u_{xxxx}]\delta u$$

и нелинейную составляющие вариации внутренней энергии стержня

$$\delta W_н = \{-B_1 u_x u_{xx} - \nu^2 r^2(\tilde{\lambda}+2\tilde{\mu})u_{xx}u_{xxx} - 2\mu\gamma p(\varepsilon_u^2 e_{11})_x - 2A_1 u_x u_{xx} -$$

$$-\frac{3}{2}B_1 u_x^2 u_{xx} - \frac{\nu^2 r^2}{2}(\tilde{\lambda}+2\tilde{\mu})(u_x u_{xx}^2)_x - 2\mu\gamma p(\varepsilon_u^2 e_{11}u_x)_x +$$

$$+\nu^2 r^2 A_1(u_x u_{xx})_{xx} + \nu^2 r^2\frac{B_1}{2}(u_x^2 u_{xx})_{xx} + \frac{\nu^4 r^4}{2}(\tilde{\lambda}+2\tilde{\mu})(u_{xx}^3)_{xx} +$$

$$+\nu^2 r^2 2\mu\gamma p(\varepsilon_u^2 e_{11}u_{xx})_{xx} + 2[\nu B_2 u_x u_{xx} + \nu^3 r^2\tilde{\lambda}u_{xx}u_{xxx} + 2\mu\nu\gamma p(\varepsilon_u^2 e_{22})_x -$$

$$-2\nu^2 A_2 u_x u_{xx} - \frac{3\nu^2}{2}B_2 u_x^2 u_{xx} - \frac{\nu^4 r^2}{2}\tilde{\lambda}(u_x u_{xx}^2)_x - 2\nu^2\mu\gamma p(\varepsilon_u^2 e_{22}u_x)_x] -$$

$$-2\tilde{\mu}\frac{\nu^3 r^2}{2}(u_x u_{xx})_{xx} - 2\mu\gamma p\nu y(\varepsilon_u^2 e_{12})_{xx} + \tilde{\mu}\nu^3 r^2 2u_{xx}u_{xxx} -$$

$$-2\tilde{\mu}\frac{\nu^4 r^2}{2}(u_x u_{xx}^2)_x - 2\mu\gamma p\nu^2 y(\varepsilon_u^2 e_{12}u_{xx})_x - \mu\nu^3 r^2(u_x u_{xx})_{xx} +$$

$$+2\tilde{\mu}\frac{\nu^4 r^2}{2}(u_x^2 u_{xx})_{xx} + 2\mu\gamma p\nu^2 y(\varepsilon_u^2 e_{12}u_x)_{xx} - 2\mu\gamma p\nu z(\varepsilon_u^2 e_{13})_{xx} -$$

$$-2\mu\gamma p\nu^2 z(\varepsilon_u^2 e_{13}u_{xx})_x + 2\mu\gamma p\nu^2 z(\varepsilon_u^2 e_{13}u_x)_{xx}\}\delta u.$$

Здесь использованы обозначения

$$A_1 = \tilde{\lambda}(1-2\nu) + 2\tilde{\mu}; \qquad B_1 = (1+2\nu)\tilde{\lambda} + 2\tilde{\mu};$$
$$A_2 = (1-2\nu)\tilde{\lambda} + 2\tilde{\mu}\nu; \qquad B_2 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}\nu^2.$$

Ее полная вариация

$$\delta W = \{-N_1 u_{xx} + \tilde{\mu}\nu^2 r^2 u_{xxxx} - N_2 u_x u_{xx} - \nu^2 r^2 N_3 u_{xx} u_{xxx} +$$
$$+ \nu^2 r^2 N_4 (u_x u_{xx})_{xx} - N_5 u_x^2 u_{xx} - \frac{\nu^2 r^2}{2} N_6 (u_x u_{xx}^2)_x + \frac{\nu^2 r^2}{2} N_7 (u_x^2 u_{xx})_{xx} +$$
$$+ \frac{\nu^4 r^4}{2} N_8 (u_{xx}^3)_{xx} - 2\mu\gamma p[(\varepsilon_u^2)_x (e_{11} - 4\nu e_{22} + e_{11} u_x + 2\nu^2 e_{22} u_x +$$
$$+ \nu^2 y e_{12} u_{xx} + \nu^2 z e_{13} u_{xx}) + \varepsilon_u^2 (e_{11} - 4\nu e_{22} + e_{11} u_x + 2\nu^2 e_{22} u_x +$$
$$+ \nu^2 y e_{12} u_{xx} + \nu^2 z e_{13} u_{xx})_x + \frac{\partial}{\partial x}((\varepsilon_u^2)_x (\nu y e_{12} + \nu z e_{13} - \nu^2 r^2 e_{11} u_{xx} -$$
$$- \nu^2 y e_{12} u_x - \nu^2 z e_{13} u_x) + \varepsilon_u^2 (\nu y e_{12x} + \nu z e_{13x} - \nu^2 r^2 (e_{11} u_{xx})_x -$$
$$- \nu^2 y (e_{12} u_x)_x - \nu^2 z (e_{13} u_x)_x))]\}\delta u.$$

Здесь введены переменные

$$N_1 = \tilde{\lambda}(1-2\nu)^2 + 2\tilde{\mu}(1+2\nu^2); \; N_2 = 3(1-2\nu)(1+2\nu^2)\tilde{\lambda} + 6\tilde{\mu}(1-2\nu^3);$$
$$N_3 = (1-2\nu)\tilde{\lambda} + 2\tilde{\mu}(1-\nu); \quad N_4 = \tilde{\lambda}(1-2\nu) + 2\tilde{\mu}(1-2\nu);$$
$$N_5 = \frac{3}{2}\tilde{\lambda}(1+2\nu^2)^2 + 3\tilde{\mu}(1-2\nu^4); \; N_6 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}(1+\nu^2);$$
$$N_7 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}(1+\nu^2); \; N_8 = \tilde{\lambda} + 2\tilde{\mu}.$$

С учетом выражения δW по принципу виртуальных перемещений найдем уравнение движения стержня

$$\rho(-u_{tt} + \nu^2 r^2 u_{ttxx}) + N_1 u_{xx} - \tilde{\mu}\nu^2 I u_{xxxx} + N_2 u_x u_{xx} + \nu^2 r^2 N_3 u_{xx} u_{xxx} -$$
$$- \nu^2 r^2 N_4 (u_x u_{xx})_{xx} + N_5 u_x^2 u_{xx} + \frac{1}{2}\nu^2 r^2 N_6 (u_x u_{xx}^2)_x - \frac{1}{2}\nu^2 r^2 N_7 (u_x^2 u_{xx})_{xx} -$$
$$- \frac{1}{2}\nu^4 r^4 N_8 (u_{xx}^3)_{xx} + 2\mu\gamma\rho\{\frac{\partial}{\partial x}[\frac{1}{3}(1+u_x)(2(1+\nu)u_x + (1-\nu^2)u_x^2 -$$
$$+ \frac{1}{2}(1-\nu^2)u_x^2)(2\nu^2 u_x - 4\nu))Q + ((\frac{1}{3}\nu^2 u_{xx}^2 (1+u_x) - \frac{1}{6}\nu^2 u_{xx}^2 (2\nu^2 u_x -$$
$$- 4\nu) + \frac{1}{2}\nu^2 (\nu^2 u_x u_{xx}^2 - \nu u_{xx}^2)) \cdot Q] + \quad [(-\frac{1}{3}\nu^2 u_{xx}(2(1+\nu)u_x + (1-\nu^2)u_x^2) +$$
$$+ \frac{1}{2}(\nu - \nu^2 u_x) \cdot (\nu^2 u_x u_{xx} - \nu u_{xx})) \cdot Q - \frac{1}{2}\nu^4 r^4 N_8 (u_{xx}^3)_{xx} + 2\mu\gamma p\{\frac{\partial}{\partial x}[(\frac{1}{3}(1+u_x) +$$
$$+ \frac{1}{3}\nu^4 u_{xx}^3 Q]_{xx}\} = 0,$$

где

$$Q = R_1 + R_2 + R_3; \quad R_1 = \frac{1}{3}[2(1+\nu)u_x + (1-\nu^2)u_x^2]^2; \quad R_3 = \frac{1}{3}\nu^4 u_{xx}^4;$$
$$R_2 = \frac{2}{3}\nu^2 u_{xx}^2 [2(1+\nu)u_x + (1-\nu^2)u_x^2]^2 + (\nu^2 u_x u_{xx} - \nu u_{xx})^2.$$

В нулевом приближении метода возмущений с использованием (3) получим равенство

$$[-\frac{\rho c^2}{E}+(1-\frac{\alpha a_1}{\beta})]u_{0\xi\xi}=0,$$

здесь $a_1=\frac{2}{3}(1+\nu).$

Скорость волны деформации вычисляется по формуле:

$$c=\sqrt{\frac{E}{\rho}[1-\frac{2\alpha}{3\beta}(1+\nu)]}.$$

В первом приближении метода возмущения получаем модифицированное уравнение КДВ:

$$\psi_\tau+b_1\psi\psi_\xi-b_2\psi^2\psi_\xi+b_3\psi_{\xi\xi}+b_4\psi_{\xi\xi\xi}=0,$$

где

$$\psi=u_{0\xi};\qquad b_1=m(3-\frac{\alpha a_2}{\beta});\quad m=\frac{E}{2\rho c^2};$$

$$b_2=\frac{m\alpha\gamma\varepsilon a_3}{\beta};\qquad b_3=-\frac{m\alpha c a_1}{\beta^2 L\varepsilon};\qquad b_4=m\nu^2 I[\frac{1}{2m}-\frac{\beta-\alpha}{2\beta(1+\nu)}];$$

$$a_2=2(1-\nu^2);\qquad a_3=\frac{8}{3}(1+\nu^2)(1+2\nu).$$

Представлены новые математические модели для описания волн продольной деформации в стержнях с нелинейными реологическими свойствами.

Уточненные формулы для вычислений скорости волны могут быть использованы для совершенствования акустических методов поиска скрытых микродефектов материала.

Литература

1. Аршинов Г.А. Продольные нелинейные волны в вязкоупругих стержнях, пластинах и цилиндрических оболочках / Г.А. Аршинов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2003. – №02(002). С. 1–15. – IDA [article ID]: 0020302001. – Режим доступа: http://ej.kubagro.ru/2003/02/pdf/01.pdf, 0,938 у.п.л.

2. Аршинов Г.А. Нелинейные уединенные ударно-волновые структуры в вязкоупругих стержнях / Г.А. Аршинов, В.Н. Лаптев, Н.И. Елисеев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2003. – № 02(002). С. 42–51. – IDA [article ID]: 0020302006. – Режим доступа: http://ej.kubagro.ru/2003/02/pdf/06.pdf, 0,625 у.п.л.

3. Аршинов Г.А. Оценка экономической и эксплуатационной надежности строительных сооружений на основе исследования волновых характеристик нелинейных вязкоупругих стержневых элементов конструкций / Г.А. Аршинов, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. – № 153. – С. 113–122.

4. Аршинов Г.А. Совершенствование акустических методов диагностики скрытых микродефектов и эксплуатационная надежность вязкоупругих элементов конструкций / Г.А. Аршинов, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. – № 154. – С. 84–93.

Сведения об авторе

Аршинов Георгий Александрович, доктор технических наук, доцент, профессор кафелры комьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: arshinov_kts@mail.ru.

Аршинов Георгий Александрович

УТОЧНЕНИЕ АКУСТИЧЕСКИХ МЕТОДОВ ДИАГНОСТИКИ МИКРОДЕФЕКТОВ МАТЕРИАЛА В ВЯЗКОУПРУГИХ СТЕРЖНЯХ

Надежность сооружений, содержащих стержни, опоры, балки, определяется их способностью сохранять несущую способность под воздействием внешней нагрузки. Прочностные свойства материала элементов конструкций зависят от микродефектов структуры, которые могут образовываться при изготовлении.

Необходимо совершенствовать методы акустики, применяемые для диагностики микродефектов, с помощью более точных моделей деформационных волн в стержнях с учетом реальных нелинейных свойств материалов.

Большое количество материалов, проявляя линейно-упругое объемное деформирование, при сдвиговых деформациях подвержены ползучести. Исследуем динамику ползучести стержней, изготовленных из материалов с такими физико-механическими свойствами, проведя анализ бесконечного стержня, когда к нему не приложены нагрузки.

Рассмотрим функции

$$u_1 = u(x,t);\ u_2 = -\nu y u_x;\ u_3 = -\nu z u_x,$$

задающие компоненты вектора перемещений точек стержня: u_1 – по оси x, совпадающей с его осью, u_2 – по оси y и u_3 – по оси z.

Воспользуемся тензором конечных деформаций

$$\varepsilon_{ij} = \frac{1}{2}(u_{i,j} + u_{j,i} + u_{k,i}u_{k,j}).$$

Реологию поведения материала стержня опишем наследственной теорией вязкоупругости:

$$\begin{aligned} s_{ij}(t) &= 2\mu[e_{ij}(t) - \alpha\int_{-\infty}^{t} e^{-\beta(t-\tau)}e_{ij}(\tau)]d\tau \\ \sigma(t) &= K\theta(t) \end{aligned}. \qquad (1)$$

Запишем ряды Тейлора по степеням $(t-\tau)$ для функций $f(\tau) = e_{ij}(\tau)$, заменим интегральный оператор в (1) дифференциальными, тогда

$$\sigma_{ij} = \tilde{\lambda}\theta\delta_{ij} + 2\tilde{\mu}\varepsilon_{ij}.$$

Здесь $\tilde{\lambda} = \lambda - \frac{2\mu}{3}$, $2\tilde{\mu} = 2\mu(1+p)$, $p = \frac{\alpha}{\beta^2}\frac{\partial}{\partial t} - \frac{\alpha}{\beta}$.

Компоненты девиатора деформаций зададим уравнениями

$$e_{11} = \frac{2(1+\nu)}{3}u_x + \frac{1}{3}(1-\nu^2)u_x^2 + \frac{\nu^2 r^2}{3}u_{xx}^2;$$

$$e_{22} = -\frac{1}{3}(1+\nu)u_x - \frac{1}{6}(1-\nu^2)u_x^2 - \frac{\nu^2 r^2}{6}u_{xx}^2;$$

$$e_{12} = -\frac{\nu y}{2}u_{xx} + \frac{\nu^2 y}{2}u_x u_{xx},\ e_{13} = -\frac{\nu z}{2}u_{xx} + \frac{\nu^2 z}{2}u_x u_{xx},$$

где $r^2 = z^2 + y^2$.

Определим вариации деформаций

$$\delta\varepsilon_{11} = \delta u_x + u_x\delta u_x + \nu^2 r^2 u_{xx}\delta u_{xx}; \qquad \delta\varepsilon_{22} = \delta\varepsilon_{33} = (-\nu + \nu^2 u_x)\delta u_x;$$

$$\delta\varepsilon_{12} = -\frac{\nu y}{2}\delta u_{xx} + \frac{\nu^2 y}{2}(u_{xx}\delta u_x + u_x\delta u_{xx}); \quad \delta\varepsilon_{13} = -\frac{\nu z}{2}\delta u_{xx} + \frac{\nu^2 z}{2}(u_{xx}\delta u_x + u_x\delta u_{xx})$$

и используем операторное представление:

$$\delta\varepsilon_{11} = [-\frac{\partial}{\partial x} - u_x\frac{\partial}{\partial x} + \nu^2 r^2 u_{xx}\frac{\partial^2}{\partial x^2}]\delta u;$$

$$\delta\varepsilon_{22} = \delta\varepsilon_{33} = [\nu\frac{\partial}{\partial x} - \nu^2 u_x\frac{\partial}{\partial x}]\delta u;$$

$$\delta\varepsilon_{12} = [-\frac{\nu y}{2}\frac{\partial^2}{\partial x^2} - \frac{\nu^2 y}{2}u_{xx}\frac{\partial}{\partial x} + \frac{\nu^2 y}{2}u_x\frac{\partial^2}{\partial x^2}]\delta u;$$

$$\delta\varepsilon_{13} = [-\frac{\nu z}{2}\frac{\partial^2}{\partial x^2} - \frac{\nu^2 z}{2}u_{xx}\frac{\partial}{\partial x} + \frac{\nu^2 z}{2}u_x\frac{\partial^2}{\partial x^2}]\delta u.$$

Вычислим вариацию внутренней энергии стержня с помощью формулы

$$\delta W = \sigma_{11}\delta\varepsilon_{11} + 2\sigma_{22}\delta\varepsilon_{22} + 2\sigma_{12}\delta\varepsilon_{12} + 2\sigma_{13}\delta\varepsilon_{13}$$

и применим вариационный принцип виртуальных перемещений. В результате получим уравнение движения стержня

$$\begin{aligned}\rho(-u_{tt} + \nu^2 r^2 u_{ttxx}) + N_1 u_{xx} - \tilde{\mu}\nu^2 r^2 u_{xxxx} + N_2 u_x u_{xx} + \\ + \nu^2 r^2 N_3 u_{xx} u_{xxx} - \nu^2 r^2 N_4 (u_x u_{xx})_{xx} + N_5 u_x^2 u_{xx} + \\ + \frac{1}{2}\nu^2 r^2 N_6 (u_x u_{xx}^2)_x - \frac{1}{2}\nu^2 r^2 N_7 (u_x^2 u_{xx})_{xx} - \\ - \frac{1}{2}\nu^4 r^4 N_8 ((u_{xx})^3)_{xx} = 0,\end{aligned} \tag{2}$$

где

$$N_1 = \tilde{\lambda}(1-2\nu)^2 + 2\tilde{\mu}(1+2\nu^2); \; N_2 = 3(1-2\nu)(1+2\nu^2)\tilde{\lambda} + 6\tilde{\mu}(1-2\nu^3);$$

$$N_3 = (1-2\nu)\tilde{\lambda} + 2\tilde{\mu}(1-\nu); \; N_4 = \tilde{\lambda}(1-2\nu) + 2\tilde{\mu}(1-2\nu);$$

$$N_5 = \frac{3}{2}\tilde{\lambda}(1+2\nu^2)^2 + 3\tilde{\mu}(1-2\nu^4); \; N_6 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}(1+\nu^2);$$

$$N_7 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}(1+\nu^2); \; N_8 = \tilde{\lambda} + 2\tilde{\mu}, \; r^2 = z^2 + y^2.$$

Преобразуем уравнение (2) к безразмерным переменным

$$\xi = \frac{x}{L} - \frac{c}{L}t; \quad \tau = \varepsilon\frac{c}{L}t; \quad u^* = \frac{u}{A}.$$

Полагаем, что длина деформационной волны L намного больше ее амплитуды A, параметр $\varepsilon = L/A << 1$, а константы α, β и поперечный размер d стержня удовлетворяют отношениям порядка

$$\frac{\alpha c}{\beta^2 L} = O(\varepsilon); \quad \frac{d}{L} = O(\sqrt{\varepsilon}). \tag{3}$$

Применим в (2) разложение

$$u = u_0 + \varepsilon u_1 + \varepsilon^2 u_2 + \ldots, \tag{4}$$

получим уравнение

$$\frac{\rho c^2}{E}[-u_{\xi\xi} + 2\varepsilon u_{\xi\tau} - \varepsilon^2 u_{\tau\tau} + \varepsilon\nu^2 I(u_{\xi\xi\xi\xi} - 2\varepsilon u_{\xi\xi\xi\tau} + \varepsilon^2 u_{\xi\xi\tau\tau})] +$$

$$+(1-\frac{\alpha a_0}{\beta})u_{\xi\xi}-\frac{\varepsilon\nu^2 I}{2(1+\nu)}(1-\frac{\alpha}{\beta})u_{\xi\xi\xi\xi}+\varepsilon(3-\frac{\alpha a_3}{\beta})u_\xi u_{\xi\xi}+$$

$$+\frac{\alpha c}{\beta^2 l}(\varepsilon\frac{\partial}{\partial\tau}-\frac{\partial}{\partial\xi})\cdot[a_0u_{\xi\xi}-\frac{\varepsilon\nu^2 I}{2(1+\nu)}u_{\xi\xi\xi\xi}+\varepsilon a_3u_\xi u_{\xi\xi}]=0,$$

описывающее динамику точек стержня.

Применение формул (3) и (4) дает уравнение

$$\left[-\frac{\rho c^2}{E}+\left(1-\frac{\alpha a_1}{\beta}\right)\right]u_{0\xi\xi}=0,$$

в котором $a_1=\frac{2}{3}(1+\nu)$ и $u_{0\xi\xi}\neq 0$, поэтому значение скорости продольной волны деформации

$$c=\sqrt{\frac{E}{\rho}[1-\frac{2\alpha(1+\nu)}{3\beta}]}.$$

Учет первого приближения позволяет вывести для определения компоненты $u_{0\xi}$ эволюционное уравнение Кортевега де Вриза – Бюргерса (КДВ) вида

$$\psi_\tau+b_1\psi\psi_\xi+b_2\psi_{\xi\xi}+b_3\psi_{\xi\xi\xi}=0, \qquad (5)$$

где

$$\psi=u_{0\xi};\qquad b_1=\frac{E(3\beta-\alpha a_2)}{2\rho c^2\beta};\quad b_2=-\frac{E\alpha a_1}{2\rho c\beta^2 l\varepsilon};$$

$$a_2=2(1-\nu^2);\qquad b_3=\nu^2 I[\frac{1}{2}-\frac{E(\beta-\alpha)}{4\rho c^2\beta(1+\nu)}].$$

Формула для точного решения уравнения (5) имеет вид

$$\psi=-\frac{12b_2k_1^2}{b_1}\,th^2(\frac{k_1\xi-\omega\tau}{2})+\frac{6b_3k_1}{5b_1}\,th(\frac{k_1\xi-\omega\tau}{2})+\frac{12b_2k_1^2}{b_1}+\frac{6b_3k_1}{5b_1};$$

$$k_1=\pm\frac{b_3}{5b_2};\qquad \omega=\frac{6b_3^3}{125b_2^2}.$$

С помощью обозначений

$$c_1=-\frac{12\,b_2k_1^2}{b_1};\qquad c_2=\frac{6\,b_3k_1}{5b_1};\qquad c_3=\frac{12\,b_2k_1^2}{b_1}+\frac{6\,b_3k_1}{5b_1}$$

получим следующее выражение:

$$\psi=c_1th^2(\frac{k_1\xi-\omega\tau}{2})+c_2th(\frac{k_1\xi-\omega\tau}{2})+c_3.$$

Если $\frac{\alpha}{\beta}<1$, то $b_1>0;\ b_2>0;\ b_3<0;\ \omega<0.$

Найдем параметры c_1, c_2, c_3:

$$c_1=-\frac{12b_3^2}{25b_1b_2};\ c_1<0;\ c_2=\pm\frac{6b_3^2}{25b_1b_2},$$

знак c_2 совпадает со знаком k_1

$$c_3=\frac{12b_3^2}{25b_1b_2}\pm\frac{6b_3^2}{25b_1b_2}=\frac{6b_3^2}{25b_1b_2}(2\pm1),\ c_3>0.$$

Если знак выбран “+”, то с учетом неравенств $b_3<0$ и $k_1<0$ получим функцию:

$$\psi=c_1th^2(\frac{|k_1|\xi-|\omega|\tau}{2})-c_2th(\frac{|k_1|\xi-|\omega|\tau}{2})+c_3,$$

где $c_3 = \frac{12b_2b_3^2}{25b_1b_2^2} + \frac{6b_3b_3}{25b_1b_2} = \frac{18b_3^2}{25b_1b_2}$.

Применяя условие $\theta \to -\infty$, получим, что $\psi \to c_1 - c_2 + c_3$, где $\theta = |k_1|\xi - |\omega|\tau$, а

$$c_1 - c_2 + c_3 = -\frac{12b_3^2}{25b_1b_2^2} + \frac{6b_3^2}{25b_1b_2^2} + \frac{18b_3^2}{25b_1b_2^2} = \frac{12b_3^2}{25b_1b_2^2}.$$

При $\theta \to +\infty$ $\psi \to c_1 + c_2 + c_3 = -\frac{12b_3^2}{25b_1b_2^2} - \frac{6b_3^2}{25b_1b_2^2} + \frac{18b_3^2}{25b_1b_2^2} = 0.$

Производная функции ψ имеет вид

$$\psi'_\theta = -\frac{1}{ch^2(\frac{|k_1|\xi - |\omega\tau|}{2})} \frac{24b_3^2}{25b_1b_2^2} (th(\frac{|k_1|\xi - |\omega\tau|}{2}) + \frac{1}{4}).$$

Положим $\psi'_\theta = 0$, тогда $th(\frac{|k_1|\xi - |\omega\tau|}{2}) = -\frac{1}{4}$ и точку максимума $\theta_{кр}$ найдем, решая уравнение уравнения $th\frac{\theta}{2} = -\frac{1}{4}$.

Максимальное значение $\psi_{\max}(\frac{\theta_{кр}}{2}) = \frac{3}{4}\frac{b_3^2}{b_1b_2^2}$. Установленное решение представляет собой распространяющуюся в стержне ударную волну растяжения $(\psi > 0)$, изображенную на рисунке 1.

Перейдем к размерным переменным

$$\theta = k_1\xi - \omega\tau = \frac{k_1}{L}(x - ct - \frac{\omega}{k_1}\varepsilon ct).$$

и вычислим величину поправки $\frac{\omega}{k_1}\varepsilon$ к значению скорости волны деформации.

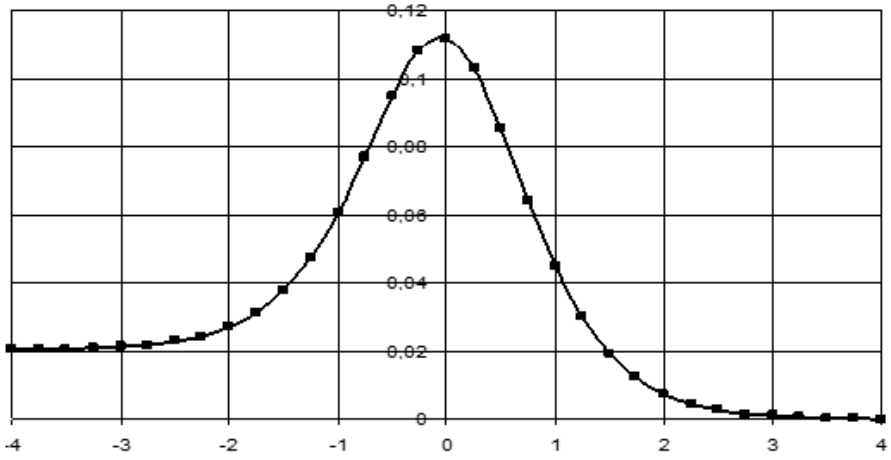


Рис. 1. Уединенная волна деформации в линейно-вязкоупругом стержне при линейно-упругих объемных деформациях

Физико-механические свойства нелинейного стержня при линейно-упругих объемных деформациях опишем уравнениями теории ползучести в виде

$$\sigma_{ij}(t) = \lambda\theta\delta_{ij} + 2\mu\varepsilon_{ij} - 2\mu\alpha\int_{-\infty}^{t} e^{-\beta(t-\tau)}[1 + \gamma\varepsilon_u^2(\tau)]e_{ij}(\tau)d\tau, \qquad (6)$$

Для упрощения (6) применим разложения в ряды Тейлора функций $[1+\gamma\varepsilon_u^2(\tau)]e_{ij}(\tau)$

по степеням (t-τ), получим уравнения состояния в виде:

$$\sigma_{ij} = \tilde{\lambda}\theta\delta_{ij} + 2\tilde{\mu}\varepsilon_{ij} + 2\gamma\mu p(\varepsilon_u^2 e_{ij}),$$

где $\tilde{\lambda} = \lambda - \frac{2\mu}{3}p$; $\tilde{\mu} = \mu(1+p)$; $p = \frac{\alpha}{\beta^2}\frac{\partial}{\partial t} - \frac{\alpha}{\beta}$.

Вычислим компоненты девиатора деформаций, их вариации и найдем вариацию внутренней энергии

$$\delta W = \sigma_{11}\delta\varepsilon_{11} + 2\sigma_{22}\delta\varepsilon_{22} + 2\sigma_{12}\delta\varepsilon_{12} + 2\sigma_{13}\delta\varepsilon_{13},$$

линейная часть которой

$$\delta W_л = \{-[\tilde{\lambda}(1-2\nu) + 2\tilde{\mu} - 2\nu((1-2\nu)\tilde{\lambda} - 2\mu\nu)]u_{xx} + 2\tilde{\mu}\frac{\nu^2 r^2}{2}u_{xxxx}]\delta u,$$

а нелинейная –

$$\delta W_н = \{-B_1 u_x u_{xx} - \nu^2 r^2(\tilde{\lambda} + 2\tilde{\mu})u_{xx}u_{xxx} - 2\mu\gamma p(\varepsilon_u^2 e_{11})_x - 2A_1 u_x u_{xx} -$$
$$-\frac{3}{2}B_1 u_x^2 u_{xx} - \frac{\nu^2 r^2}{2}(\tilde{\lambda} + 2\tilde{\mu})(u_x u_{xx}^2)_x - 2\mu\gamma p(\varepsilon_u^2 e_{11}u_x)_x +$$
$$+\nu^2 r^2 A_1(u_x u_{xx})_{xx} + \nu^2 r^2\frac{B_1}{2}(u_x^2 u_{xx})_{xx} + \frac{\nu^4 r^4}{2}(\tilde{\lambda} + 2\tilde{\mu})(u_{xx}^3)_{xx} +$$
$$+\nu^2 r^2 2\mu\gamma p(\varepsilon_u^2 e_{11}u_{xx})_{xx} + 2[\nu B_2 u_x u_{xx} + \nu^3 r^2\tilde{\lambda}u_{xx}u_{xxx} + 2\mu\nu\gamma p(\varepsilon_u^2 e_{22})_x -$$
$$-2\nu^2 A_2 u_x u_{xx} - \frac{3\nu^2}{2}B_2 u_x^2 u_{xx} - \frac{\nu^4 r^2}{2}\tilde{\lambda}(u_x u_{xx}^2)_x - 2\nu^2\mu\gamma p(\varepsilon_u^2 e_{22}u_x)_x] -$$
$$-2\tilde{\mu}\frac{\nu^3 r^2}{2}(u_x u_{xx})_{xx} - 2\mu\gamma p\nu y(\varepsilon_u^2 e_{12})_{xx} + \tilde{\mu}\nu^3 r^2 2u_{xx}u_{xxx} -$$
$$-2\tilde{\mu}\frac{\nu^4 r^2}{2}(u_x u_{xx}^2)_x - 2\mu\gamma p\nu^2 y(\varepsilon_u^2 e_{12}u_{xx})_x - \mu\nu^3 r^2(u_x u_{xx})_{xx} +$$
$$+2\tilde{\mu}\frac{\nu^4 r^2}{2}(u_x^2 u_{xx})_{xx} + 2\mu\gamma p\nu^2 y(\varepsilon_u^2 e_{12}u_x)_{xx} - 2\mu\gamma p\nu z(\varepsilon_u^2 e_{13})_{xx} -$$
$$-2\mu\gamma p\nu^2 z(\varepsilon_u^2 e_{13}u_{xx})_x + 2\mu\gamma p\nu^2 z(\varepsilon_u^2 e_{13}u_x)_{xx}\}\delta u,$$

Здесь введены обозначения

$$A_1 = \tilde{\lambda}(1-2\nu) + 2\tilde{\mu}; \qquad B_1 = (1+2\nu)\tilde{\lambda} + 2\tilde{\mu};$$
$$A_2 = (1-2\nu)\tilde{\lambda} + 2\tilde{\mu}\nu; \qquad B_2 = (1+2\nu^2)\tilde{\lambda} + 2\tilde{\mu}\nu^2.$$

Складывая линейную и нелинейную части, получаем полную вариацию

$$\delta W = \{-N_1 u_{xx} + \tilde{\mu}\nu^2 r^2 u_{xxxx} - N_2 u_x u_{xx} - \nu^2 r^2 N_3 u_{xx}u_{xxx} +$$
$$+\nu^2 r^2 N_4(u_x u_{xx})_{xx} - N_5 u_x^2 u_{xx} - \frac{\nu^2 r^2}{2}N_6(u_x u_{xx}^2)_x + \frac{\nu^2 r^2}{2}N_7(u_x^2 u_{xx})_{xx} +$$
$$+\frac{\nu^4 r^4}{2}N_8(u_{xx}^3)_{xx} - 2\mu\gamma p[(\varepsilon_u^2)_x(e_{11} - 4\nu e_{22} + e_{11}u_x + 2\nu^2 e_{22}u_x +$$
$$+\nu^2 y e_{12}u_{xx} + \nu^2 z e_{13}u_{xx}) + \varepsilon_u^2(e_{11} - 4\nu e_{22} + e_{11}u_x + 2\nu^2 e_{22}u_x +$$
$$+\nu^2 y e_{12}u_{xx} + \nu^2 z e_{13}u_{xx})_x + \frac{\partial}{\partial x}((\varepsilon_u^2)_x(\nu y e_{12} + \nu z e_{13} - \nu^2 r^2 e_{11}u_{xx} -$$
$$-\nu^2 y e_{12}u_x - \nu^2 z e_{13}u_x) + \varepsilon_u^2(\nu y e_{12x} + \nu z e_{13x} - \nu^2 r^2(e_{11}u_{xx})_x -$$
$$-\nu^2 y(e_{12}u_x)_x - \nu^2 z(e_{13}u_x)_x))]\}\delta u.$$

С учетом выражения для δW из вариационного принципа виртуальных переме-

щений найдем уравнение движения стержня:

$$\rho(-u_{tt}+\nu^2r^2u_{ttxx})+N_1u_{xx}-\tilde{\mu}\nu^2Iu_{xxxx}+N_2u_xu_{xx}+\nu^2r^2N_3u_{xx}u_{xxx}-$$

$$-\nu^2r^2N_4(u_xu_{xx})_{xx}+N_5u_x^2u_{xx}+\frac{1}{2}\nu^2r^2N_6(u_xu_{xx}^2)_x-\frac{1}{2}\nu^2r^2N_7(u_x^2u_{xx})_{xx}-$$

$$-\frac{1}{2}\nu^4r^4N_8(u_{xx}^3)_{xx}+2\mu\gamma\rho\{\frac{\partial}{\partial x}[\frac{1}{3}(1+u_x)(2(1+\nu)u_x+(1-\nu^2)u_x^2-$$

$$-\frac{1}{2}(1-\nu^2)u_x^2)(2\nu^2u_x-4\nu))Q+((\frac{1}{3}\nu^2u_{xx}^2(1+u_x)-\frac{1}{6}\nu^2u_{xx}^2(2\nu^2u_x-$$

$$-4\nu)+\frac{1}{2}\nu^2(\nu^2u_xu_{xx}^2-\nu u_{xx}^2))\cdot Q]+\quad[(-\frac{1}{3}\nu^2u_{xx}(2(1+\nu)u_x+(1-\nu^2)u_x^2)+$$

$$+\frac{1}{2}(\nu-\nu^2u_x)\cdot(\nu^2u_xu_{xx}-\nu u_{xx}))\cdot Q-\frac{1}{2}\nu^4r^4N_8(u_{xx}^3)_{xx}+2\mu\gamma p\{\frac{\partial}{\partial x}[(\frac{1}{3}(1+u_x)+\frac{1}{3}\nu^4u_{xx}^3Q]_{xx}\}=0,$$

где

$$N_1=\tilde{\lambda}(1-2\nu)^2+2\tilde{\mu}(1+2\nu^2);\ N_2=3(1-2\nu)(1+2\nu^2)\tilde{\lambda}+6\tilde{\mu}(1-2\nu^3);$$

$$N_3=(1-2\nu)\tilde{\lambda}+2\tilde{\mu}(1-\nu);\ \ N_4=\tilde{\lambda}(1-2\nu)+2\tilde{\mu}(1-2\nu);$$

$$N_5=\frac{3}{2}\tilde{\lambda}(1+2\nu^2)^2+3\tilde{\mu}(1-2\nu^4);\ N_6=(1+2\nu^2)\tilde{\lambda}+2\tilde{\mu}(1+\nu^2);$$

$$N_7=(1+2\nu^2)\tilde{\lambda}+2\tilde{\mu}(1+\nu^2);\ N_8=\tilde{\lambda}+2\tilde{\mu}.$$

$$Q=R_1+R_2+R_3;\ \ R_1=\frac{1}{3}[2(1+\nu)u_x+(1-\nu^2)u_x^2]^2\ ;\ \ R_3=\frac{1}{3}\nu^4u_{xx}^4\ ;$$

$$R_2=\frac{2}{3}\nu^2u_{xx}^2[2(1+\nu)u_x+(1-\nu^2)u_x^2]^2+(\nu^2u_xu_{xx}-\nu u_{xx})^2.$$

В нулевом приближении метода возмущений получим равенство

$$[-\frac{\rho c^2}{E}+(1-\frac{\alpha a_1}{\beta})]u_{0\xi\xi}=0,$$

Здесь $a_1=\frac{2}{3}(1+\nu).$

Скорость волны деформации вычисляется по формуле:

$$c=\sqrt{\frac{E}{\rho}[1-\frac{2\alpha}{3\beta}(1+\nu)]}.$$

В первом приближении метода возмущения получаем модифицированное уравнение КДВ:

$$\psi_\tau+b_1\psi\psi_\xi-b_2\psi^2\psi_\xi+b_3\psi_{\xi\xi}+b_4\psi_{\xi\xi\xi}=0, \qquad (7)$$

где

$$\psi=u_{0\xi};\qquad b_1=m(3-\frac{\alpha a_2}{\beta});\ \ m=\frac{E}{2\rho c^2};$$

$$b_2=\frac{m\alpha\gamma\varepsilon a_3}{\beta};\qquad b_3=-\frac{m\alpha c a_1}{\beta^2L\varepsilon};\qquad b_4=m\nu^2I[\frac{1}{2m}-\frac{\beta-\alpha}{2\beta(1+\nu)}];$$

$$a_2=2(1-\nu^2);\qquad a_3=\frac{8}{3}(1+\nu^2)(1+2\nu).$$

Решение уравнения (7) имеет вид:

$$\psi=\pm\frac{k_1}{n}\sqrt{\frac{6b_4}{b_2}}\mathrm{th}(\frac{k_1\xi-\omega\tau}{n})]\mp\frac{b_3}{\sqrt{6b_2b_4}}+\frac{b_1}{2b_2},$$

где $\omega = (\frac{1}{4}\frac{b_1^2}{b_2} - \frac{1}{6}\frac{b_3^2}{b_4})k_1 - \frac{2b_4}{n^2}k_1^3;\ n \in Z;$ k_1 – произвольный параметр.

График волны деформации представлен на рисунке 2. Вычисляя поправку к скорости волны, получаем $\frac{\omega}{k_1}\varepsilon$.

Нелинейность, дисперсия и диссипация в результате компенсации их влияния не волновой процесс приводят к образованию в стержнях с реологическими свойствами уединенных деформационных волн, причем их скорость возрастет с ростом амплитуды.

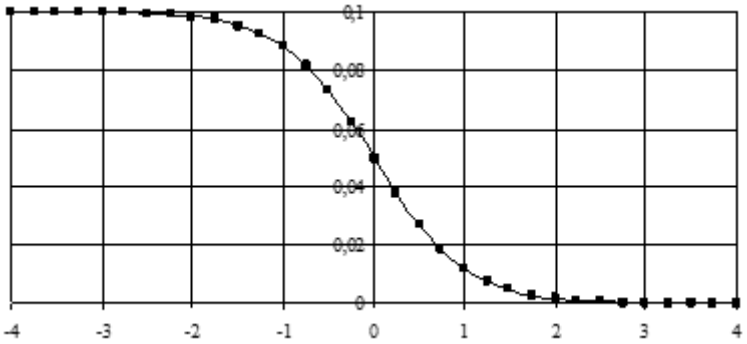


Рис. 2. Уединенная волна продольной деформации в нелинейно-вязкоупругом стержне при линейно-упругих объемных деформациях

Теоретически полученные формулы для скорости волны могут быть использованы для совершенствования акустических способов обнаружения микродефектов в материале вязкоупругих стержней.

Литература

1. Аршинов Г.А. Продольные нелинейные волны в вязкоупругих стержнях, пластинах и цилиндрических оболочках / Г. А. Аршинов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2003. – №02(002). С. 1–15. – IDA [article ID]: 0020302001. – Режим доступа: http://ej.kubagro.ru/2003/02/pdf/01.pdf, 0,938 у.п.л.

2. Аршинов Г.А. Математическая модель продольных колебаний и эволюционные уравнения для линейно-вязкоупругого стержня / Г. А. Аршинов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2004. – №03(005). С. 144–150. – IDA [article ID]: 0050403010. – Режим доступа: http://ej.kubagro.ru/2004/03/pdf/10.pdf, 0,438 у.п.л.

3. Аршинов Г.А. Оценка экономической и эксплуатационной надежности строительных сооружений на основе исследования волновых характеристик нелинейных вязкоупругих стержневых элементов конструкций / Г.А. Аршинов, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2019. – №09(153). С. 122–131. – IDA [article ID]: 1531909011. – Режим доступа: http://ej.kubagro.ru/2019/09/pdf/11.pdf, 0,625 у.п.л.

Сведения об авторе

Аршинов Георгий Александрович, доктор технических наук, доцент, профессор кафелры комьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: arshinov_kts@mail.ru.

Атласов Игорь Викторович,
Орехов Павел Васильевич

ВАРИАНТ ОПТИМИЗАЦИИ НАПРАВЛЕНИЯ АВТОТРАНСПОРТНОГО ДОРОЖНОГО ПОТОКА (ПОЛОСЫ ДВИЖЕНИЯ) С ПОМОЩЬЮ ПРЕДВИДЕНИЯ ДОРОЖНОГО ЗАТОРА НА РЕГУЛИРУЕМОМ ПЕРЕКРЕСТКЕ, ОСНАЩЕННОМ ВИДЕОНАБЛЮДЕНИЕМ

В настоящей статье рассматривается вопрос оптимизации одного из инструментов организации дорожного регулирования, такого как эффективная работа транспортного перекрестка, с насыщенным трафиком, в качестве вспомогательных средств помимо светофора берем установленную систему видеонаблюдения перекрестка с возможностью видеофиксации и визуального мониторинга дорожного движения.

Постановка задачи оптимизации. Работа светофора на перекрестке с выбранной производной моделью перекрестка состоит в том, чтобы не было больших пробок. Будем считать, что перед камерой светофора постоянно проходят, или стоят, машины. Пусть стоящие рядам перед светофором машины в количестве $\boldsymbol{m_1}$ заставляют увеличивать время работы зеленого цвета на $\boldsymbol{\Delta t}$. А прибавление к $\boldsymbol{m_1}$ еще одной заставляют увеличивать время работы зеленого цвета на $\boldsymbol{2\Delta t}$. И так далее, до $\boldsymbol{m_2}$. Итак, $\boldsymbol{m_1}$ – то минимальное значение машин, когда требуется вмешательство в работу светофора и $\boldsymbol{m_2}$ – то максимальное значение машин, которое может видеть камера работающая параллельно со светофором. Пусть число $\boldsymbol{m}$ лежит в промежутке $\boldsymbol{m_1 \le m \le m_2}$. Далее, чтобы решить задачу будем считать, что машины либо стоят друг за другом, либо находятся на расстоянии целого числа машинно-мест (без машин) друг от друга. Итак, наша задача - определить вероятность того, что перед светофором будет находиться ровно $\boldsymbol{m}$ машин и после них такого сочетания подряд идущих машин уже не будет, так как после $\boldsymbol{m}$ машины будет обязательно хоть одно свободное место, куда может проехать хоть одна машина. То есть скопление машин происходит только перед светофором. Теперь рассмотрим работу камеры. Камера, начиная с некоторого момента времени (это время, когда машин практически нет), фиксирует общее количество прошедших машин и пустых машинно – мест. То есть перед камерой как бы проходит полоса, разбитая на отдельные участки одинаковой фиксированной длины на каждом из которых может находиться машина с вероятностью $\boldsymbol{p}$ и не находиться с вероятностью $\boldsymbol{q = 1 - p}$. Будем считать, что событие, состоящее в том, что машина находится на некотором участке, или нет, никак не связано с тем, что было на предыдущих участках.

Итак, имеется полоса из k машинно-мест, количество которых не постоянная величина, так как связана со скоростью движения потока машин и с временем начала отчета этого потока.

Условие из математической части. Напомним сведения о производящих функциях. Пусть дискретная целочисленная случайная величина ζ задана своим законом распределения - $P(\zeta = k) = w_k,\ k = 0, \dots, \infty$. В этом случае для $|u| < 1$ определена производящая функция $\varphi(u) = \sum_{k=0}^{\infty} w_k u^k$, которая мажорируется сходящимся рядом $\sum_{k=0}^{\infty} w_k$, не зависящем от u. То есть, ряд $\sum_{k=0}^{\infty} w_k u^k$ сходится равномерно. Аналогично, доказывается равномерная сходимость ряда из производных любого порядка. И отсюда следует формула для вычисления вероятностей $w_n = \frac{1}{n!}\frac{\partial^n \varphi(u)}{\partial u^n}\Big|_{u=0}$.

Переходим к решению математической части. Фиксируем m. Обозначим через $p_k \overset{def}{=} p_k^{(m)}$ вероятность того, что имеется только одна серия из m машин, которая

закончится на k-м участке полосы (то есть в полосе всего k машинно- мест). Через $q_k \overset{def}{=} q_k^{(m)}$ обозначим вероятность того, что среди первых k машинно-мест не будет ни одной серии из m последовательно находящихся машин. Очевидно, что при $k < m$ величина $p_k = 0$ и $q_k = 1$. Вероятность появления хотя бы одной серии из m подряд находящихся на полосе машин за первые k машинно-мест равна $1 - q_k$. Такая серия впервые может произойти при s-м испытании с вероятностью p_s, $(s = m, \dots, k)$.

События, имеющие указанные вероятности, несовместные, поэтому имеет место равенство $1 - q_k = \sum_{s=m}^{k} p_s$, или $1 - q_{k-1} = \sum_{s=m}^{k-1} p_s$.

Вычитая одно неравенство из другого, получим: $q_k - q_{k-1} = -p_k$ (1)

Обозначим $G(u) \overset{def}{=} G^{(m)}(u) = \sum_{k=0}^{\infty} p_k u^k, R(u) \overset{def}{=} R^{(m)}(u) = \sum_{k=0}^{\infty} q_k u^k$

Умножая обе части выражения (1) на u^k и суммируя по k от единицы до бесконечности и пользуясь равенством $p_0 + q_0 = 1$, получаем неравенства

$$\sum_{k=1}^{\infty} q_k u^k - \sum_{k=1}^{\infty} q_{k-1} u^k = -\sum_{k=1}^{\infty} p_k u^k$$
$$\sum_{k=0}^{\infty} q_k u^k - q_0 - u\sum_{k=1}^{\infty} q_{k-1} u^{k-1} = -\sum_{k=0}^{\infty} p_k u^k + p_0$$
$$\sum_{k=0}^{\infty} q_k u^k - (q_0 + \mathrm{p}_0) - u\sum_{i=0}^{\infty} q_i u^i = -\sum_{k=0}^{\infty} p_k u^k$$
$$R(u) - 1 - uR(u) = -G(u)$$

Поэтому, $G(u) = 1 - (1 - u)R(u)$ (2)

При $k \geq m$ серия из m последовательных находящихся на полосе машин может не возникнуть только одним из следующих m способов: сначала имеет место серия из $s - 1$ последовательных находящихся на полосе машин, затем пустое машинно-место, и наконец, среди оставшихся $k - s$ машинно-мест не будет серии из m последовательных находящихся на полосе машин $(s = 1, \dots, m)$. Вероятности указанных независимых событий соответственно равны p^{s-1}, q_{k-s} и $q = 1 - p$, поэтому справедливы равенства

$$q_k = q\sum_{s=1}^{m} p^{s-1} q_{k-s}, k = m, \dots, \infty$$

Так как при $k < m$ имеем $q_k = 1$, то умножив последнее равенство на u_k и суммируя по k, получим:

$$\sum_{k=m}^{\infty} q_k u^k = q\sum_{s=1}^{m} p^{s-1} u^s \sum_{k=m}^{\infty} q_{k-s} u^{k-s} = q\sum_{s=1}^{m} p^{s-1} u^s \sum_{j=m-s}^{\infty} q_j u^j =$$
$$= q\sum_{s=1}^{m} p^{s-1} u^s \left(\sum_{j=m-s}^{m-1} q_j u^j + \sum_{j=m}^{\infty} q_j u^j\right) = q\sum_{s=1}^{m} p^{s-1} u^s \sum_{j=m-s}^{m-1} u^j +$$
$$+q\sum_{\mathrm{s}=1}^{m} p^{s-1} u^s \sum_{j=m}^{\infty} q_j u^j = q\sum_{s=1}^{m} p^{s-1} \sum_{j=m-s}^{m-1} u^{j+s} + +qu\sum_{j=m}^{\infty} q_j u^j \sum_{i=0}^{m-1} (pu)^i =$$
$$q\sum_{s=1}^{m} p^{s-1} \sum_{k=m}^{m+s-1} u^k + qu\sum_{j=m}^{\infty} q_j u^j \frac{1-(pu)^m}{1-pu} =$$
$$= qu^m \sum_{s=1}^{m} p^{s-1} \frac{1-u^{m+s}}{1-u} + \frac{qu(1-(pu)^m)}{1-pu} \sum_{j=m}^{\infty} q_j u^j +$$
$$= \frac{qu^m}{1-u}\left(\sum_{i=0}^{m-1} p^i - u^{m+1}\sum_{i=0}^{m-1} (pu)^i\right) + \frac{qu(1-(pu)^m)}{1-pu}\sum_{j=m}^{\infty} q_j u^j =$$
$$= \frac{qu^m}{1-u}\left(\frac{1-p^m}{1-p} - u^{m+1}\frac{1-(pu)^m}{1-pu}\right) + \frac{qu(1-(pu)^m)}{1-pu}\sum_{j=m}^{\infty} q_j u^j$$

Отсюда имеем:

$$\sum_{k=m}^{\infty} q_k u^k \left(1 - \frac{qu(1-(pu)^m)}{1-pu}\right) = \frac{qu^m}{1-u}\left(\frac{1-p^m}{1-p} - u^{m+1}\frac{1-(pu)^m}{1-pu}\right) =$$
$$= \frac{qu^m}{1-u}\frac{(1-p^m)(1-pu) - u^{m+1}(1-(pu)^m)q}{q(1-pu)}$$
$$\sum_{k=m}^{\infty} q_k u^k = \frac{1-pu}{1-u+qu(pu)^m}\frac{qu^m}{1-u} \times \frac{(1-p^m)(1-pu) - u^{m+1}(1-(pu)^m)q}{q(1-pu)} =$$
$$= \frac{u^m\left((1-p^m)(1-pu) - qu^{m+1}(1-p^m u^m)\right)}{(1-u+qp^m u^{m+1})(1-u)}.$$

Далее, так как при $k < m$ имеем $q_k = 1$, то:

$$\sum_{k=m}^{\infty} q_k u^k = \sum_{k=0}^{\infty} q_k u^k - \sum_{k=0}^{m-1} q_k u^k = \sum_{k=0}^{\infty} q_k u^k - \sum_{k=0}^{m-1} u^k = R(u) - \frac{1-u^m}{1-u}$$

Поэтому, $R(u) = \sum_{k=m}^{\infty} q_k u^k + \frac{1-u^m}{1-u} = \frac{u^m\left((1-p^m)(1-pu)-qu^{m+1}(1-p^m u^m)\right)}{(1-u+qp^m u^{m+1})(1-u)} + \frac{1-u^m}{1-u}$.

Согласно (2), имеем $G(u) = 1-(1-u)R(u) =$

$$= 1-(1-u)\left(\frac{u^m\left((1-p^m)(1-pu)-qu^{m+1}(1-p^m u^m)\right)}{(1-u+qp^m u^{m+1})(1-u)} + \frac{1-u^m}{1-u}\right) =$$

$$= u^m\left(1-\frac{(1-p^m)(1-pu)-qu^{m+1}(1-p^m u^m)}{1-u+qp^m u^{m+1}}\right) =$$

$$= u^m\frac{1-u+qp^m u^{m+1}-(1-p^m)(1-pu)-qu^{m+1}(1-p^m u^m)}{1-u+qp^m u^{m+1}} =$$

$$= u^m\frac{1-u+qp^m u^{m+1}-1+pu+p^m-up^{m+1}-qu^{m+1}+qp^m u^{2m+1}}{1-u+qp^m u^{m+1}} =$$

$$= u^m\frac{p^m-up^{m+1}+(qp^m u^{m+1}-qu)+(qp^m u^{2m+1}-qu^{m+1})}{1-u+qp^m u^{m+1}} =$$

$$= \frac{u^m\left(p^m(1-up)-qu(1+u^m)(1-p^m u^m)\right)}{1-u+qp^m u^{m+1}}$$

Итак, доказана формула $G^{(m)}(u) = \frac{u^m\left(p^m(1-up)-qu(1+u^m)(1-p^m u^m)\right)}{1-u+qp^m u^{m+1}}$ (3)

Итак, получена удобная формула для вычисления вероятности того, что серия из m машин, которая закончится на k-м участке полосы

$$p_n^{(m)} = \frac{1}{n!}\frac{\partial^n G^{(m)}(u)}{\partial u^n}\Big|_{u=0} = \frac{1}{n!}\left(\frac{u^m p^m(1-up)-qu^{2m}(1+u^m)(1-p^m u^m)}{1-u+qp^m u^{m+1}}\right)_u^{(n)}\Bigg|_{u=0}.$$

Рассмотрим, как приведенную формулу применить.

1. Сначала рассмотрим наибольшее возможное число машин N, которые могут проехать от начала отсчета до конца отсчета. Для этого разделим временное расстояние между двумя точками отсчета и разделим на минимальную скорость, которая может быть на участке.

2. Далее, найдем вероятность p из следующих соображений - находим среднее количество машин появляющееся на выделенном участке (для одной машины).

3. Выбираем число m, такое что можно назвать состояние пробкой.

4. Далее, для всех возможных $n \in [m, N]$ находим $p_n^{(m)}$ и выбираем наименьшее $n_0 \in [1, N]$, такое чтобы было справедливо равенство

$$p_{n_0}^{(m)} = \max_{n\in[m,N]} p_n^{(m)}.$$

5. Далее, камера следит за полосой дороги. До того, как пройдена $n_0 - m$ позиция, автоматически включается более длинный зеленый сигнал светофора для машин.

6. После этого начинаем новый отчет позиций на полосе, может с новым p.

Благодаря использованию приведенной методики и математической модели с представленным алгоритмом функционирования, можно сделать вывод о большой степени эффективности регулирования вспомогательных систем выбранной модели перекрестка дорожного движения для оптимизации дорожного потока с предвидением образования дорожного затора. Иными словами, мы заранее включаем разрешающий сигнал светофора для движения транспорта в выбранном направлении, предвидя образование дорожного затора.

Литература

1. Отчет федеральной государственной службы статистики «Наличие транспортных средств по Российской Федерации 2000-2019» [Электронный ресурс]. URL: https://rosstat.gov.ru/folder/23455 (Дата обращения: 17.02.2021).

2. Меньших В.В. Алгоритм классификации потенциальных мест размещения сил и средств контроля безопасности дорожного движения / В.В. Меньших, П.В. Орехов // Вестник Воронежского института ФСИН России. – 2016. – № 1. – С. 38–43.

3. Нормирование проезжей части [Электронный ресурс]. URL: https://ru.qaz.wiki/wiki/Road_space_rationing (Дата обращения: 17.02.2021).

4. Крамер Г. Математические методы статистики. Москва, Мир, 1976.

5. Уишарт Дж., Бартлетт М.С. (Wishart J., Bartlett M.S.) The distribution of the second order moment statistics in a normal system / / Proc. Cambridge Phil. Soc- 1932.- V. 28.- P. 455-459.

Сведения об авторах

Атласов Игорь Викторович, доктор физико-математических наук, профессор, профессор кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя; e-mail: mathematic1@ramber.ru.

Орехов Павел Васильевич, кандидат технических наук, старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя; e-mail: s.r.t@bk.ru.

Астафьев Евгений Рудольфович,
Варфоломеева Светлана Васильевна

ВЛИЯНИЕ И УЧЕТ СЕМИОТИЧЕСКИХ ОСОБЕННОСТЕЙ ЯЗЫКА МАТЕМАТИКИ НА ФОРМИРОВАНИЕ ПОЗНАВАТЕЛЬНЫХ И КОММУНИКАТИВНЫХ КОМПЕТЕНЦИЙ

Современная педагогика представляет собой совокупность нескольких разнонаправленных тенденций, с одной стороны, она опирается на классическую модель, с другой стороны, открыта новому. Для совершенствования научно-образовательной составляющей профессионально-педагогической деятельности требуется внедрение в образовательный процесс инновационных методов, средств и технологий, учитывающих многообразие языковых представлений различных знаний в полифункциональной образовательной среде.

Актуальным становится развитие комплексного (интегрального) мышления обучающихся, направленного, прежде всего, на формирование универсальных учебных действий, а также общекультурных и профессиональных компетенций, определенных в Федеральном государственном образовательном стандарте высшего образования.

Комплексный подход к обучению математике в вузе, и полилингвальный подход , являясь составляющими системно-деятельностного подхода, вместе позволяют выявить категориальные структуры процесса обучения математике как системообразующие универсальные средства обучения. Актуальным в представлении знаний становится понимание операциональных и предметных значений объектов, а также интерпретация их взаимных переходов на различных математических моделях. По этой схеме представления определим знания тройкой (мысль, знак, действие). Такая структура позволяет реальному материальному объекту по определенным существенным его признакам ставить в соответствие некоторый знак, который, осмыслив, получает значение символа в действии. Поскольку любая система письма языка может быть отнесена к одному из типов – фонетическому или иероглифическому, то в первом типе письма в качестве языковых единиц выделяют буквы, а во втором

типе – слоги или слова.

Анализируя алфавиты древнейших языков(финикийского, китайского), можно выявить логическую схему процесса присвоения объектам реальной природы определенных знаков (символов), называемых, в зависимости от семантико-синтаксических особенностей языка, буквами или иероглифами, с помощью которых строятся слова и выражения.

Для осуществления поставленной цели будут использоваться схемы образовательной деятельности, в которой выделяются следующие структурные компоненты: общество – культура – субъект – язык(знание, содержание образования) – объект (среда). Полученный результат должен быть интерпретирован с точки зрения практической целесообразности проекта и уровня сформированности общекультурных и профессиональных компетенций у обучающихся. При этом соотношение различных подходов к обучению математике следует рассматривать как основу проектирования и мониторинга приобретения ключевых компетенций.

Обучение математике в соответствии с этой схемой деятельности позволит применить знания всех наук, тесно связанных с математикой, способствует целостному восприятию окружающего мира и формированию духовно-нравственных атрибутов. В такой стратегии образования осуществляются процессы переноса знаний в много дисциплинарных исследованиях, фиксируются классы знаний, этапы и факторы познавательного процесса.

Математическое моделирование реализует культурологическую функцию в современном образовании, поскольку является методологической основой формирования умения гармоничного сочетания формального языка математики и неформального языка науки.

Генетическое родство алфавитов современных языков сравниваем по двум лингвистическим направлениям: финикийского и китайского языков. От финикийского алфавита происходят арамейский и греческий алфавиты, на основе которых в последующем были построены алфавиты еврейского, сирийского, арабского, латинского, кириллицы и т.д. Следовательно, для всех этих алфавитов характерны наиболее общие (категориальные) смысловые и знаковые принципы построения и применения их в грамматиках этих языков. Математическое осмысление этих знаков – геометрическая интерпретация и числовые значения – играет важную роль в семантико-синтаксическом упорядочении научных понятий и языковых текстов в соответствии с определенной логической схемой.

Простейшими геометрическими фигурами считаются точки, отрезки, углы, окружности и их дуги, а также различные их простые комбинации. Часто встречающиеся в математике два непересекающихся под различными углами отрезка, окружность и ее части, различные их комбинации являются символическими обозначениями расположенности соответствующих им объектов в объемлющем физическом пространстве. С древнейших времен именно с помощью этих геометрических фигур стали обозначать особые отношения человека к предметам материального и нематериального (духовного) мира. Так, например, пересекающимся под прямым углом двум отрезкам соответствует прямоугольная система координат, в которой на языке различных символов устанавливается связь между материальными предметами, геометрическими фигурами и их алгебраическими значениями.

В единичном круге с центром в точке пересечения этих отрезков дается интерпретация всех связей между отрезками и углами на языке тригонометрических функций и соответствующих формул. С другой стороны, в религиозно-философских учениях (верованиях) крест – это символ жизни, а круг – символ вечности. На математическом языке этому символу соответствует переменная «икс» X. В китайском

языке различные формы креста, с некоторыми добавлениями, определяют основные иероглифы, имеющие важное значение в обыденной жизни человека.

Функции геометрических фигур круга и прямоугольника оказываются почти сходными, и они, как символы алфавитов различных языков, несут почти одинаковые смысловые нагрузки. Кроме того, различные формы и дополнения креста определяют новые символы, иероглифы, буквы и соответствующие им предметные значения. Лексикологический анализ китайского языка показывает, что иероглифы, связанные с крестом, выражают преимущественно культурологические феномены и ценностно-смысловые категории жизненного пространства субъектов образовательной деятельности.

Подобным же образом происходит присваивание предметным значениям символических форм (букв) и в финикийском языке, которые с сохранением своих предметных значений трансформируются в буквы алфавитов основных мировых фонетических языков.

Итак, выявляя фундаментальные семантико-синтаксические связи между фонетическими и иероглифическими единицами (символами) алфавитов различных языков, с помощью определенных правил синтеза понятий, по одной и той же логической схеме, образуют новые слова, на основе которых строятся базисные предложения (аксиомы). Таким образом, аналогией действий выявляются наиболее общие семантико-синтаксические признаки структур алфавитов различных языков, позволяющие глубоко осмыслить фонетические и лингвистические основы современных языков с точки зрения их применения для построения программных языков в информатике и анализа структур текстов в математической лингвистике. Такой подход к образовательной деятельности способствует развитию интегрального мышления и формированию коммуникативных и математических компетенций у обучающихся.

Семиотика рассматривает три главных направления для изучения знака и знаковой системы: синтаксис (синтактика), семантика, прагматика.

Основываясь на аспектах семиотики и исследованиях психологов, установивших необходимость выделения трёх планов в овладении символикой: синтаксический, семантический и прагматический, необходимо для организации понимающего усвоения математики выделение всех трёх планов в овладении математической символикой.

При работе с математической символикой рассмотрен пример изучения понятия функции (на первых курсах училища или вуза). Согласно синтаксическому плану, преподаватель должен детально объяснить: правила написания нового символа; использование нового символа в сочетании с обозначением функции; место аргумента при использовании этого символа и др.

На этом этапе важно создать условия, которые бы позволили обучающимся осознать важность грамотного написания и использования нового символа. При этом задача преподавателя состоит в том, чтобы обучающиеся смогли понять смысл вводимых обозначений – новые действия над функциями.

Наконец, осуществляя прагматический план овладения символикой, преподаватель: учит «читать» обучающихся запись в виде символьных знаков; применять для решения задач формулы, с использованием новой системы обозначений; декодировать информацию в словесную или графическую форму; организовывать соот ветствующую работу обучающихся.

Критерием овладения символикой в прагматическом плане может служить умение обучающихся переходить от одной формы представления информации(символьной) к другим и обратно: от других форм представления – к символьной. Так, при изучении теоремы Лагранжа обучающимся после словесной формулировки теоремы предлагается сделать геометрическую иллюстрацию к данной теореме.

Практика показывает, что она может реализоваться только в совместной деятельности преподавателя и обучающихся.

Создание знаково-символической деятельности основано на специальной работе преподавателя совместно с обучающимися по формированию всех знаково-символических операций:

- Моделирование – знаково-символическая операция, которая состоит в объективном получении новой информации (познавательная функция) с помощью задействования знаково-символических средств, в которых использованы структурные, функциональные и генетические связи (изучение не самого объекта, а вспомогательной системы);
- Кодирование – знаково-символическая операция, которая передаёт и принимает сообщения (коммуникативная функция); умение записать информацию на основе знаково-символической формы;
- Схематизация – знаково-символическая операция (структурирование), которая позволяет ориентироваться в действительности;
- Замещение – знаково-символическая операция по оперированию не самим объектом, а его знаковым заместителем.

Таким образом, взаимосвязь понимания и знаково-символической деятельности способствует:

- применению различных схем представления явлений, понятий, фактов; созданию образа (форм) исследуемого предмета или явления;
- использованию эмпирического опыта (ассоциирование реальных объектов с абстрактными).

Важный момент заключается в том, чтобы связать формализованный знаковый язык математики, математического моделирования с содержанием математического знания, используя абстрактную точку зрения. Понимание этой связи предполагает освоение знаковой и объективно-реальной ситуации и помогает в осмыслении полученной информации.

В процессе формирования данного типа понимания, в частности, математического понятия, обучающийся для осознания словесного определения, использует весь свой накопленный опыт. При формулировании математического понятия практически необходимо вводить словесную интерпретацию этого понятия, формализовать запись, используя при этом знаковую и иллюстрационную символику (таблицы, рисунки, схемы, модели).

Реализация взаимосвязи понимания и знаково-символической деятельности обеспечивает повышение качества усвоения математического материала обучающимися, их осознанное восприятие, структурирование и запоминание, формирует познавательные и коммуникативные компетенции у обучающихся.

Литература

1. Волкова, Е.Е. Соотнесение традиционного и компетентностного подходов к обучению математике как основа проектирования и мониторинга приобретения ключевых компетенций / Е.Е. Волкова // Стандарты и мониторинг. – 2018. – № 4. – С. 39-44.

2. Ярахмедов, Г.А. Комплексный подход к математическому образованию в вузе: теория и методология: Монография / Г.А. Ярахмедов. – М.: АЛЕФ, 2017. – 340 с.

3. Варфоломеева, С.В. Использование оптимизационных методов в преподавании математики студентам гуманитарного профиля / С.В. Варфоломеева, Н.В. Головнина, В.В. Терехов // Наука. Техника. Технологии (политехнический вестник). – 2019. – № 3. – С. 320-325

Сведения об авторах

Астафьев Евгений Рудольфович, кандидат физико-математических наук, доцент, доцент кафедры математики (и информатики) Краснодарского высшего военного авиационного училища лётчиков имени Героя Советского Союза А.К. Серова; e-mail: eeast18@mail.ru.

Варфоломеева Светлана Васильевна, кандидат педагогических наук, доцент, профессор кафедры математики (и информатики), Краснодарского высшего военного авиационного училища имени Героя Советского Союза А.К. Серова; e-mail: varph2000@mail.ru.

Баранов Владимир Витальевич,
Журбин Григорий Евгеньевич

НЕКОТОРЫЕ ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Опыт последних боестолкновений с использованием беспилотных летательных аппаратов (БПЛА) в Нагорном Карабахе показал беспомощность наземной системы противовоздушных сил (ПВО) вооруженных сил (ВС) республики Армения. Вооруженные силы республики Азербайджан при помощи ВС республики Турция применили широкий спектр БПЛА, начиная от разведывательных БПЛА Elbit Hermes 450, Hermes 900, IAI Heron, IAI Searcher, барражирующих боеприпасов IAI Harop, Elbit SkyStriker и Orbiter 1K и средний ударный БПЛА Bayraktar [1].

Применение БПЛА сопровождались активным применением средств радиоэлектронной борьбы (РЭБ). Так, например, в ходе боевых действий была уничтожена станция РЭБ «Репеллент», защищавшая один из штабов ВС республики Армения. В уничтожении станции РЭБ большую роль сыграл БПЛА Bayraktar, выполнявший наведение артиллерийских систем. Тенденция активного применения средств РЭБ просматривается во всех вооруженных конфликтах с применением современных вооружений. Результаты массового применения БПЛА в Нагорном Карабахе приведены в [2].

В настоящее время ведутся разработки БПЛА, имеющих возможность применять средства поражения не только по наземным, но по воздушным целям. К таким БПЛА можно отнести тяжелый ударный БПЛА С-70 «Охотник». 27 сентября 2019г. Министерство обороны РФ сообщило о совместном полете самолета Су-57 и С-70.

Таким образом, воздушный бой между двумя БПЛА становится актуальным уже в настоящее время. Рассмотрим более подробно аспекты воздушного боя БПЛА. В составе возможного радиотехнического оборудования БПЛА можно выделить следующие компоненты:

- датчики обнаружения объектов противника;
- телекоммуникационное оборудование канала связи с оператором;
- комплекс радиоэлектронной борьбы.

К датчикам обнаружения объектов противника наиболее реалистично отнести пассивные локационные каналы, такие как: телевизионная прицельная система, оптоэлектронная прицельная система. На многие современные БПЛА так же устанавливается лазерный дальномер или система подсвета цели. Не исключено, что на тяжелые БПЛА могут устанавливаться и РЛС.

К телекоммуникационному оборудованию следует отнести телекоммуникационную информационную систему, охватывающую широкий рабочий диапазон частот, для

успешной отстройки от средств РЭБ противника и обеспечивающий устойчивый цифровой канал связи.

Комплекс радиоэлектронной борьбы, как правило, включает в себя пассивную систему радиотехнической разведки (РТР) и активный канал силового подавления. Силовой канал ставит помеху либо в заградительном, либо в прицельном режимах, а так же различные уводящие помехи.

Все перечисленные выше радиотехнические устройства являются потребителями электрической энергии, имеющейся на БПЛА в ограниченном количестве. С большой долей вероятности можно предположить, что тот, кто успешнее сможет реализовать потенциал энергетической установки БПЛА, тот и победит в воздушном бою с применением БПЛА. Распределение энергетического ресурса между локационными каналами подробно рассмотрено в [3,4].

Дальность радиосвязи определяется из уравнения Фрииса [5]:

$$d = \frac{\sqrt{P_T G_T G_R \lambda^2}}{(4\pi)^2 P_R},$$

где P_T – мощность, передаваемая для излучения в передающую антенну;

P_R – мощность, снимаемая с приемной антенны;

G_T и G_R – коэффициенты усиления приемной и передающей антенны;

λ - длина волны радиолинии.

С учетом возможной постановки противником радиопомех P_R наводимая в приемной антенне полезным сигналом должна превышать мощность наводимую помехой в заданном диапазоне частот.

Достоверность передачи определяется отношением числа правильно принятых элементов кодовых комбинаций, к числу переданных и так же зависит от соотношения сигнал / шум в приемнике радиолинии.

Для увеличения достоверности и помехоустойчивости радиолинии необходимо увеличивать долю, выделяемого ей, энергоресурса БПЛА. В то же время увеличение мощности излучения приведет к улучшению условий для работы РТР противника. В этом случае противник может перейти из режима заградительной помехи в режим прицельной или уводящей помехи и заблокировать каналы радиоуправления БПЛА в полном объеме, что приведет к невыполнению боевой задачи.

Эффективность радиоэлектронного противодействия можно оценить как энергетически, так и информационно. При энергетической оценке критерием подавления является уменьшение вероятности $P_1(y_1|x_1)$ правильного приема сообщения $\boldsymbol{x_1}$ по принятой реализации $\boldsymbol{y_1}$ до уровня 0,5.

Качество маскирующих и имитирующих радиопомех с использованием информационного критерия оценивается их энтропией. Помехи должны исключить возможность обнаружения полезного сигнала с вероятностью, превышающей заданное значение, при некоторых ограничивающих условиях. Непременным условием правильного функционирования систем информационного подавления является априорное знание полезного сигнала.

В рассматриваемом нами примере оператор БПЛА является по совместительству летчиком самолета Су-57, следовательно, возможности улучшения энергетических соотношений информационного канала за счет второй стороны так же ограничены размером летательного аппарата и его энерговооруженностью. Следовательно, задачу обеспечения безопасности информации с учетом требуемой дальности и достоверности информационного канала в условиях помех необходимо решать, опираясь только на оптимальное распределение имеющегося энергоресурса между каналом датчиков, информационным каналом (радиолиния) и силовым (канал РЭБ БПЛА).

В результате воздействия заградительной помехи аддитивную смесь дискретного сигнала информационного канала и помехи можно считать непрерывным сигналом. Аналитические выражения для максимальной энтропии непрерывного сигнала в условиях помех [6]

$$h_{max}(x) = log_2\sqrt{2\pi\sigma^2 e},$$

с учетом того, что дисперсия определяется мощностью принятого сигнала $\sigma^2 = \int x^2\omega(x)dx$ показывают, то и энтропия будет так же определяться только мощностью сигнала.

Пропускная способность информационного радиоканала так же в свою очередь зависит от соотношения сигнал/шум

$$C = Flog_2\left(\frac{P_c + P_ш}{P_ш}\right) = Flog_2\left(1 + \frac{P_c}{P_ш}\right),$$

где *F* ширина полосы пропускания канала.

Следовательно, реализация критерия максимизации количества передаваемой от БПЛА информации в условиях помех приведет к перераспределению энергетического ресурса БПЛА в пользу информационного канала в ущерб силового канала подавления. В результате чего контроль над безопасностью информационного канала будет утерян. Противник получит необходимую для успешного подавления априорную информацию для организации прицельной или уводящей помехи. Затем неминуемо последует воздействие прицельной или уводящей помехи с последующей потерей БПЛА.

Теоретически распределение энергетического ресурса между каналом датчиков $R^{Eд}$, информационным каналом R^{Eu}, и силовым каналом подавления $R^{ЕРЭБ}$ лишено этого недостатка. Поэтому критерий минимизации необходимого энергического ресурса

$$R^{E}{}_{min} = R^{Eд} + R^{Eu} + R^{ЕРЭБ}$$

имеет большие возможности для организации взаимодействия между каналами. Авторским коллективом были разработаны математические модели взаимодействия каналов. Результаты эксперимента подтвердили предположения о высокой эффективности энергетического критерия управлением информационной безопасностью радиоканала.

Литература

1. А.М. Рамм. Правда и мифы беспилотной битвы. https://nvo.ng.ru/nvo/2020-10-29/1_1115_dron.html.

2. S. Mitzerh, J. Janovsky, The Fight For Nagorno-Karabakh: Documenting Losses On The Sides Of Armenia And Azerbaijan. https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html.

3. Минимизация расхода энергетического ресурса при обнаружении и сопровождении воздушных целей / Г.Е. Журбин, Н.В. Соколик, А.С. Черненко. Известия вузов. Северокавказский регион. Южно-Российский государственный университет. 2011. №2. – С. 24 – 27.

4. Оптимизация распределения энергоресурса в многоканальном комплексе между локационными каналами / Г.Е. Журбин, С.В. Чамлай, Т.В. Мельникова; Изв. Вузов. Электромеханика. – 2018. – №.3 – С.85–87.

5. Теория обнаружения сигналов / П.С. Акимов, П.А. Бакут, В.А. Богданович и др.; под ред. П.А. Бакута. М.: Радио и связь, 1984. 440 с.

6. Теория электрической связи: курс лекций. Учебное пособие для вузов / Р.Н. Андреев, Р.П. Краснов, М.Ю. Чепелев. –Горячая линия – Телеком, 2014 -230с. ISBN 978-5-9912-0381-4.

Сведения об авторах

Баранов Владимир Витальевич, кандидат военных наук, доцент, заведующий кафедрой «Информационная безопасность» ЮРГПУ (НПИ) им. М.И. Платова; e-mail: baranov.vv.2015@yandex.ru.

Журбин Григорий Евгеньевич, доцент кафедры «Информационная безопасность» ЮРГПУ (НПИ) им. М.И. Платова, кандидат технических наук, доцент; e-mail: gregazov@yandex.ru.

Бессонов Алексей Александрович

О НЕКОТОРЫХ ВОПРОСАХ ИСПОЛЬЗОВАНИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ В КРИМИНАЛИСТИКЕ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Математические методы традиционно входят в методологический инструментарий криминалистики, вместе с тем, на наш взгляд, их потенциал всё ещё в недостаточной степени реализован в этой науке. В то же время стремительное развитие информационно-компьютерных технологий, современные достижения науки о данных, большие объёмы накопленной информации научной и практической направленности открывают новые горизонты приобретения необходимых и актуальных научных знаний в области криминалистики и деятельности по расследованию преступлений.

Сегодня арсенал математического инструментария приобретения новых научных и эмпирических знаний простирается от теории вероятностей и математической статистики до алгоритмов машинного и глубокого обучения. Важным условием плодотворной жизнеспособности этих методов в любой научной сфере выступают, во-первых, знания сущности, возможностей и ограничений каждого из таких методов и технологии их использования для работы с данными, а также умения и навыки их применения для решения научных и прикладных задач, во-вторых, владение знаниями, входящими в предмет конкретной науки, и опыт их практической реализации. Сказанное справедливо относится и к применению этих методов в практической деятельности. Одновременно это же условие является серьёзным препятствием к широкому распространению указанных методов в научных исследованиях, посвящённых криминалистической тематике.

Справедливости ради отметим, что в расследовании преступлений и судебной экспертизе для решения отдельных задач они применяются более активно, однако и здесь в полной мере их ресурс в жизнь не воплощён. Сегодня по-прежнему актуальна мысль авторов коллективной работы «Типовые модели и алгоритмы криминалистического исследования», изданной в 1989 году, о том, что «сложность процесса расследования и предупреждения преступлений делает бесперспективной практику принятия уполномоченными лицами решений на основе лишь личного опыта и интуиции, без использования современных методов познания различных наук, накопления и переработки криминалистически значимой информации, помноженных на возможности современных ЭВМ» [3, с. 65].

Отправным пунктом решения обозначенной проблемы в первую очередь видится популяризация в сообществе учёных-криминалистов методов математической статистики, а также алгоритмов машинного и глубокого обучения, включаемых в понятие «искусственный интеллект». В настоящее время это приобретает особую актуальность, поскольку согласно результатам проведённого компанией «Ростелеком» мониторинга глобальных трендов цифровизации по итогам 2020 года технологии искусственного интеллекта являются ведущим направлением науки и практики. Более того в качестве одной из целей развития искусственного интеллекта в нашей стране Указом Президента

Российской Федерации от 10.10.2019 № 490 определено обеспечение национальной безопасности и правопорядка, что в полной мере корреспондирует цели криминалистики. В этой связи обеспечение современного уровня научного знания в криминалистике и соответственно в деятельности по расследованию преступлений не представляется возможным без широкой интеграции в них этих методов и технологий.

Поскольку одним из объектов изучения в криминалистике выступает преступная деятельность, рассмотрим некоторые вопросы изучения последней с использованием алгоритмов искусственного интеллекта и математической статистики.

Ядром криминалистического изучения преступлений различных видов с применением перечисленных методов выступает их цифровая криминалистическая модель. Под такой моделью мы понимаем представление криминалистической характеристики преступлений в машиночитаемой форме, в которой сведения об их криминалистически значимых признаках и закономерных связях последних между собой выражены в виде математических категорий, уравнений и/или неравенств [2, с. 60]. Подробно технология построения цифровой криминалистической модели рассмотрена нами в монографии «Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений» [1].

Природа цифровой криминалистической модели преступлений такова, что с одной стороны она является результатом научно-исследовательской деятельности с использованием рассматриваемых методов, с другой – потенциальным объектом дальнейших научных исследований и практического использования в расследовании криминальных деяний с применением этого же инструментария. Иными словами, она имеет как научное, так и прикладное значение, что существенно повышает её потенциал.

В то же время важно понимать, что модель может содержать не больше информации, чем сам реальный объект. По этой причине она при условии её адекватности будет отражать лишь те признаки и закономерности, которые существуют собственно в реальном объекте. В этой связи главной задачей является стремление к обеспечению максимально возможного соответствия модели представляемому ею объекту, иначе могут последовать недостоверные выводы и решения. Это налагает особую ответственность на исследователя, работающего над созданием такой цифровой криминалистической модели в части идентичности преступлениям того вида, которые служат её основой.

Одновременно нужно учитывать, что никакая созданная человеком модель не сможет со стопроцентной точностью отразить природу какого-либо объекта или явления объективной действительности хотя бы ввиду наличия ещё не изученных и не известных на сегодняшнем этапе развития научного знания закономерностей. Тем более это справедливо относится к преступным деяниям, которым в рамках одного вида имманентно типичное, однако всегда есть место уникальному и даже аномальному. К примеру, изучением 1068 серийных преступлений, совершённых 184 лицами по сексуальному мотиву, установлено, что 1,3% из них имеют уникальный способ совершения, не повторяющийся в системе других аналогичных деяний.

Процесс построения цифровой криминалистической модели преступлений имеет несколько этапов: 1) изучение эмпирического материала и сбор необходимых данных; 2) обработка полученных данных, включающая разведочный анализ; 3) построение модели и её оценка; 4) использование модели в научных целях и/или в практической деятельности [1, с. 18–22].

Применение в исследовании упомянутых серийных деяний методов математической статистики и искусственного интеллекта позволило нам построить их цифровую криминалистическую модель, содержащую 27 признаков с различным числом градаций, а также выявить закономерные связи между элементами их системы. Закономерности изученных преступлений детерминировали выбор признаков, позволяющих

устанавливать серийный характер нераскрытых преступлений и причастных к ним лиц, а также строить поисковый портрет серийного преступника.

Эта модель послужила основой создания использующейся в настоящее время в работе управления научно-исследовательской деятельности (научно-исследовательского института криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации системы поддержки принятия решений на основе наивного байесовского классификатора и градиентного бустинга, позволяющая с точностью 92,5–98,2% (*AUC* = 0,969–0,981) устанавливать из числа нераскрытых преступных деяний те, которые с наибольшей вероятностью составляют серию, а также конкретных подозреваемых, сведения о совершённых деяниях которых включены в соответствующую информационную базу, наиболее вероятно их совершивших. Преимуществом этой системы является возможность её применения к криминальным деяниям серийного характера различных видов.

Помимо этого нами создан алгоритм построения портрета серийного преступника, совершающего свои криминальные деяния по сексуальному мотиву, на основании ряда признаков, которые устанавливаются следователем, как правило, уже на первоначальном этапе расследования. Эта система базируется на алгоритмах искусственного интеллекта, а именно – нейронных сетях и градиентном бустинге, и позволяет прогнозировать расстояние от места преступления до места жительства такого преступника с точностью 88,3–93,5% (в зависимости от количества используемых интервалов расстояний), его возраст (точность 80,3%, доверительный интервал ±6 лет), наличие у него психического заболевания (точность 81,5%) и судимости (точность 82%), факт совершения преступления с использованием автотранспортного средства и без него (90%), наличие связи между преступником и потерпевшим до совершения деяния (96%), семейный статус – имеется собственная семья или нет (73,8%).

В настоящее время эта комплексная система на основе алгоритмов искусственного интеллекта проходит апробацию в Главном управлении криминалистики (Криминалистическом центре) Следственного комитета Российской Федерации.

Изложенное и результаты наших исследований позволяют сформулировать следующие выводы. Во-первых, возможно и необходимо использовать методы математической статистики и алгоритмы искусственного интеллекта в научном изучении преступлений в криминалистике как инструменты получения новых и необходимых знаний, а в практической деятельности – в качестве эффективного инструмента их расследования.

Во-вторых, неотъемлемой частью процесса использования систем поддержки принятия решений, основу которых составляют методы математической статистики и алгоритмы искусственного интеллекта, в деятельности по расследованию преступлений должно быть понимание их возможностей и ограничений во избежание некорректного использования и разочарования в этих современных и перспективных технологиях.

Литература

1. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. – Москва: Проспект, 2021. – 816 с.

2. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. – 2020. – № 4 (13). – С. 58–61.

3. Типовые модели и алгоритмы криминалистического исследования / Под ред. В.Я. Колдина. – М., 1989. – 184 с.

Сведения об авторе

Бессонов Алексей Александрович, доктор юридических наук, доцент, руководитель управления научно-исследовательской деятельности (научно-исследовательского института криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации, профессор кафедры криминалистики ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации»; e-mail: bestallv@mail.ru

Болтачев Эльдар Филаридович

О НЕКОТОРЫХ НЕГАТИВНЫХ ТЕНДЕНЦИЯХ РАЗВИТИЯ ТЕХНОЛОГИИ АНОНИМНЫХ СЕТЕВЫХ СОЕДИНЕНИЙ

Развитие информационно-коммуникационных технологий внесло ряд существенных изменений в организацию информационного процесса. В настоящее время можно наблюдать, что данные технологии, включая сеть Интернет, выступает составной частью сферы услуг, органов управления, промышленного производства, социальных и иных процессов.

Одновременно с этим, развитие получили технологии анонимных сетевых соединений, которые предназначены для обеспечения анонимности информационного взаимодействия. Однако их использование может детерминировать различные негативные тенденции, особенно в социально-правовой сфере.

Анонимное сетевое соединений реализуется посредством передачи в открытой компьютерной сети пакетов, в которых данные, наряду с исходной информацией, включают комбинацию различных протоколов передачи данных и многоуровневое шифрование. Существует множество решений анонимных сетевых соединений, большая часть из которых основана на применении децентрализованной сети. В такой сети каждая клиентская сторона, наряду с решением пользовательских задач, выполняет функции сервера, реализуя административные и вспомогательные функции, а также обрабатывая запросы на предоставление ресурсов.

Наиболее известной и развитой среди существующих анонимных сетевых соединений является сеть Tor (The Onion Router, луковая маршрутизация). В этой сети клиент формирует цепочку из трех произвольно выбранных узлов сети Tor. Среди них есть входной по отношению к клиенту узел и выходной, сеть Tor при этом функционирует как шлюз между клиентом и внешней сетью. Каждому Tor-серверу известно только о предшествующем ему и последующем, а замыкающие узлы не знают, кто находится на другой стороне канала и кто инициировал соединение [4].

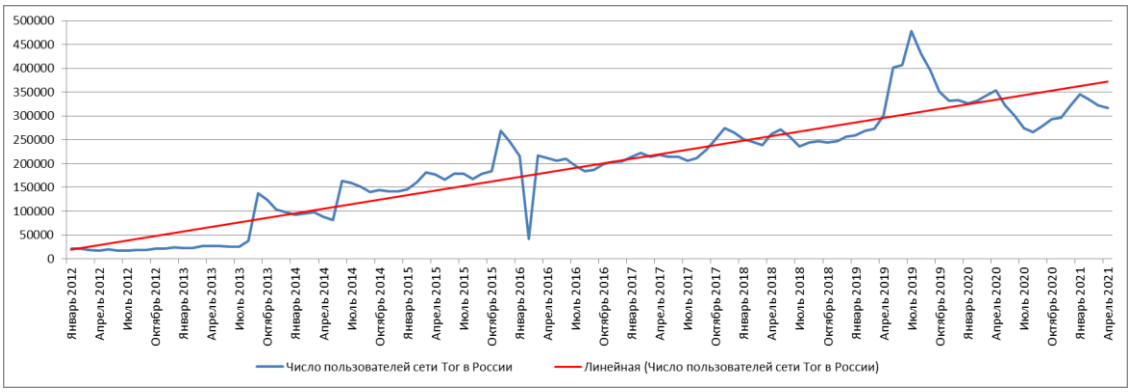


Рис. 1. Среднее число пользователей сети Tor из России.

В общем числе пользователей сети Tor почти 15% отводится пользователям из России [5], при этом динамический ряд показывает, что с января 2012 года по апрель 2021 года их число возросло в 14,6 раз (рис. 1). Линия тренда задана уравнением f(x) = 3174,7x + 16411 с коэффициентом детерминации 0,86.

Далее, в статье речь пойдет о пользователях сети Tor из России.

Внутри сети Tor существуют анонимные сервера, предоставляющие «скрытые» ресурсы, отличаемые старшим доменным именем .onion. Для навигации по имеющимся ресурсам, как правило, используется ресурс-каталог, содержащий ссылки, в том числе на русскоязычные ресурсы (рис. 2).

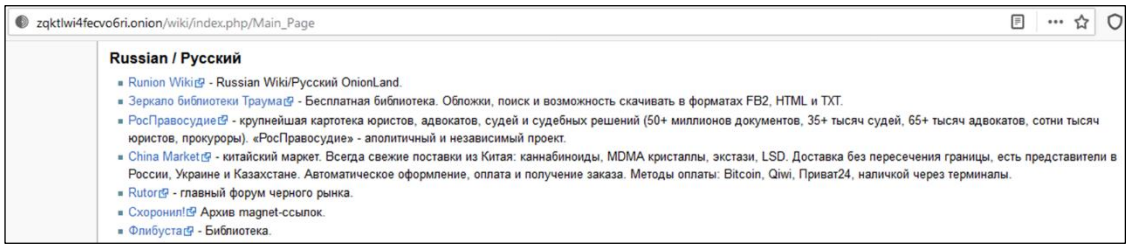


Рис. 2. Фрагмент ссылок на русскоязычные ресурсы сети Tor.

Обзор некоторых ресурсов сети Tor показывает, что их содержимое имеет явные признаки противоправной деятельности (рис. 3). Большое число объявлений связано с незаконным оборотом наркотиков.

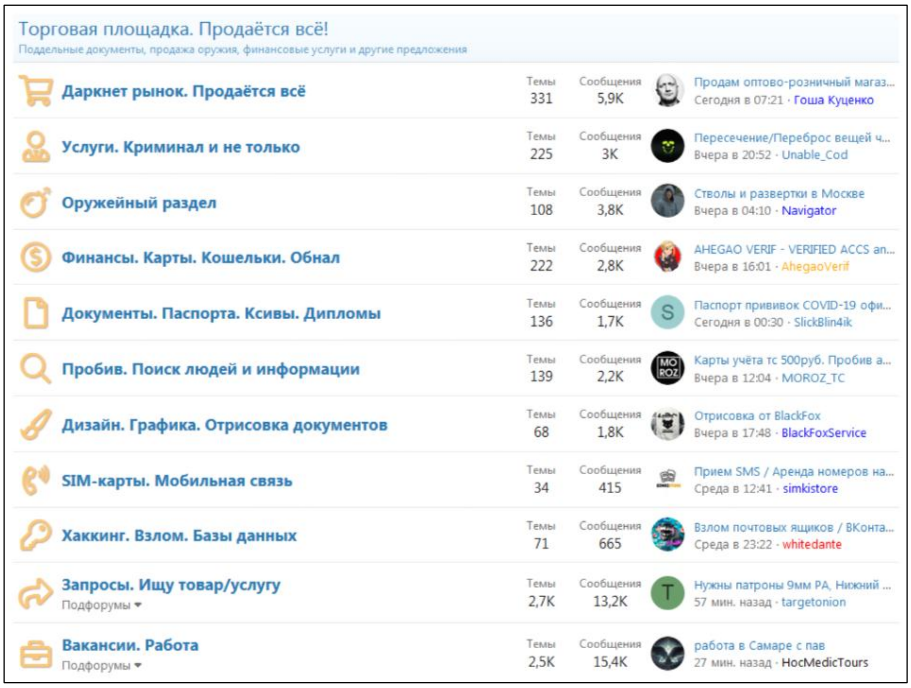


Рис. 3. Пример ресурса в сети Tor.

На первый взгляд может показаться, что относительная открытость подобных объявлений, при возросшем числе пользователей сети Tor, не может не пройти стороной уголовные нормы. Однако официальная статистическая отчетность свидетельствует об обратном.

Так, динамический ряд регистрируемых по России преступлений, связанных с незаконным оборотом наркотиков, характеризуется заметным падением (рис. 4). При этом отмечается снижение числа выявленных лиц, совершивших данные преступления, и, как следствие, снижается количество предварительно расследованных преступлений и количество преступлений, уголовные дела о которых направлены в суд [1].

Рис. 4. Число зарегистрированных по России преступлений, связанных с незаконным оборотом наркотиков, с января 2012 по апрель 2021 года.

С целью установления связи между пользователями сети Tor и некоторыми показателями официальной статистической отчетности была составлена корреляционная матрица, результаты которой были представлены в виде сводных данных с оценкой силы связи по шкале Чеддока (таблица 1) [3].

Таблица 1

Сводные данные корреляционной матрицы

Показатель	**Коэффициент (оценка по шкале Чеддока)**
Предварительно расследовано преступлений, связанных с незаконным оборотом наркотиков	**-0,73 (высокая)**
Предварительно расследовано преступлений, связанных с незаконным оборотом оружия	-0,05
Не раскрыто преступлений, связанных с незаконным оборотом наркотиков	-0,02
Не раскрыто преступлений, связанных с незаконным оборотом оружия	-0,03
Зарегистрировано преступлений, связанных с незаконным оборотом наркотиков	**-0,47 (умеренная)**
Зарегистрировано преступлений, связанных с незаконным оборотом оружия	-0,09
Количество преступлений, связанных с незаконным оборотом наркотиков, уголовные дела о которых направлены в суд	**-0,55 (заметная)**
Количество преступлений, связанных с незаконным оборотом оружия, уголовные дела о которых направлены в суд	-0,09
Выявлено лиц, совершивших преступления, связанных с незаконным оборотом наркотиков	**-0,44 (умеренная)**
Выявлено лиц, совершивших преступления, связанных с незаконным оборотом оружия	-0,23

Из представленных результатов выделим показатель, имеющий высокую связь [2]. Точечная диаграмма наглядно отражает обратно-пропорциональную связь между числом пользователей сети Tor и предварительно расследованными преступлениями, связанными с незаконным оборотом наркотиков (рис. 5). Коэффициент детерминации полученной прямой составляет 0,54.

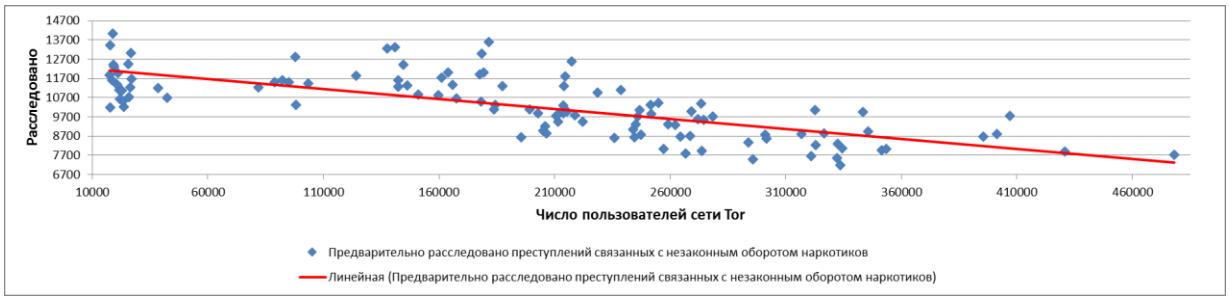


Рис. 5. Точечная диаграмма между числом пользователей сети Tor и предварительно расследованными преступлениями, связанными с незаконным оборотом наркотиков.

Для всех показателей, характеризующихся наличием связи с числом пользователей сети Tor (таблица 1), были построены линейные модели парной регрессии и выполнена оценка их параметров (таблица 2).

Таблица 2

Параметры линейных моделей парной регрессии

Y	***f(x)***	***R^2***	***p-value***
Предварительно расследовано преступлений, связанных с незаконным оборотом наркотиков	*-0,01x + 1230,5*	0,54	$3{,}9\times10^{-20}$
Количество преступлений, связанных с незаконным оборотом наркотиков, уголовные дела о которых направлены в суд	*-0,009x + 11824,4*	0,3	$3{,}2\times10^{-10}$
Зарегистрировано преступлений, связанных с незаконным оборотом наркотиков	*-0,01x + 20102,5*	0,2	2×10^{-7}
Выявлено лиц, совершивших преступления, связанных с незаконным оборотом наркотиков	*-0,007x + 10371,7*	0,19	$1{,}6\times10^{-6}$

Следует заметить, что для всех уравнений (таблица 2) число пользователей Tor выступает значимой переменной полученной модели, а все коэффициенты имеют отрицательный знак. Это свидетельствует о том, что при дальнейшем росте числа пользователей Tor рассматриваемые показатели, связанные с незаконным оборотом наркотиков, продолжат отрицательную динамику. Так, при увеличении числа пользователей Tor на 10 тысяч можно ожидать, что количество предварительно расследованных преступлений, связанных с незаконным оборотом наркотиков, снизится на 50 преступлений.

На основе проведенного исследования автор пришел к следующим выводам. Показатели состояния преступности, связанной с незаконным оборотом наркотиков, на фоне существующих ресурсов сети Tor, не отражают реальной складывающейся ситуации. Пользователи сети Tor из России детерминируют латентную составляющую преступлений, связанных с незаконным оборотом наркотиков. Дальнейшее увеличение пользователей сети Tor из России при отсутствии должных мер со стороны правоохранительных органов может негативно сказаться на реальном состоянии преступности, связанной с незаконным оборотом наркотиков.

Литература

1. Ежемесячный сборник о состоянии преступности в России // Генеральная прокуратура Российской Федерации: портал правовой статистики. URL: http://crimestat.ru/analytics.

2. Торопов Б.А., Болтачев Э.Ф., Баранов В.В. Математические методы исследования социальных систем: учебное пособие / Торопов Б.А. и др. – М.: Академия управления МВД России, 2020.

3. Елисеева, И.И. Эконометрика: учебник / И.И. Елисеева [и др.]; под ред. И.И. Елисеевой. − 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2007. – 576 с.

4. Погребенник А. «Какова цена анонимности в Сети» (рус.) // Системный администратор: Компьютерный журнал[en]. – М.: ООО «ИД «Положевец и партнеры», 2006. – Февраль (вып. 2, № 39). – С. 74-81.

5. Top-10 countries by relay users // Tor metrics. URL: https://metrics.torproject.org/userstats-relay-table.html

Сведения об авторе

Болтачев Эльдар Филаридович, кандидат технических наук, доцент кафедры информационных технологий Академии управления МВД России; e-mail: eleldar@mail.ru.

Васин Олег Иванович,
Щербаков Виктор Андреевич,
Кулаков Андрей Анатольевич

ТЕХНОЛОГИЯ БЛОКЧЕЙН В АВТОМАТИЗИРОВАНЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Технология блокчейн в настоящее время считается самой безопасной, так как вобрала в себя все передовые решения, «заточенные» на обеспечение информационной безопасности.

Очевидно, что развитие технологий управления информационными ресурсами эволюционируют поэтапно от централизованного к распределенному типу и этому есть логическое объяснение [1].

Первый этап характеризуется применением централизованных систем управления информационными ресурсами, когда крупные центры обработки данных содержали большое количество вычислительных мощностей, располагались в больших зданиях и управлялись централизовано. Все это привело к существенным затратам на обслуживание и перегрузке сетей операторов из-за необходимости передавать огромные массивы трафика от центров обработки данных к пользователям. В дальнейшем количество подключаемых устройств будет постоянно расти и еще сильнее усугубит обозначенную проблему.

Второй этап связан с появлением облачных технологий, которые обеспечивают удаленный доступ к совокупности информационных ресурсов (серверам, хранилищам данных, приложениям, сервисам, программному обеспечению). Однако централизация облачных сервисов стала причиной проблем связанных, прежде всего с защитой информации.

Со временем количество подключаемых устройств будет постоянно расти и ситуация, связанная с защитой информации, будет усугубляться.

Третий этап характеризуется внедрением концепции «туманных вычислений» (Fog Computing), позволяющей расширить возможности облачных вычислений и сетевого взаимодействия. Главное отличие от концепции облачных вычислений заключается в том, что обработка данных происходит не в облаке, а с помощью оконечных устройств сети (компьютеры, мобильные устройства, датчики). Таким образом, с появлением технологии «туманных вычислений» архитектура сети приобретает иерархическое построение.

Четвертый этап эволюции систем управления информационными ресурсами предполагает их полную децентрализацию на основе инновационной технологии

распределенного реестра (блокчейн). Такая технология обеспечивает одновременно децентрализацию информационных ресурсов и их безопасность. В блокчейне используется децентрализованное распределение и хранение информационных ресурсов на множестве автоматизированных рабочих местах (далее – АРМ), объединенных в одно ранговую сеть. В общем виде блокчейн представляет собой папку для хранения данных с множеством страниц, где каждая страница представляет собой массив данных, который называется блоком. Содержание блоков, записанных в папку, изменить невозможно, а копии папок хранятся у множества пользователей на АРМ, которые называются узлами. Блоки в цепи связаны хэш-кодами заголовков блоков. Благодаря такой связи блоков ни один из участников не может изменить содержимое блока, так как изменится содержимое заголовков последующих блоков. Попытки внесения изменений будут обнаружены всеми участниками и нейтрализованы сетью.

В заголовке указываются хэш-коды текущего, предыдущего блока, хэш-код транзакций и их число, информация для проведения процедуры получения права на запись блока, время записи блока. В поле транзакция в соответствии с протоколом записывается служебная информация по каждой транзакции. Для добавления нового блока, необходимо, чтобы другие участники сети проверили данную информацию.

Таким образом, безопасность информационных ресурсов при использовании технологии распределенного реестра обеспечивается посредством децентрализованного управления и хранения данных на множестве АРМ, применения криптографии (хэш-функций) при записи данных, использованием консенсусного протокола, предписывающего, как транзакции записываются и согласовываются между участниками.

Все перечисленные свойства делают возможным создание атмосферы доверия без каких-либо посредников, так как сама технология является гарантом безопасности как в обмене информацией между участниками, так и в отношении информации, хранящейся в рамках одной структуры. Именно это качество является ключевым свойством технологии блокчейн.

Технология блокчейн предотвращает целый спектр различных атак.

Например, атаки типа man-in-the-middle.

Шифрованные соединения (например, HTTPS и TLS) для защиты каналов опираются на инфраструктуру сертификации открытых ключей (PKI) и удостоверяющие центры. Каждый участник сети имеет пару открытый/закрытый ключ. Закрытый ключ он хранит в тайне. Открытый ключ хранит удостоверяющий центр.

Когда пользователь хочет установить безопасное соединение (зайти на сайт), он запрашивает открытый ключ ресурса у сертификационного центра и шифрует данные перед отправкой. Чтобы расшифровать данные, сайт использует свой закрытый ключ. Однако в этом случае надежность системы зависит от того, насколько хорошо защищен удостоверяющий центр. Если злоумышленникам удается скомпрометировать его, то они получают возможность провести атаку man-in-the-middle (MITM). В этом случае выполняется рассылка поддельных открытых ключей, к которым у хакеров есть соответствующие закрытые ключи. С их помощью выполняется расшифровка передаваемой информации.

Однако в системе, основанной на блокчейне, реализовать атаку типа MITM невозможно. Когда пользователь публикует открытый ключ в блокчейн, об этом становится известно всем узлам сети. Эта информация записывается в блок, и с помощью криптографии блокчейна защищается целостность реестра. Таким образом, хакеры (злоумышленники) лишаются шансов незаметно опубликовать ложные ключи и реализовать атаку man-in-the-middle (MITM).

Технологию блокчейн можно применять как полностью, так и частично:

1. Пример применения технологии блокчейн без удостоверяющих центров. Это пример одной из первых реализаций инфраструктуры сертификации открытых ключей (PKI), основанных на блокчейне проект Cert Coin. Проект, разработанный в MIT, исключает удостоверяющие центры и использует блокчейн как распределенный реестр доменов и ассоциированных с ними публичных ключей [2].
2. Пример с удостоверяющими центрами. Компания Pomcor представила проект, который не исключает удостоверяющие центры, но применяет блокчейн для хранения хэшей выданных и отозванных сертификатов. Такой подход дает пользователям возможность проверить аутентичность сертификатов. Это также оптимизирует доступ к сети (в том числе и SSO), поскольку верификация ключа и подписи проводятся на локальных копиях блокчейна. Таким образом, аутентификация в рамках консорциума проводится удостоверяющими центрами, а применение технологии блокчейн позволит усовершенствовать данный механизм путем хранения хэшей, выданных и отозванных сертификатов. Такой механизм позволит избежать атак типа man-in-the-middle (MITM).

Однако технология блокчейн, хоть и является самой защищенной, не свободна от угроз, нейтрализовать которые не потребует значительных ресурсов.

Рассмотрим наиболее вероятные угрозы технологии блокчейн [3] и отметим пути их нейтрализации.

Угроза атаки 51% когда злоумышленник, контролируя более пятидесяти процентов подтверждающих ресурсов сети блокчейн, может создать свою цепочку блоков, которая опередит основную цепочку блокчейна и в результате станет основной. Таким образом, только теоретически можно отменить транзакцию задним числом, а практически это потребует вычислительной мощности, во много раз превышающей мощность всех суперкомпьютеров из рейтинга Топ-500 на 2020 год. Нейтрализуется такая угроза увеличением производственных мощностей.

Угроза отказа в обслуживании (DoS), когда отправка большого количества «мусорных» данных на узел, обрабатывающий транзакции, может усложнить его работу. Однако, например, клиент Bitcoin Satoshi версии 0.7.0 все подозрительные узлы и транзакции блокирует, не позволяет дублировать транзакции, контролирует появление атаки DoS, ловит в системе злоумышленников, исправляет ошибки и т.д.

Угроза взлома крипто алгоритмов хэш-функций. Появление высокопроизводительных квантовых компьютеров увеличат риск реализации такой угрозы.

Угроза атаки Сибиллы, когда злоумышленник может попытаться наполнить сеть подконтрольными ему узлами, и остальные пользователи смогут подключиться только к блокам, созданным для злого умысла. Нейтрализовать такую угрозу возможно путем совершенствования защиты сети.

Угроза замедления времени в системе, когда хакеры атакуют сеть, в которой находятся абоненты, и путем создания большой вычислительной нагрузки на систему замедляют время внутри сети, что усложняет передачу данных, сообщений между пользователями, обновление информации в сети, формирование блоков, цепочек и их фиксацию участниками транзакций.

Нейтрализация такой угрозы возможна путем совершенствования алгоритма создания и утверждения достоверности блокчейна.

Угроза уязвимости транзакций, когда существует возможность изменить параметры транзакции так, что изменится хеш, но подпись останется прежней. Нейтрализация угрозы осуществляется дополнительными мерами проверки целостности транзакции.

Угроза ошибки кода из-за бага. Не произошло быстрое обновление в узле, и в цепочке не появилась нужная информация, неправильные данные начали

распространяться по сети и т.д. Все это может стать причиной остановки работы сети на несколько часов. Для ликвидации такой угрозы необходимо проверять программный код.

Данный этап развития АС СН характеризуется развертыванием ее перспективных средств, реализацией единого информационного пространства и перехода на автоматизированные способы управления.

Актуальные уязвимости АС СН с точки зрения обеспечения безопасности информации в настоящее время характеризуются отсутствием современных безопасных системотехнических решений по идентификации, аутентификации и авторизации доступа пользователей к ресурсам сетеориентированного пространства.

Кроме того, АС СН должна обеспечить безопасность, достоверность и целостность информации на всех этапах ее передачи хранения и обработки, что может быть достигнуто решением ряда задач, в том числе:

- созданием подсистемы управления безопасностью, обеспечивающей комплексную многоуровневую защиту информации, циркулирующую в АС СН путем разработки и внедрения средств защиты информации и управления безопасностью нового поколения (в том числе и с применением элементов искусственного интеллекта и технологии блокчейн);

- обеспечением информационной безопасности на основе применения профилей многоуровневого обеспечения требований по конфиденциальности информации.

Кроме того, должен быть предусмотрен переход на полное закрытие информации с использованием средств криптографической защиты информации (технология SSO).

SSO (Single Sign-On), технология единого входа пользователей. Владея одной учетной записью, пользователь может посещать множество различных сервисов, то есть переходит из одного раздела портала в другой без повторной аутентификации.

АС СН являются важнейшей составной частью технической основы системы управления Вооруженных Сил, подсистемы военного управления единой (взаимоувязанной) системы государственного и военного управления.

Поэтому существующие АС СН требуют совершенствования системного и технологического характера, в том числе касающихся криптографических средств защиты информации, надежной защиты от радиоэлектронного и информационного воздействия, а также внедрения современных средств идентификации и аутентификации.

Для нейтрализации угроз информационной безопасности необходимо решить ряд задач и, прежде всего, создать и внедрить в АС СН средства защищенного электронного документооборота, создать средства связи, криптографической защиты информации, обеспечивающие доступ к ресурсам АС СН на подвижных объектах (в т.ч. летательных аппаратах).

Несовершенство системы защиты информации в АС СН, а порой, и ее отсутствие может быть в большей степени компенсировано с помощью внедрения самых передовых технологий, например - технологии блокчейн.

Внедрение технологии блокчейн в АС СН позволит решить ряд задач, основными из которых являются:

внедрить информационную технологию, изначально устойчивую к различным видам воздействия, применение которой позволит уменьшить критичность проблемы обеспечения безопасности информационных ресурсов;

обеспечить переход на комплексную многоуровневую защиту информации (с использованием средств криптографической защиты информации);

внедрить современное безопасное системотехническое решение по идентификации, аутентификации и авторизации доступа пользователей к ресурсам сетеориентированного пространства;

отказаться от электронной подписи и наличия удостоверяющего центра, если технология будет использована как распределенный реестр;

внедрить SSO (Single Sign-On), технологию единого входа пользователей.

Литература

1.Elibrary.ru > Другие новости >id = 36934391.

2. Habr.com > p/341902/

3. Securitylab.ru > blog/personal/infornacionaya.

Сведения об авторах

Васин Олег Иванович, кандидат физико-математических наук, старший научный сотрудник НИЦ КВВУ Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознаменное училище имени генерала армии С.М. Штеменко (КВВУ), научно-исследовательский центр; e-mail: ovassin@mail.ru.

Щербаков Виктор Андреевич, кандидат технических наук, старший научный сотрудник НИЦ КВВУ, Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознаменное училище имени генерала армии С.М. Штеменко (КВВУ), научно-исследовательский центр; e-mail: sherbakov_viktor@list.ru.

Кулаков Андрей Анатольевич, начальник отдела НИЦ КВВУ Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознаменное училище имени генерала армии С.М. Штеменко (КВВУ), научно-исследовательский центр; e-mail: Andrei9614@rambler.ru.

Дрога Андрей Анатольевич,
Ковалева Екатерина Геннадьевна,
Савотченко Сергей Евгеньевич

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

В современных условиях, с учетом построения информационного общества, все большую актуальность приобретают вопросы обеспечения информационной безопасности мобильных устройств в правоохранительных органах, предотвращение и устранение разнообразными средствами и способами угроз в информационной сфере. Сегодня они стали их основой, первоисточником, основным ресурсом и главным оружием.

В этом контексте закономерно возрастает роль механизмов в обеспечении информационной безопасности мобильных устройств в правоохранительных органах, необходимость эффективного законодательного урегулирования общественных отношений, возникающих в данной сфере, определение правовых основ организации и координации действий субъектов обеспечения информационной безопасности, разработке приоритетных направлений государственной политики в сфере информационной безопасности [1, 2].

Исследование информационной безопасности мобильных устройств, в правоохранительных органах с юридической точки зрения связано с формированием качественной системы информационной и правовой защиты, которая отвечает современным требованиям и неотложным служебным потребностям сотрудников правоохранительной системы. Данная проблема появилась сравнительно не давно и становится все

более актуальной в связи с развитием технического обеспечения сотрудников правоохранительных органов.

Целью данной работы является анализ проблем обеспечения информационной безопасности мобильных устройств в правоохранительных органах. В работе будет охарактеризована роль информационной безопасности в правоохранительных органах. Будут проанализированы проблемные вопросы, возникающие в процессе обеспечения информационной безопасности мобильных устройств в правоохранительных органах и выявлены тенденции ее совершенствования в современных условиях.

Сейчас стремительное развитие информационного общества способствует постоянному накоплению научных разработок, касающихся детального рассмотрения и решения вопроса защиты информации во всех сферах ее использования. В этом смысле важной вехой в истории человечества стало принятие Всеобщей декларации прав человека (1948 г.), которая имеет большое значение на международном и наднациональном уровнях.

Значительное возрастание роли информации в процессе налаживания общественных отношений, а также активизация использования современных информационных технологий существенно влияют как на деятельность государственного аппарата в целом, так и на работу системы правоохранительных органов отдельно. Ведь информатизация может не только нанести прямых убытков конкретному лицу в случае несанкционированного доступа к его данным, их использованию, модификации или уничтожению, но и превратиться в источник серьезных угроз развития государства.

Задачи информационной безопасности в сфере правоохранительной деятельности в первую очередь ориентированы на построение защиты секретной информации и для служебного пользования от несанкционированного и последующего неправомерного использования.

Сейчас есть необходимость в формировании системы, обеспечивающей функционирование корпоративных организаций, отдельных юридических лиц правоохранительных органов. В течение последних лет в Российской Федерации имели место неоднократные попытки реализации комплекса мер, направленных на совершенствование механизмов гарантирования информационной безопасности. Однако, как свидетельствуют статистические данные, их внедрение не ликвидировало угроз информационной безопасности (в том числе правоохранительных органов), поэтому ее система требует неотложного пересмотра и совершенствования. Эти процессы, непосредственно связанные с пересмотром действующей политики государства по обеспечению информационной безопасности и, следовательно, с коренным реформированием ее системы.

Комплексные исследования обеспечения информационной безопасности правоохранительных органов проводились очень мало. Полноценное научное изучение этой тематики обусловлено стремительным развитием научно-технического прогресса, поскольку он актуализирует вопрос создания надлежащих гарантий защиты во время деятельности правоохранительных органов и формулировка соответствующих научно обоснованных предложений по их совершенствование. Поэтому такие исследования актуальны и содержат элементы научной новизны.

Формирование информационного общества требует создания совершенной, слаженной системы защиты информации. Поэтому одной из составляющих обеспечение общей безопасности информации в государстве должно быть надлежащее обеспечение информационной безопасности в деятельности правоохранительных органов. Это позволит повысить уровень их результативности, обеспечить надлежащее хранение документов, доступ к которым ограничен, и использовать имеющуюся информацию непосредственно по назначению. Исследуя этот вопрос, Е.В. Алексеева выделила такие раз-

новидности информационной безопасности как информационная безопасность лица, общества и государства [3].

Теоретический и аналитический материал, а также анализ практической составляющей развития этой сферы дали нам возможность сделать вывод о целесообразности выделение информационной безопасности правоохранительных органов как разновидности информационной безопасности. Потому ее изучение требует в дальнейшем более детального рассмотрения, выработка необходимых нормативно-правовых документов, координации процессов надлежащего использования информации в деятельности правоохранительных органов.

Нормы отечественного законодательства определяют не в достаточной степени требования и стандарты, меры и способы обеспечения информационной безопасности, в том числе и гарантирования информационной безопасности деятельности правоохранительных органов. Учитывая это, необходимо разработать проект закона «Об информационной безопасности правоохранительных органов Российской Федерации» и, соответственно, пересмотреть нормативно-правовую базу этой сферы [4].

Информационная безопасность правоохранительных органов заключается в способности их работников обезопасить информационные ресурсы от несанкционированного доступа к ним. Объем прав и обязанностей информационной сфере установлен законами и подзаконными нормативно-правовыми актами Российской Федерации.

Информационная безопасность правоохранительных органов отражает состояние защищенности прав и интересов государства, общества, отдельных физических и юридических лиц, касающиеся сбор, обработка, хранение, распространение информации и доступа к ней.

Однако защита информации не относится к основным функциям правоохранительных органов Российской Федерации, поэтому их деятельность не сконцентрирована на обеспечении собственной информационной безопасности. Такое положение обусловлено отсутствием единой системы служб и подразделений, работа которых базировалась на обеспечении защиты информации на различных уровнях.

Количество посягательств на информационную безопасность в нашей стране достигла угрожающих масштабов. Это свидетельствует прежде всего о низком уровне мер, предпринимаемых для обеспечения информационной безопасности, ненадлежащий контроль за информацией с стороны ее владельцев и неумение правильно имплементировать нормы права, направленные на защиту информации.

По мнению С.В. Корякина, обеспечение информационной безопасности правоохранительных органов Российской Федерации осуществляют по двум формам [5]:

- организационной (организация работы правоохранительных органов, работы, связанной с обращением, сбором, обработкой, хранением и использованием информации, взаимодействие сотрудников правоохранительных органов по обеспечение информационной безопасности);

- правовой (издание приказов и распоряжений, разработка положений, инструкций, составление планов и т. п.).

Проанализировав практическую деятельность правоохранительных органов, считается целесообразным разграничить формы обеспечения их информационной безопасности на:

- законодательную - принятие нормативно-правовых актов, которые устанавливают правила использования и обработки информации, доступ к которой ограничен, и определяют степень ответственности за нарушение этих правил;

- техническую - администрирование доступа к информационным ресурсам с учетом определения прав пользователей.

В то же время процедура применения механизмов обеспечения информационной безопасности деятельности правоохранительных органов, не может ограничивать права и свободы человека и гражданина в информационной сфере. Эти вопросы должно быть сбалансировано на основе принятия нормативно-правовых актов, где четко были бы определены обязанности и полномочия правоохранительных органов относительно применения мер информационной безопасности и предоставления доступа к определенным видам информации (или в нем) физическим и юридическим лицам.

Опыт работы полиции зарубежных стран по обеспечению информационной безопасности дает возможность выделить два направления деятельности отечественных правоохранительных органов. Первый – заключается в совершенствовании деятельности правоохранительных органов по обеспечению собственной информационной безопасности изнутри, то есть, так внутренней реформы. Второй – в улучшении правового обеспечения информационной безопасности на государственном уровне, то есть в имплементации своеобразной внешней реформы.

Используя такие механизмы совершенствования процесса обеспечения информационной безопасности, следует помнить о их взаимосвязь. Ведь для достижения высшего уровня обеспечения информационной безопасности правоохранительных органов необходима не только трансформация действующего законодательства, а и навыки его реализации [6]. Таков комплекс мероприятий способен, по нашему мнению, активизировать все факторы, необходимые для обеспечения информационной безопасности нашего государства.

Учитывая развитие и распространение современных мобильных устройств, рост их аппаратных возможностей, а также скорости передачи данных в сетях мобильной связи, для более эффективной защиты надо быть внимательнее, использовать проверенное программное обеспечение, различные пароли для учетных записей, блокировка устройства (пин-код, пароль и т. д.), удаленное управление на случай потери.

Неосведомленность сотрудников и администраторов сетей, что приводит к большой вероятности перехвата информации решается обучением правилам информационной безопасности. Вероятность перехвата информации можно уменьшить путем использования средств защиты в полном объеме, но проблема отсутствия корректной настройки может оставаться, из-за использования неустойчивых паролей.

Используя специализированное программно-аппаратное обеспечение, дает возможность повысить уровень защиты сетей от злонамеренных действий, а правильная настройка и ответственное использование личной техники поможет эффективно и безопасно использовать возможности современных мобильных устройств.

В настоящее время создана, скоростная единая цифровая ведомственная телекоммуникационную сеть, объединившая в себе все подразделения полиции, и, в свою очередь, стала платформой для дальнейшего развития внедрения и использования информационных технологий.

Все существующие в подразделениях полиции автоматизированные учеты, что были накопленные годами, сегодня объединены в единую общую реляционную базу данных с доступом через веб-интерфейс - информационный портал полиции. Это позволяет создать общее информационная среда работы полицейского и обеспечить получение исчерпывающей имеющейся информации из всех существующих информационных подсистем на обычном рабочем месте.

Благодаря использованию программного обеспечения реализована интеграция в существующую информационную систему мобильных и планшетных устройств с использованием закрытой 2G/3G сети оператора мобильной связи. Есть возможность осуществлять не только доступ к информационным ресурсам полиции, а и, используя технологию GPS, определять местонахождение указанных устройств и отображать их

на карте единой дислокации подразделений полиции области для более эффективного управления.

Также, подключены и соответствующим образом зарегистрированы в системе планшетные устройства, обеспечивающие возможность ввода информации в информационные подсистемы загрузки видео и фотоматериалов, в свою очередь, способствовало внедрению в практическую деятельность подразделений полиции упрощенного порядка рассмотрения заявлений и сообщений без признаков уголовных правонарушений, снижению нагрузки на участковых офицеров полиции, улучшению качества сбора первичных материалов работниками патрульной полиции непосредственно по месту вызова.

Более эффективному использованию планшетных устройств в территориальных подразделениях полиции, к сожалению, мешает слабое развитие инфраструктуры связи по технологии 3G за пределами крупных городов, но это вопрос времени.

Изучается вопрос объединения и использования в служебной деятельности подразделений полиции уже существующих местных систем видеонаблюдение. Цель такого объединения - создание единого программно-аппаратного комплекса с интеграцией его с уже существующими банками данных полиции, что дало бы возможность в автоматическом режиме осуществлять аналитическую обработку поступающих видеопотоков целью выявления правонарушений, реагирования на чрезвычайные том числе и техногенного характера, раскрытие уголовных правонарушений.

Бесспорно, следует отметить, что в современных условиях развития информатизации подразделений полиции чрезвычайного значение приобретают вопросы обеспечения надлежащей информационной безопасности при обработке данных, которые, собираются и хранятся у ведомственных информационных ресурсах.

Здесь следует отметить проблему несанкционированного вмешательства посторонних лиц в работу ведомственных информационных ресурсов с помощью вредоносного программного обеспечения (компьютерных вирусов), что распространяется через всемирную информационную сеть Интернет [7].

Постоянно проводятся организационные мероприятия, направленные на предотвращение утечки служебной информации из мобильных устройств, правоохранительных органов в частности [8]:

- все сотрудники под личную подпись предупреждаются о недопустимость любым способом распространять информацию, которая им стала известна в связи с работой с ведомственными информационными ресурсами;

- разработана и введена процедура предоставления атрибутов доступа к ведомственным информационным ресурсам, что делает невозможным их несанкционированное получение;

- проводится мониторинг активности сотрудников, по результатам чего проверяются основания проработки ими информационных запросов.

К сожалению, следует отметить, что изложенные меры недостаточны и в полной мере не обеспечивают необходимый уровень информационной безопасности.

Никакие приборы, используемые с одной стороны линии, не могут выявить наличие средств снятия информации на противоположном полюсе связи, то есть у абонента, с которым ведется разговор (если он, конечно, сам не позаботился о защите своей части линии). Поэтому для надежной защиты телефонных разговоров следует использовать «закрытые» каналы связи, где применяется криптографическая защита информации [9].

Существует несколько принципов криптографической защиты акустической информации. Согласно этому есть и различные приборы защиты, которые отличаются разной стоимостью и надежностью.

Наиболее надежными являются приборы и методы, с последующим шифрованием. Принцип работы таких устройств заключается в цифровой обработке аналоговых

сигналов, обнаружении и разложении слов и звуков на отдельные форманты и передачи речи в виде предварительного зашифрованного наборе формате. При этом ключевое слово к шифру может достигать длины до 512 знаков, а иногда и еще больше. Это системы сверхвысокой надежности, например, правительственная связь. На расшифровку такого перехваченного разговора за правило нужно много времени, иногда миллионы лет.

Существуют менее сложные системы, основанные на цифровой обработке спектра сигналов и передаче сигналов с другим спектром. На приемном конце в соответствии с заданными правилами приема происходит обратное преобразование сигналов.

Разработка и внедрение мобильных устройств, криптографического преобразования цифровой информации, которые бы использовали, для передачи данных общие сети имеет большое значение. Во-первых, с точки зрения экономической целесообразности, не требующей отдельных выделенных линий и технических средств. Во-вторых, гибкость применения в зависимости от обстановки и наличии общих сетей для передачи данных. В-третьих, оперативность обмена информацией между потребителями (абонентами). В-четвертых, не потребуется задействование системы генерации и распределения ключей между потребителями. На сегодняшний день эта проблема актуальна, как элемента системы охраны государственной тайны и служебной информации в правоохранительных органах.

Понятно, что все аппараты криптографической защиты информации работают в закрытом режиме лишь тогда, когда они установлены с обоих концов линии связи, то есть имеющиеся у обоих абонентов, разговаривающих между собой. Поэтому, на наш взгляд, системы криптографической защиты информации являются наиболее перспективными с точки зрения обеспечения информационной безопасности мобильных средств связи.

Эффективно решать задачи по защите информации, циркулирующей в информационных и мобильных системах, а также обеспечить надежную защиту информационно-мобильных систем правоохранительных органов от преступных посягательств можно лишь путем создания в их составе комплексных систем защиты информации, сочетающих правовые, организационные, инженерные мероприятия, а также технические и программные средства защиты.

То есть, одним, едва ли не главным фактором процесса создания системы обеспечения безопасности информации становится разработка и совершенствование правовой основы в этой сфере, и в частности, такой нормативной базы, которая бы, учитывая требования современности, регламентировала общественные отношения в сфере защиты информации и обеспечения безопасности ее во время информационного обмена. Причем процессы формирования и совершенствования нормативно-правовой базы системы защиты информации проходят как путем внесения изменений в существующие, так и путем разработки новых нормативно-правовых актов.

При этом они должны соответствовать требованиям по гармонизации российского законодательства с международным законодательством, они должны создать для Российской Федерации возможность стать равноправным участником международного информационного обмена при условии сохранения информационного суверенитета нашей страны.

Как свидетельствует опыт ведущих стран мира, эффективная деятельность в сфере обеспечения информационной безопасности должна проходить путем наращивания мощностей тех структур, на которые возложена реализация государственной политики по основным, технологическим ее составляющими: мер по защите информационных ресурсов, защите информации, обеспечению безопасности информационного обмена. Это позволяет не только создать дополнительные рычаги влияния на процессы реализации государственной политики в сфере информационной безопасности, но и обеспе-

чить, в условиях дальнейшей демократизации общества, открытость мероприятий, внедряются для поддержания и обеспечения информационной безопасности лица, общества и государства.

Необходимо следовать единой ведомственной политике информационной безопасности мобильных устройств с коллегиальным обсуждением и документальным закреплением основных направлений деятельности, связанной с процессами информатизации МВД, защитой ведомственной информации, а также профилактикой и борьбой с правонарушениями, совершаемыми с использованием информационных технологий – компьютерными преступлениями.

Литература

1. Прокопенко А.Н., Дрога А.А., Александров А.Н. Правовая защита информации (информационное право): учебное пособие / Белгородский юридический институт МВД РФ. 2-е изд., перераб. и доп. Белгород, 2012. – 150 с.

2. Жукова П.Н., Насонова В.А., Прокопенко А.Н. Основы информационной безопасности в ОВД: учебное пособие / Бел ЮИ МВД России имени И.Д. Путилина, 2015. – 72 с.

3. Алексеева Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. – 2016. – № 4. – С.7.

4. Шушков Г.М., Сергеев И.В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции. – М.: МГОУ, 2016. – С.31-35.

5. Корякин С. В. Современные тенденции развития систем информационной безопасности // Проблемы автоматики и управления. – 2017. – №.10. – С.13-17.

6. Романенко А.С. Некоторые аспекты борьбы с киберпреступностью // Актуальные проблемы права, экономики и управления. – 2015. – №11. – С.5-9

7. Страхов А.А., Анисимова Т.В. Правовые аспекты использования сети Интернет в Российской Федерации // Вестник Московского университета МВД России. – 2015. – № 11. – С. 229-233.

8. Черкасов, В. Н. Информационная безопасность. Правовые проблемы и пути их решения / В.Н. Черкасов // Информационная безопасность регионов. – 2018. – № 5. – С. 6–14.

9. Столинг Вильям Криптография и защита сетей: принципы и практика, 2-е изд.; пер. с англ. – М.: Издательский дом «Вильямс», 2001. –672 с.

Сведения об авторах

Дрога Андрей Анатольевич, заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: ABulet@rambler.ru.

Ковалева Екатерина Геннадьевна, кандидат технических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

Савотченко Сергей Евгеньевич, доктор физико-математических наук, доцент, профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: savotchenko@hotbox.ru.

Епифанцева Виктория Александровна,
Хромых Анна Алексеевна

ОБ ОПЫТЕ РАЗРАБОТКИ ЭЛЕКТРОННОГО УЧЕБНО-МЕТОДИЧЕСКОГО КОМПЛЕКСА ДЛЯ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Современные образовательные технологии невозможно представить без применения инновационных средств обучения. Информационные технологии в образовании играют всё более существенное значение. Разработчики средств обучения уже давно предложили учебным заведениям отказаться от рабочих тетрадей, учебных пособий и обычной доски и внедрить в учебный процесс инновационные технологии [4]. Наиболее значимыми стратегиями современного образования являются: цифровая трансформация, глобализация, гуманитаризация и гуманизация образовательного пространства [2].

Цифровая трансформация заключается в процессе полной замены ручных, традиционных и устаревших способов ведения образовательного процесса новейшими цифровыми технологиями во всем образовательном процессе, требующем внесение коренных изменений в информационные технологии и принципов создания новых информационных продуктов [6].

Требование предметного содержания подразумевает, что электронный учебно-методический комплекс должен включать как учебный материал по определенной предметной области (дисциплине, курсу, разделу, теме), так и его информационное сопровождение (презентация, видеоролики, звуковое сопровождение и.т.д). Обсуждение результатов использования электронного учебно-методического комплекса осуществлено на XVII Всероссийской научно-практической конференции «Математические методы и информационно-технические средства». Апробация проведена в процессе преподавания учебных дисциплин [5].

Электронный учебно-методический комплекс является средством интегрированного воздействия на курсанта путем сочетания концептуальной, иллюстративной, справочной, тренажерной и контролирующей частей [7]. Структура и пользовательский интерфейс этих частей курса должны обеспечивать эффективную помощь при изучении материала [1].

Электронный учебно-методический комплекс, разработанный на платформе Google Disc, включает в себя лекционный и презентационный материал, представленный в современной мультимедийной форме (текст, изображения, анимация, звук, видео). Дополняется списком основной и дополнительной литературы [3].

Пример графического интерфейса электронного учебно-методического комплекса представлен на рис. 1.

Электронный учебно-методический комплекс создан в виде web-сайта. Состоит из 4 web-страниц, где в верхней части окна находятся кнопки навигации, благодаря которым легко перемещаться с одной страницы на другую.

Во вкладке главная электронного учебно-методического комплекса расположена информация о цели изучения дисциплины кафедры, также расположены кнопки в виде иконок при нажатии на которые мы переходим на нужный сайт.

Важным элементами электронного учебно-методического комплекса являются Интернет-ресурсы. В частности, Сетевая академия Cisco. Обучение в виртуальной академии в университет ведется с 2014 года, в настоящее время ежегодно обучается более 100 курсантов и слушателей. Процесс обучения полностью интегрирован в самостоятельную работу обучающихся.

Рис. 1. Пример графического интерфейса электронного учебно-методического комплекса

Во вкладке Литература расположены учебно-методические пособия, подготовленные преподавателями кафедры информатики и математики, а также ссылки на библиотечные ресурсы.

Во вкладке Методическая копилка электронного учебно-методического комплекса, находятся кнопки в виде иконок с названиями тем изучаемой дисциплины кафедры, при нажатии на которые осуществляется переход в нужную тему. В верхней части каждой темы расположена панель навигации.

Во вкладке Главная расположено краткое описание каждой темы и кнопка в виде иконки домика, которая возвращает на основную страницу электронного учебно-методического комплекса (рис. 2. Вкладка «Методическая копилка»).

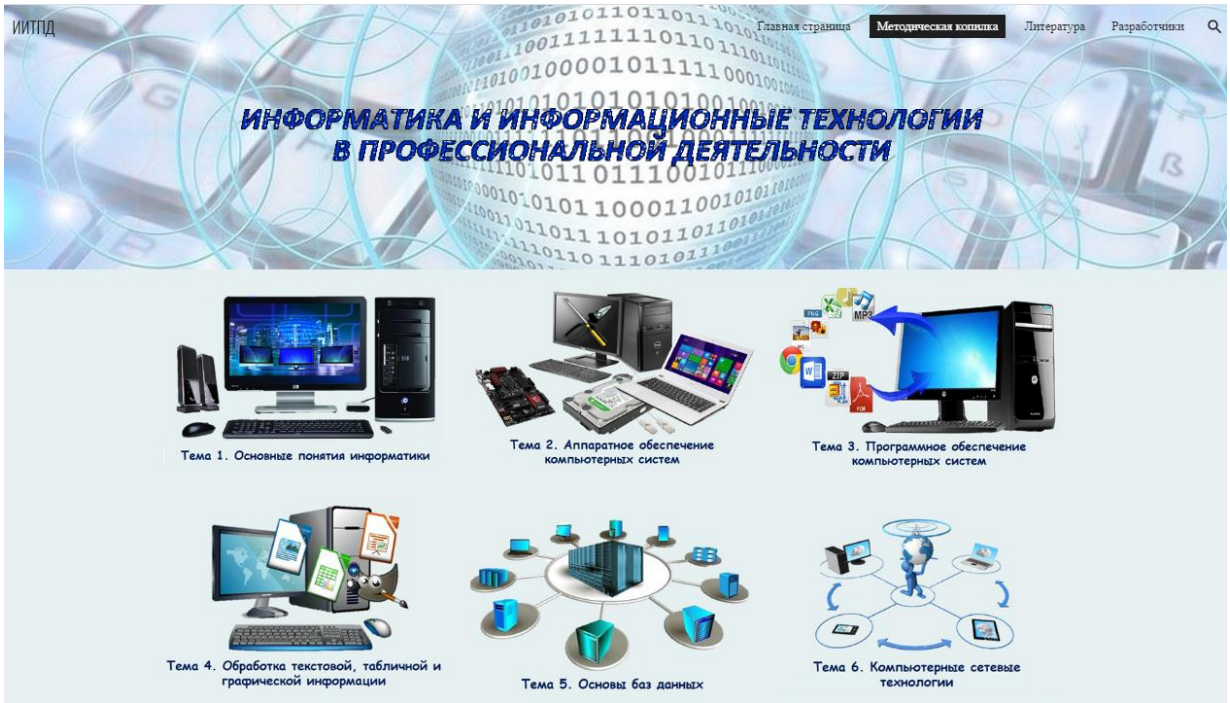


Рис. 2. Вкладка «Методическая копилка»

Во вкладке Лекции содержится теоретический материал, в виде 3D книги, для того чтобы просмотреть материал, содержащийся в лекции необходимо нажать на иконку с изображением обложки книги, далее скачиваем для изучения.

Во вкладке Презентации расположены презентации, которые включают мультимедийное сопровождение лекций и практических занятий по дисциплине ИИТПД. Презентации можно скачать, либо осуществлять просмотр на странице, не прибегая к скачиванию.

Во вкладке Практические работы расположен материал для практических занятий. Практические задания можно скачать, либо осуществлять просмотр на странице, не прибегая к скачиванию.

Вкладка Тестовые задания, содержит тестовое задание. Тестовые задания закрытого типа. Задания множественного выбора предлагают наличие вариативности в выборе. Курсант или слушатель должен выбрать один из предложенных вариантов. После того как будет завершена работа с тестовым заданием, можно перейти к результатам.

Во в кладке Видеоматериалы, расположены различные видеофрагменты, сюжеты, обучающее видео по дисциплине. Данный элемент содержит как ссылки на уже имеющиеся на жестком диске сервера видео, так и ссылки на ресурсы видеохостинга Yuotube. Благодаря видеоматериалам курсанты и слушатели получают возможность варьировать темп поступления информации и ее количество в соответствии с индивидуальными возможностями и потребностями. К примеру, при помощи стоп-кадра можно внимательно исследовать детали сложной схемы, которая на занятии была представлена лишь кратковременно.

Во вкладке Интерактивные задания расположены готовые интерактивные материалы, которые может представлять преподаватель с помощью проектора или можно копировать ресурс в локальную сеть с правом полного доступа, чтобы. После того как будет завершена работа с интерактивным заданием, можно просмотреть результат.

Во вкладке Самостоятельные работы расположены задания для самостоятельной работы курсантов и слушателей, задания можно просмотреть в режиме онлайн или скачать.

Благодаря используемой платформе Google, в которой был создан web-сайт, особых требований к компьютерной системе не предъявляется, т.к. возможность использования электронного учебно-методического комплекса в любом аппаратном и программном окружении, имеющем браузер.

Литература

1. Булгаков О.М. Моделирование надежности компьютерного теста с повышенной устойчивостью к возникновению ошибок второго рода / О.М. Булгаков, И.Н. Старостенко, А.А. Хромых, А.О. Дедикова // Вестник Воронежского института ФСИН России. – 2021. – №1. – С. 50-58.

2. Епифанцева В.А. Использование цифровых образовательных ресурсов в учебном процессе в условиях реализации ФГОС нового поколения: опыт, проблемы // В.А. Епифанцева // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2019. С. 210 – 214.

3. Епифанцева В.А. Онлайн обучение – необходимость или эволюция образования в целом / В.А. Епифанцева, А.А. Хромых // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Международной научно-практической конференции (22 мая 2020 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2020.

4. Епифанцева В.А. Технология создания электронного портфолио Краснодарского университета МВД РФ / В.А. Епифанцева, А.А. Хромых // Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 7 Всерос. науч.-практ. конф., 21 мая 2021 г. /ред. кол.: И.Ф. Амельчаков, И.Н. Озеров, В.Л. Акапьев, А.Н. Прокопенко, В. А. Насонова. – Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2021.

5. Старостенко И.Н. Актуальные вопросы информатизации образования // Общество и право. 2017. № 4 (62). С. 274-277.

6. Старостенко И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

7. Хромых А.А. Технология разработки электронного образовательного ресурса по дисциплине «Математика» / А.А. Хромых, И.Н. Старостенко // Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 7 Всерос. науч.-практ. конф., 21 мая 2021 г. /ред. кол.: И.Ф. Амельчаков, И.Н. Озеров, В.Л. Акапьев, А.Н. Прокопенко, В. А. Насонова. – Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2021.

Сведения об авторах

Епифанцева Виктория Александровна, преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: torohova_viktori@mail.ru.

Хромых Анна Алексеевна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: AnnXA@mail.ru.

Еськин Дмитрий Леонтьевич

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

За последние десятилетия человечество совершило огромный рывок в технологической сфере. Возникли и продолжают стремительно развиваться технологии, которые несколько десятков лет назад можно было встретить лишь в трудах авторов научной фантастики, а сегодня они уже влились во все сферы жизни человека и во многом стали обыденными. Одним из таких перспективных направлений развития информационных технологий является так называемая технология дополненной реальности.

Термин «дополненная реальность» (англ. augmented reality, сокр. AR) впервые был введен сотрудником американской корпорации Boeing Томасом Коделлом в 1990 году для описания дисплеев, которые инженеры компании закрепляли на своей голове использовались для облегчения монтажа проводки в самолетах [1]. В отличие от виртуальной реальности, создающей виртуальную модель физической реальности в искусственном информационном поле [2], которая передается человеку через его органы чувств, дополненная реальность не заменяет реальный мир на виртуальный, а расширяет его посредством внедрения в поле восприятия человека в режиме реального времени виртуальных цифровых объектов – текста, изображений, звуков, анимации и т.д. Таким образом, основная цель технологий дополненной реальности – усилить восприятие реальности посредством наложения контекстных цифровых объектов на окружающую действительность.

Несмотря на то, что использование возможностей дополненной реальности сопряжено с рядом трудностей, в большей части связанных с реализацией взаимодействия пользователя и компьютерного устройства, данные технологии сегодня применяются во многих областях деятельности человека. В частности, в военной сфере данная технология используется для вывода оперативной информации на лобовое стекло техники, дисплей, стекло шлема пилота. Кроме того, активно ведутся исследования по разработке систем дополненной реальности для пехотных соединений как компонента экипировки «солдата будущего». Например, в США с 2018 года в интересах армии разрабатывается система дополненной реальности Integrated Visual Augmentation System (IVAS), основная задача которой – повысить ситуационную осведомленность бойцов [3]. Ожидается, что производство IVAS на базе гарнитуры Microsoft HoloLens начнется уже в 2021 году [4]. Технология дополненной реальности имеет огромный потенциал в сфере образования. Она позволяет дополнить учебный материал трехмерными моделями объектов, анимацией, видеофрагментами, звуком; позволяет в наглядной форме в динамике воспроизвести те процессы, которые в рамках занятия в реальности затруднительно или даже невозможно воспроизвести. В результате за счет наглядности и интерактивности учебный материал намного лучше усваивается. Технология дополненной реальности сегодня нашла широкое применение и в сфере отдыха и развлечений. Так на базе данной технологии разрабатываются приложения для мобильных устройств с различными интерактивными играми, наиболее известной из которых сегодня является Pokemon Go, фильтров для камеры мобильного устройства и т.д. В музеях и на выставках технология дополненной реальности позволяет посетителю получать детальную информацию о заинтересовавших его экспонатах и даже «оживлять» их. Например, Министерством культуры России совместно с порталом «Культура.РФ» создано мобильное приложение Artefact, представляющее собой мультимедийный гид с технологией дополненной реальности, позволяющее получать информацию о деталях и истории экспонатов. Примечательно, что на сегодняшний день к данному проекту подключилось уже более 90 музеев и организаций [5].

Очевидно, что технология дополненной реальности может быть весьма полезна для сотрудников правоохранительных органов, способствуя повышению эффективности их деятельности.

Подобно применению в военной сфере технология дополненной реальности может использоваться для предоставления сотруднику органов внутренних дел информации об оперативной обстановке на местности в режиме реального времени и организации оперативного управления. Также системы дополненной реальности делают возможным получение сотрудником информации об окружающих его объектах, включая планы зданий и расположенных в них коммуникаций, организациях, о нахождении ближайших нарядов и т.д. Причем для этого достаточно лишь навести камеру мобильного устройства или специальных очков на интересующий объект.

Сотрудники органов внутренних дел, несущие наружную службу, могут использовать технологию дополненной реальности для выявления среди прохожих лиц, находящихся в розыске. В этом случае система дополненной реальности работает совместно с системой распознавания лиц, которая сопоставляет изображение с видеокамеры устройства с содержимым ведомственной базы. В Китае, например, такие системы начали применяться с начала 2018 года [6]. Кроме того, в условиях пандемии COVID-19 полицейские Китая стали использовать дополненную реальность и для борьбы с распространением коронавируса, выявляя с помощью интегрированной в специальный шлем тепловизионной камеры представляющих потенциальную угрозу лиц с повышенной температурой тела.

В мае 2019 года из СМИ стало известно о том, что в Российской Федерации планируется экипировка полицейских крупных городов очками дополненной реальности с технологией распознавания лиц компании NtechLab. Предполагается, что очки будут интегрированы в систему FindFace Security, использующей стационарные камеры видеонаблюдения, которая была внедрена в нескольких крупных городах во время проведения чемпионата мира по футболу в 2018 году, и благодаря которой было задержано более 180 правонарушителей [7]. Вместе с тем за прошедшие два года данный проект так и не был реализован в полном объеме.

Поскольку технология дополненной реальности позволяет работать не только со зрительной информацией, но и с акустической, то она может помочь сотруднику полиции при общении с иностранными гражданами, осуществляя перевод их речи в режиме реального времени.

Технология дополненной реальности может быть полезна при осмотре места происшествия. Так голландские полицейские используют ее возможности уже с 2016 года. В частности, прибывший на место происшествия полицейский с помощью специализированного приложения и камеры транслирует его изображение экспертам, получая от них дальнейшие указания и необходимые комментарии на свое мобильное устройство. В 2018 году специалисты из Астрахани разработали для Следственного комитета России программу для планшетных компьютеров «Конструктор места происшествия», позволяющую с помощью технологии дополненной реальности осуществлять фиксацию данных с места происшествия и составлять его трехмерную модель [9]. Кроме того, технология дополненной реальности дает возможность проводить некоторые криминалистические исследования непосредственно на месте происшествия. Например, осуществлять поиск отсканированных дактилоскопических узоров в дактилоскопических базах с целью установления личности.

Таким образом, технология дополненной реальности сегодня является достаточно перспективным направлением развития информационных технологий, нашедшим применение в различных отраслях народного хозяйства. Внедрение технологии дополненной реальности в деятельность сотрудников правоохранительных органов также видится весьма перспективным. В частности, это позволит повысить эффективность их служебной деятельности и уровень личной безопасности за счет возможности получения в режиме реального времени дополнительной информации об окружающих их объектах реального мира.

Литература

1. A Brief History of Augmented Reality (+Future Trends & Impact) [Электронный ресурс]. Режим доступа: https://www.g2.com/articles/history-of-augmented-reality (дата обращения: 07.06.2021).

2. Цветков В.Я. Естественное и искусственное информационное поле // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 5, ч. 2. – С. 178–180.

3. Пехотная система дополненной реальности IVAS (США) [Электронный ресурс]. Режим доступа: https://topwar.ru/181316-pehotnaja-sistema-dopolnennoj-realnosti-ivas-ssha.html (дата обращения: 08.06.2021).

4. Army moves ahead on ‘mixed reality’ goggle with Microsoft in $21.8 billion contract [Электронный ресурс]. Режим доступа: https://www.armytimes.com/news/your-army/2021/03/31/army-moves-ahead-on-mixed-reality-goggle-with-microsoft-in-218-billion-contract/ (дата обращения: 08.06.2021).

5. Вышла новая версия приложения дополненной реальности Artefact [Электронный ресурс]. Режим доступа: https://www.culture.ru/news/253131/ vyshla-novaya-versiya-prilozheniya-dopolnennoi-realnosti-artefact (дата обращения: 09.06.2021).

6. Chinese police literally use 'Skynet' surveillance system [Электронный ресурс]. Режим доступа: https://www.cnet.com/news/chinese-police-wear-facial-recognition-surveillance-glasses/ (дата обращения: 09.06.2021).

7. Российская полиция получит очки с распознаванием лиц [Электронный ресурс]. Режим доступа: https://ria.ru/20190523/1554845480.html (дата обращения: 10.06.2021).

8. Следователь Go: о дополненной реальности на службе правоохранительных органов [Электронный ресурс]. Режим доступа: https://ceur.ru/news/ekspertiza/item351520/ (дата обращения: 11.06.2021).

Сведения об авторе

Еськин Дмитрий Леонтьевич, кандидат физико-математических наук, заместитель начальника кафедры информатики и математики Волгоградской академии МВД России; e-mail: yd38@bk.ru.

Ефремов Сергей Константинович

АНАЛИЗ ОШИБОК ПРОГНОЗИРОВАНИЯ УСПЕВАЕМОСТИ КУРСАНТОВ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

При приеме на обучение в ВУЗ приемная комиссия опирается, в основном, на результаты обучения абитуриента в школе (оценки в аттестате и результаты ЕГЭ) и результаты установленных вступительных испытаний. В работах [2-4, 11] проанализирована возможность и разработаны основы методики прогнозирования будущей успеваемости курсанта при обучении по выбранной специальности с использованием искусственной нейронной сети (ИНС). Нейронная сеть реализована программно (программа обучения сети и программа прогнозирования оценок) на языке VBA в среде MS Excel [1].

На текущем этапе работы проведена проверка работы ИНС на примере специальности 40.05.02 Правоохранительная деятельность. Исходными данными о курсантах здесь являются результаты окончания школы. В качестве обучающей выборки (оценки школьного аттестата по 14 основным предметам школьной программы и по 9 вузовским дисциплинам) взяты данные о 70 курсантах набора 2018 года. После обучения ИНС было проведено прогнозирование по этим же дисциплинам для 41 курсанта набора 2019 года и сравнение результатов прогнозирования с реально полученными по упомянутым 9 вузовским дисциплинам оценкам. Прогнозные значения определены с точностью до 0,01.

Результаты сопоставления прогнозных и реально полученных оценок:

1. Ошибки прогноза подчинены закону распределения, близкому к нормальному.
2. Среднее значение модуля ошибки прогноза составляет 0,55 балла.
3. При округлении прогнозных значений до целых величин совпадение этих значений с реальными происходит в 53% случаев.
4. Ошибка прогноза как случайная величина имеет систематическую составляющую величиной 0,15 балла в сторону уменьшения прогнозных значений по отношению к реальным.

Систематическая ошибка объяснима разными условиями сдачи экзаменов в 2018-19 (обучающая выборка) и 2019-20 (контрольный рассчет) учебных годах из-за пандемии и, как следствие, использования во втором семестре 2019-20 учебного года включая сессию режима удаленного обучения. Стандартный прием устранения систематической ошибки измерений – вычитание ее из полученных результатов. Для этого систематическую ошибку как математическое ожидание всех значений ошибок для всех кур-

сантов по всем дисциплинам необходимо вычислить. Но в данном случае этот прием не применим вследствие отсутствия реальных оценок на момент их прогнозирования и невозможности вычисления значений ошибок. Таким образом, систематическая ошибка в прогнозе сохраняется.

Случайная составляющая ошибки прогноза имеет довольно сложный характер. Как известно [6], прогнозное значение оценки определяется в ИНС как взвешенная сумма значений ее входов:

$$S_j = \sum_{i=1}^{n} x_i \cdot w_{ij} \qquad (1)$$

где S_j – прогнозируемая оценка по j-й дисциплине;

x_i – значение входного параметра – i-я характеристика курсанта (оценка по конкретному предмету из аттестата, значение конкретного анкетного параметра и т.д.); всего учитываются n параметров;

w_{ij}, - весовой коэффициент, оценивающий влияние i-го входного параметра на будущую успеваемость по j-й дисциплине.

Ошибка прогноза оценки курсанта по j-й дисциплине

$$W_j = S_j - T_j \qquad (2)$$

где T_j – реальная оценка, полученная курсантом по j-й дисциплине.

Величины S_j и T_j являются случайными.

Случайный характер реальной оценки T_j обусловлен несколькими причинами [11]:

1) существующая реально 3-балльная (по количеству вариантов значений оценок в экзаменационных ведомостях) шкала оценок знаний, принятая в стране. В результате знания двух обучаемых на уровне 3,50 и 4,49 оцениваются одинаково – 4. Хотя реальная разница в уровне их знаний – практически целый балл. В большинстве крупных стран в образовании используется более точная 10- или 12-балльная система оценки уровня знаний;

2) субъективизм в оценке уровня знаний преподавателем (влияние человеческого фактора);

3) физическое состояние обучаемого во время сдачи экзамена;

4) «повезло/не повезло» с билетом (экзаменационная лотерея), и т.д.

О первой причине ошибки в оценке можно говорить вполне определенно. Уровень знаний обучаемых в рамках непрерывной шкалы имеет закон распределения, наиболее близкий к равномерному. Поэтому можно определенно говорить о статистических характеристиках этой составляющей ошибки. Ошибки вследствие трех остальных причин сложно поддаются формализации. Но если сопоставлять разброс значений ошибок вследствие влияния первой причины (диапазон практически от -0,5 до 0,5 балла) с показателем общего разброса ошибок прогнозных значений по отношению к реальным (полученное в эксперименте среднее значение модуля ошибки прогноза 0,55 балла), то можно сделать вывод о том, что первая причина является основной в формировании ошибки оценки, получаемой обучаемым на экзамене. Остальные причины имеют намного меньшее влияние на суммарную ошибку в оценке на экзамене.

Другая составляющая ошибки прогноза, определяемой по формуле (2), ошибка в определении прогнозируемого значения оценки S_j, в количественном анализе еще более сложна. Прогнозируемое значение S_j определяется по формуле (1). Здесь значения как x_i, так и w_{ij} являются случайными. В проведенном эксперименте в качестве значений входных параметров x_i использованы оценки из школьных аттестатов. Характер ошибок здесь тот же, что и в оценках по вузовским дисциплинам.

Значения весовых коэффициентов w_{ij} определяются в ходе обучения ИНС с использованием обучающей выборки. Процесс обучения (определение значений w_{ij}) представляет собой решение задачи минимизации суммы ошибок прогноза по всем

курсантам из обучающей выборки для конкретной дисциплины. Задача обычно решается численно путем подбора таких значений w_{ij}, при которых суммарная ошибка становится минимально возможной [6]. При расчете весовых коэффициентов ошибки в их значения вносят как ошибки в школьных оценках, так и ошибки в оценках вузовских (эти оценки – содержание обучающих примеров). Но здесь проявление этих ошибок намного меньшее по сравнению с конечными ошибками прогноза, потому что совместное использование в вычислениях массивов оценок школьных и вузовских ведет к значительной взаимной нейтрализации индивидуальных ошибок оценок.

В итоге можно сделать следующие выводы:

1. Возникающие в прогнозных оценках систематические ошибки компенсировать невозможно до получения курсантами оценок реальных, когда в этой компенсации уже нет смысла.

2. Среди источников случайных ошибок в прогнозных значениях оценок основным является принятая в образовании страны по сути 3-балльная система оценок.

Основной вывод. Существующая в стране шкала оценивания знаний не позволяет с приемлемой точностью прогнозировать оценки учащихся в ВУЗах с использованием ИНС. Увеличение точности прогнозирования может дать переход на использование в качестве входных параметров других характеристик обучаемых: данных входного психо-физиологического тестирования, анкетных социальных данных и т.п. В конечном итоге может оказаться, что наиболее приемлемым вариантом набора входных параметров является смешанный набор, состоящий из оценок по наиболее существенным для вузовской специальности школьным предметам, наиболее существенным психофизиологическим параметрам и наиболее существенным социальным параметрам. Поиск такого набора входных параметров составляет суть следующего этапа работы по рассмотренной в работе теме. Определение содержания этого набора позволит использовать его и при решении других задач в сфере образования.

Литература

1. Ефремов, С.К. О возможности использования нейронной сети в индивидуализации приема и обучения студентов. / С.К. Ефремов, Е.В. Михайленко // Проблемы современного педагогического образования. – Сборник научных трудов: - Ялта: РИО ГПА, 2019. – Вып. 65. – Ч. 1, с. 114-117.

2. Ефремов, С.К. О возможности использования нейронной сети в индивидуализации приема и обучения курсантов: 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: Краснодар. ун-т МВД России, 2017. – С. 85-90.

3. Ефремов, С.К. Прогнозирование успеваемости абитуриентов образовательных организаций МВД России с использованием искусственной нейронной сети: научный доклад - Краснодар. ун-т МВД России. 2018.

4. Иванов, В. М. Интеллектуальные системы : учебное пособие / В. М. Иванов. – Екатеринбург : Изд-во Урал. ун-та, 2015. – 92 с.

5. Ильин, Е.П. Дифференциальная психология профессиональной деятельности. – СПб.: Питер, 2011. – 432 с.

6. Громов, Ю.Ю. Интеллектуальные информационные системы и технологии : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, В.В. Алексеев и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 244 с.

7. Информационные системы и технологии в профессиональной деятельности сотрудников органов внутренних дел : учебное пособие / К.М. Бондарь [и др.] ; Дальневосточный юрид. ин-т МВД РФ. – Хабаровск : РИО ДВЮИ МВД РФ, 2013. – 215 с.

8. Крылова, А.Г. Успеваемость студентов экономических специальностей и статистическая оценка факторов, на нее влияющих. // Современные научные исследования и инновации. 2012. № 6 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2012/06/14688 (дата обращения: 29.09.2017).

9. Макаренко, С.И. Интеллектуальные информационные системы: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 206 с.

10. Павлов, С. Н. Системы искусственного интеллекта : учеб. пособие. В 2-х частях. / С. Н. Павлов. — Томск: Эль Контент, 2011. – 176 с.

11. Старостенко, И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

Сведения об авторе

Ефремов Сергей Константинович, кандидат технических наук, доцент, доцент кафедры информатики и математики Краснодарского университета МВД России

Жилин Роман Андреевич

О РЕЗУЛЬТАТАХ КЛАСТЕРИЗАЦИИ ОДНОРОДНЫХ АЛЬТЕРНАТИВ

Для того чтобы найти искомый объект, необходимо выполнение нескольких условий: выбрать объект у которого большой разброс от среднего значения наиболее важных признаков и одновременно у этого же объекта значение интегрального показателя должно быть ниже среднего значения по всем имеющимся объектам.

Если у двух объектов значения интегральных показателей фактически одинаковы, то его показатель может количественно измениться за счет увеличения оценки одного из приоритетных критериев [1].

Задача: какой из признаков заменить, чтобы уровень защищенности увеличился в среднем по всем объектам.

Увеличим позиции определенных признаков для того, чтобы проанализировать, как меняется значение интегрального показателя.

Количественное увеличение по первостепенным критериям будет способствовать предельному увеличению значений интегрального показателя [2].

При едином значении интегрального показателя необходимо усиление показателей защищенности тех объектов, у которых разброс признаков относительно средних значений больше.

На приведенных ниже графиках квадратом будут обозначены средние значения по имеющимся 18 признакам, а ромбом будут обозначены отклонения от средних значений признаков в большую или меньшую сторону.

У объекта №2 видно, что значимые признаки сильно отличаются от средних значений.

У объекта №4 менее значимые признаки сильно отличаются от средних значений.

У объекта №7 отклонение признаков распределилось равномерно.

В данной работе объект №2 будет являться искомым объектом, у которого увеличение признака №5 приведет к увеличению общего среднего интегрального показателя по всем объектам.

Если нам необходимо поднять общий уровень защищенности за минимальные денежные средства в группе однородных альтернатив, то в данном случае необходимо сделать это у объекта №2.

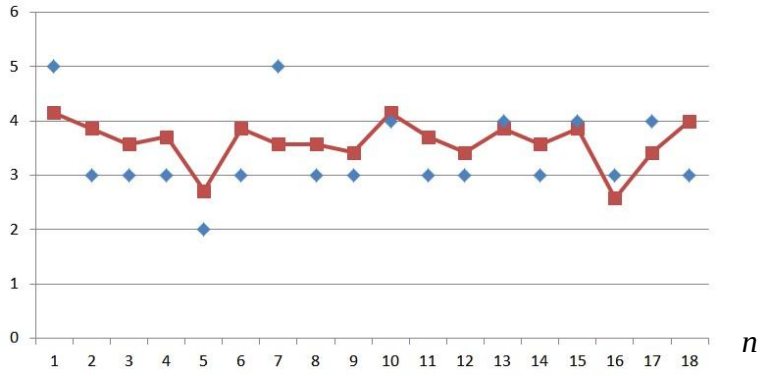


Рис.1 Результаты отклонения признаков объекта №2.

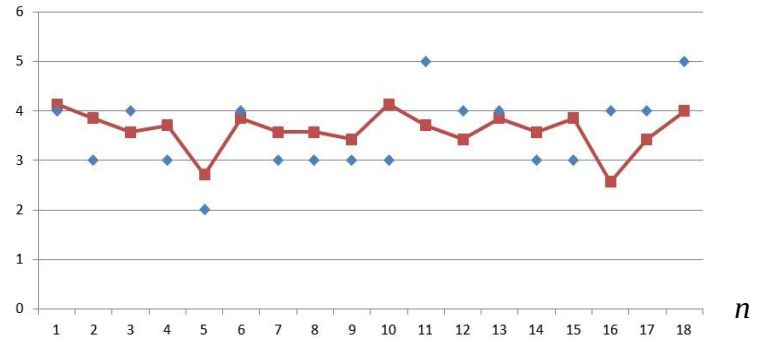


Рис.2 Результаты отклонения признаков объекта №4

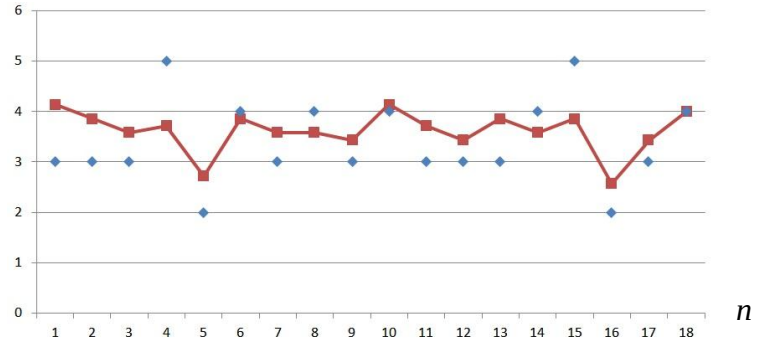


Рис.3 Результаты отклонения признаков объекта №7

В этом и заключается синтез кластеризации и кластерно-иерархического подхода. При едином интегральном показателе начинать с тех объектов, у которых разброс больше.

Совмещаем два метода, кластеризация по отличию признаков и расчет интегрального показателя.

В данном случае может получиться так, что интегральный показатель низкий и он низкий только лишь потому, что более важный признак существенно ниже, чем у остальных исследуемых объектов.

Может получиться так, что одно значение очень большое у менее важного признака, а другое маленькое у важного признака и они будут компенсировать друг друга.

Необходимо выбрать наименьший и увеличить его значение, чтобы он поднялся на уровень со всеми остальными.

Увеличение всего лишь одного признака позволит увеличить общую сумму интегральных показателей по всем объектам.

Интегральные показатели у рассматриваемых в работе объектов приблизительно одинаковые, но приоритетные признаки компенсируют друг друга с наименьшими и наибольшими значениями.

Вывод. В кластерно-иерархическом подходе многократно используется метод анализа иерархий и метод кластеризации. Кластеризация в данной работе предполагает, что увеличение показателей выбранных признаков будет способствовать повышению общего уровня интегрального показателя.

Средний уровень интегрального показателя увеличился, так как были отобраны такие альтернативы, у которых наиболее значимые признаки отклоняются.

Разные подходы к кластеризации, разные расстояния в зависимости от предметной области это и есть вклад в математическое моделирование. В данном случае радиус кластера будет зависеть от финансирования.

Литература

1. Мельников А.В. Кластерно-иерархические методы экспертизы технических и экономических объектов [Текст]: дис. … докт. техн. наук: 05.13.18: защищена 16.09.2014. Воронеж, 2014. 354 с.

2. Жилин Р.А. Численный метод оценки необходимости использования альтернативных коалиций при анализе интегральных показателей опасности нарушителей в сфере физической защиты объектов. Воронежского института ФСИН России, 2020, № 3. С.45-52.

3. Мельников А.В. Моделирование функциональной взаимосвязи результатов экспертизы опасности отдельных видов нарушителей для оценки рисков безопасности охраняемых объектов. Вестник Воронежского института ФСИН России, 2019, № 3. С. 88-92.

4. Melnikov A.V. Method of forming expert coalitions in the context of solving the expertise problem of alternatives with weakly formalized J. Phys.: Conf. Ser. 2020 1479012071.

Сведения об авторе

Жилин Роман Андреевич, преподаватель кафедры тактико-специальной подготовки Воронежского института МВД России; e-mail: zhilin99.zhilin@yandex. ru.

Жмурко Даниил Юрьевич

КОРРЕЛЯЦИЯ ВРЕМЕННЫХ РЯДОВ ПОКАЗАТЕЛЕЙ ДЕЯТЕЛЬНОСТИ АПК С ЦИКЛАМИ АСТРОНИМИЧЕСКИХ ОБЪЕКТОВ

Актуальность статьи состоит в выявлении циклической силы показателей деятельности сложных организации структур (интегрированных производственных систем или ИПС) сахарного подкомплекса АПК имеют наибольшее (наименьшее) отклонение от прогнозных значаний. Зарубежными и отечественными учеными из разных областей науки исследовали процессы воздействия астрономичсекий объектов на жизнедеятельности объектов, процессов и явлений любой природы, происходящих в Солнечной систем.

В статьях посвещенных корреляционному анализу показателей деятельности сложных организационных структур сахарного подкомплекса АПК были представлены степень связей как внутри данного ВР (АКФ и ЧАКФ), так и по отношению к другим временным рядам (кросс-корреляция). Теперь рассмотрим воздествие планет в составе солнечной системы, и их корреляционные связи на исследуемые объекты (их показатели).

Воздействие астрономических циклов на рынок ценных бумаг – это одно из самых загадочных явлений, с которыми приходится иметь дело. Загадочных во многих смыслах. Могу уверенно заявить, что наиболее надежный прогноз дают именно модели, основанные на астрономических циклах. Это является интересным фактом для научного сообщества: ученые не могут этого принять, но и не могут доказать отсутствие связи между этими явлениями.

Механизмы планетных воздействий остаются неясными, корреляция исторических и планетных ритмов до сих пор считается неустановленной, тем неменее наиболее значимые прогрессивные математические модели включают в состав исследования движение астрономических объектов солнечной системы.

В эту группу входят такие астропараметры, как координаты положения планет и других небесных объектов в пространственных координатах (т. е., знаках Зодиака), углы между планетами, скорость планет, планетарные фазы (степень освещенности планет Солнцем) [5].

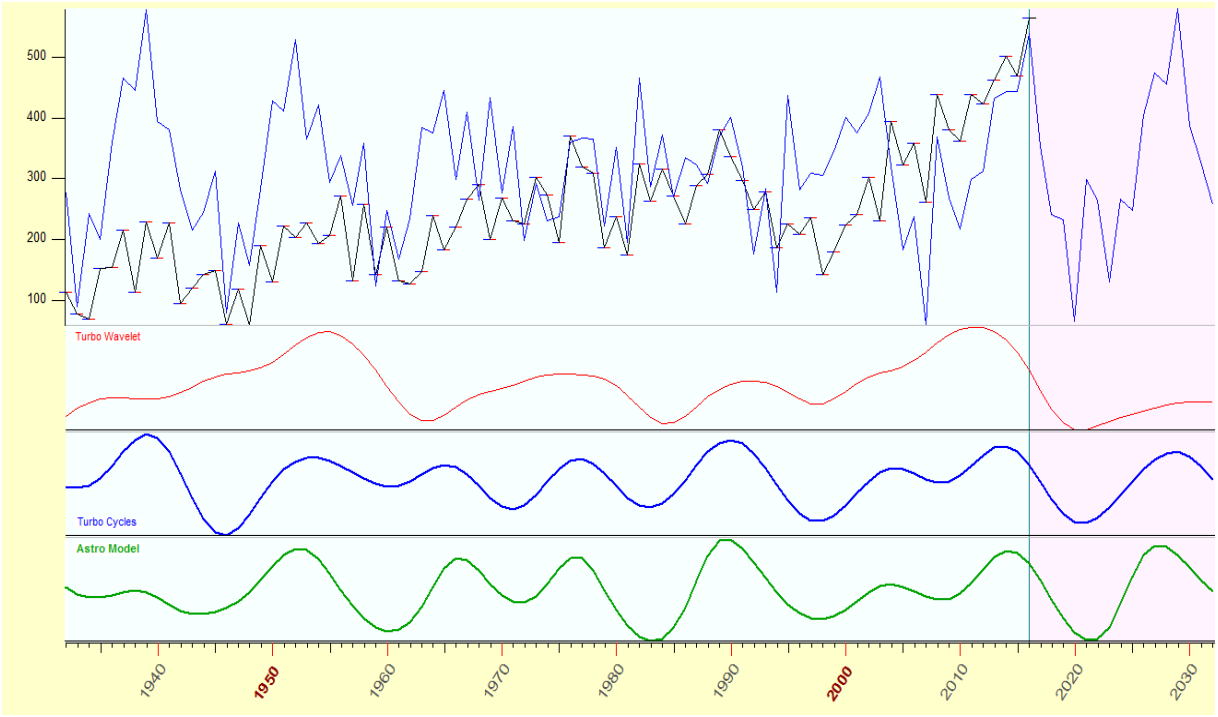


Рис. 1. Циклические колебания во временных рядах урожайность сахарной свеклы в Краснодарском крае на период до 2032 г.

Как создается такая модель? В модели, представленной на рисунке 1 определены в виде трех астрособытий – гелио-цикл Сатурна, гео-цикл Юпитер-Нептун и гео-цикл Юпитер-Плутон. В данной модели сильно проявлен Сатурн и Юпитер. При суммирование этих трех циклов коэффициент корреляции повышается и соответствует 0,833. В качестве примера мы добавим прогнозные линии полученные с помощью спектрального и вейвлет-преобразования.

Полученная информация позволит сделать объективный прогноз по ним на рассматриваемый период (до 2032 г).

В таблицах 1–2 представлены результаты корреляции. Ярко выраженный характер носят так называемые «медленные» планеты, особую роль в исследовании играют Юпитер и Сатурн. Также можно предположить, что их корреляция с астрономическими объектами и носит практически синхронный характер. Особенно это хорошо видно когда добавляется применение методов искусственных нейронных сетей.

Таблица 1

Базовые частоты (циклы) показателей производства сахара

Производство сахара	Цикл	Воздействия планет на объект и их корреляция (R^2)
Мировое, 1864–2018 гг.		
Общее, 1864–2018 гг.	18,32	Меркурий, Марс, Сатурн, Плутон (0,386)
Тростникового	14,58	Луна, Юпитер, Сатурн, Нептун (0,449)
Свекловичного	9,26	Меркурий, Венера, Марс, Юпитер, Нептун (0,455)
В России (Российская империя, СССР и РФ), 1881–2018 гг.		
Общее	8,81	Меркурий, Венера, Марс, Юпитер, Нептун (0,574)
Свекловичного, 1871–2018гг.	25,63	Луна, Марс, Юпитер, Сатурн, Уран (0,622)
Тростникового, 1956–2018 гг.	7,26	Солнце, Луна, Венера, Марс, Сатурн (0,638)
На Кубани, 1921–2015 гг.		
Общее	9,35	Луна, Меркурий, Марс, Уран, Плутон (0,812)
Тростникового, 1960–2018 гг.	9,35	Меркурий, Венера, Юпитер, Сатурн (0,582)
В США, 1832–2015 гг.		
Общее	10,48	Меркурий, Венера, Марс, Юпитер (0,522)
Тростникового, 1832–2018 гг.	22,21	Луна, Марс, Юпитер (0,562)
Свекловичного, 1873–2018 гг.	25,22	Луна, Меркурий, Марс, Уран (0,344)
В отдельных странах		
Куба, 1849–2018 гг.	22,63	Луна, Марс, Сатурн (0,671)
Германия, 1910–2018 гг.	16,52	Луна, Сатурн (0,849)
Бразилия, 1949–2018 гг.	6,81	Меркурий, Венера, Юпитер (0,506)
Индия, 1949–2018 гг.	7,64	Солнце, Луна, Венера, Плутон (0,55)

Таблица 2

Базовые частоты (циклы) производства сахарной свеклы и сахарного тростника

Показатель	Цикл	Воздействия планет на объект и их корреляция (R^2)
Россия (Российская империя, СССР и РФ), 1881–2018 гг. (сахарная свекла)		
Посевная площадь	7,58	Луна, Меркурий, Венера (0,655)
Урожайность	12,61	Меркурий, Сатурн, Нептун, Плутон (0,704)
Валовой сбор	15,57	Венера, Марс, Сатурн, Уран (0,607)
Кубань, 1932–2018 гг. (сахарная свекла)		
Посевная площадь	11,33	Меркурий, Венера, Сатурн, Нептун (0,632)
Урожайность	12,87	Солнце, Венера, Юпитер, Плутон (0,67)
Валовой сбор	13,43	Луна, Венера, Марс, Уран (0,593)
США, 1903–2018 гг. (сахарная свекла)		
Посевная площадь	9,55	Венера, Марс, Уран, Нептун (0,569)
Урожайность	7,07	Меркурий, Юпитер, Сатурн, Уран (0,593)
Валовой сбор	15,35	Солнце, Луна, Венера, Марс, Сатурн (0,535)
США, 1909–2018 гг. (сахарный тростник)		
Посевная площадь	16,08	Луна, Венера, Марс, Уран (0,577)
Урожайность	19,27	Луна, Юпитер, Сатурн, Нептун (0,633)

Показатель	Цикл	Воздействия планет на объект и их корреляция (R^2)
Валовой сбор	7,24	Луна, Меркурий, Сатурн (0,617)
Германия, 1920–2018 гг. (сахарная свекла)		
Посевная площадь	17,62	Юпитер, Сатурн, Нептун, Плутон (0,708)
Урожайность, 1920–2015 гг.	8,34	Меркурий, Венера, Марс (0,517)
Валовой сбор, 1836–2015 гг.	28,16	Меркурий, Сатурн, Уран, Нептун, Плутон (0,492)
Бразилия, 1960–2018 гг. (сахарный тростник)		
Посевная площадь	7,69	Меркурий, Юпитер, Сатурн, Уран (0,376)
Урожайность	8,91	Меркурий, Юпитер, Сатурн, Уран, Плутон (0,44)
Валовой сбор	9,36	Луна, Юпитер, Уран (0,404)
Индия, 1949–2018 гг. (сахарный тростник)		
Посевная площадь	10,74	Венера, Марс, Сатурн, Нептун, Плутон (0,525)
Урожайность	7,43	Луна, Меркурий, Марс, Сатурн, Нептун (0,514)
Валовой сбор, 1950–2015 гг.	10,74	Венера, Марс, Сатурн, Нептун, Плутон (0,471)

В подавляющем большестве, любые социально-экономические астропрогнозы строятся на солнечной активности, но помимо этих явлений в Солнечной системе существуют и другие астрообъекты, которые также существенно влияют на процессы и явления происходящие на Земле.

Часто, на практике, оказывается так, что «чисто астрономический» цикл дает более сильную корреляцию, чем хорошо известный экономистам годичный цикл (тот самый, который обуславливает наличие сезонных составляющих).

По классификации циклы бывают внешними и внутренними.

Внешние циклы – это так называемые коррелируемые циклы, т. е. связанные с какими-то сторонними факторами влияния. Например, влияние циклов Солнца, Луны и других планет на сахарный рынок, которое проявляется опосредованно – через воздействие на психическое и эмоциональное состояние участников сахарного подкомплекса.

Внутренние циклы – это временные закономерности, выявляемые непосредственно из самого сигнала. То есть, циклы, которые можно извлечь из данных, отражающих изменение величин каких-либо показателей, являются внутренними [1].

На практике, существует несколько перспективных техник анализа, позволяющих выявлять внешние и внутренние циклы с помощью математико-статистических методов и оценивать эффективность их через объективные критерии, например, коэффициент корреляции. Другие неменее известенные это индексы или индикаторы Брэдли и Барбо [6].

Индикатор Брэдли

Индикатор (барометр) Д. Брэдли – одноименная модель прогнозирования на рынке акций. Д. Брэдли полагал, что циклы в массовой психологии, проявляющиеся в движении рынка акций, определяются планетарными взаимоотношениями. Он определил 190 значимых комбинаций позиций планет, отраженных в ряде долго- и среднесрочных индикаторов.) в 1940-х годах. Метод основан на вычислении планетарных конфигураций для определенной даты. Анализ исторических данных по макроэкономическим динамическим рядам показывает, что этот индикатор действительно является эффективным инструментом. Такие аналитики, как Дж. Фейворс и У. Энг считают его одним из лучших индикаторов. У. Энг в своей книге «Технический анализ акций, опционов и фьючерсов» назвал его лучшим индикатором для определения разворотных точек рынка (пример расчетов, связанных с ним, см. рисунки 2–3).

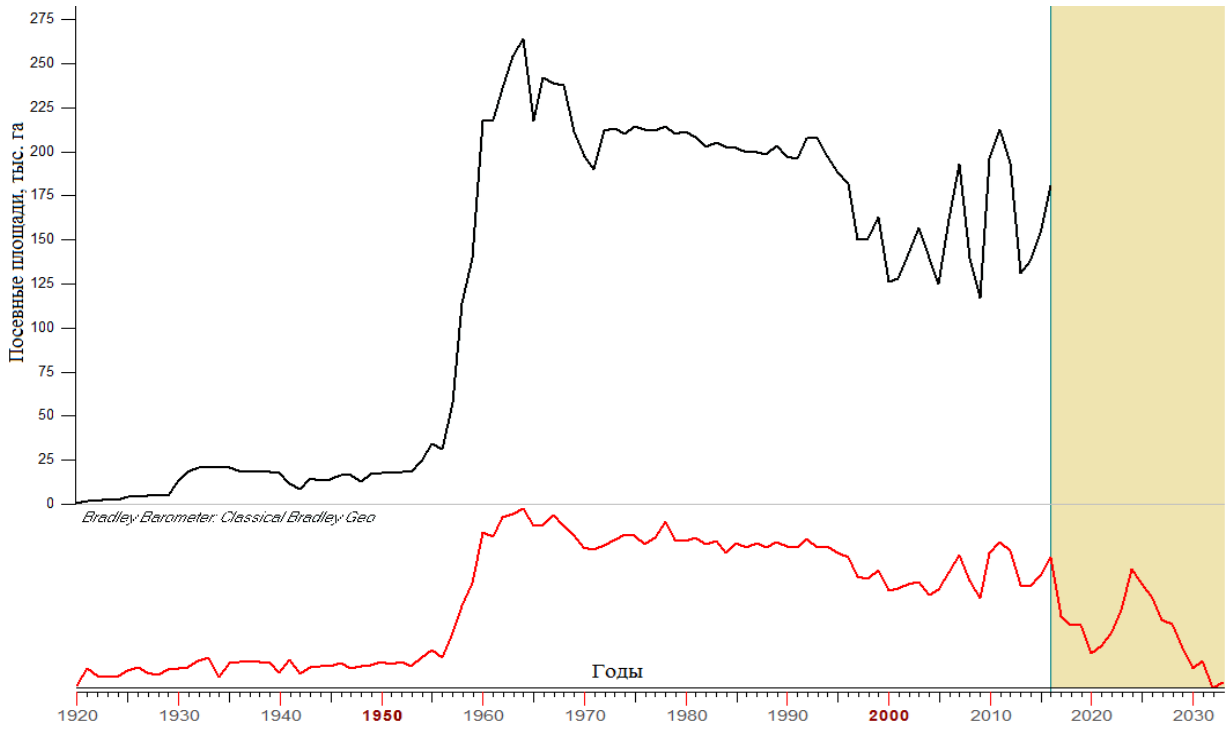


Рис. 2. Посевные площади сахарной свеклы на Кубани, 1920–2016 гг. и его астроиндикатор Брэдли (расчет произведен в программе Timing Solution Advance)

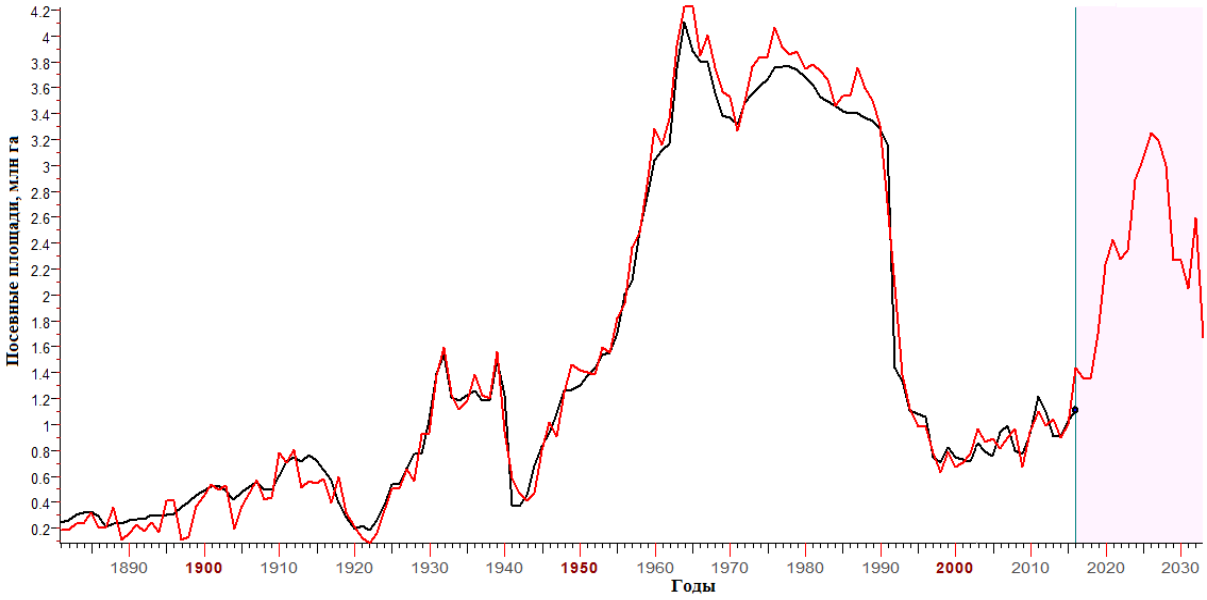


Рис. 3. Посевные площади сахарной свеклы в России, 1881–2016 гг. и его астроиндикатор Брэдли (расчет произведен в программе Timing Solution Advance)

Однако, движение индикатора не всегда совпадает с движением изучаемых величин, у него есть одно важное преимущество, которое позволяет его эффективно использовать. Когда индикатор меняет направление индекса DJIA также разворачивается почти в то же самое время (+/– 1-2 дня в большинстве случаев).

Алгоритм расчета по индикатору Брэдли

При построении сидерограммы необходимо иметь полную карту позиций планет для каждого конкретного дня (недели, месяца и т. д.). Идея заключается в том, что

необходимо отследить данные по конфигурациям всех планет (кроме Луну). Учитываются все основные конфигурации +/– 15°. Чем ближе к границам диапазонам, тем меньше влияние угла. Все квадратуры (90° и 270°) и оппозиции (180°) считаются негативным, тогда как все секстили (60° и 300°) и трины (120° и 240°) считаются позитивными. Соединения планет рассматриваются отдельно, поскольку данная конфигурация для разных планет имеет разное влияние.

Чтобы вычислить точный «вес» каждой конфигурации берется расстояние до каждой конфигурации в градусах, вычитаем его из пятнадцати, делим результат на пятнадцати и умножаем результат на десять. В результате для точных конфигураций будем иметь «вес» равный десять, а для ситуаций +/– 15° значение равное 0. Таким образом, вес зависит от приближения к точке конфигурации. Это вычисление делается для всех тридцати шести планетарных комбинаций.

Исключение. Склонение планет Венеры и Марса. Для других планет склонения не требуются. Для северного склонения используются положительные значения, для южного отрицательные. Затем они складываются и делятся на два.

Когда все данные сгруппированы для каждого дня, вы отделяете долгосрочные конфигурации от среднесрочных. Все конфигурации «медленных» планет: Юпитера, Сатурна, Нептуна, Урана и Плутона с конфигурациями планет той же группы считаются долгосрочными. Остальные планетные конфигурации считаются краткосрочными. Далее вычисляется индикатор Брэдли по следующей формуле:

$$S = W (L + C) + K,$$

W – особый фактор, придающий вес долгосрочным конфигурациям. Д. Брэдли рекомендует применять на практике W = 4, C – склонения, L – среднее долгосрочных конфигураций, К – среднее среднесрочных конфигураций.

Циклический индекс Барбо

Среди множества инструментов, доступных сегодня для анализа, особый интерес представляют циклы планет Солнечной системы. Метод, который будет изложен был открыт французом А.-Ж. Гушоном. А. Барбо переработал его более детально, и в итоге метод получил называние циклический индекс Барбо. Этот подход прост и чрезвычайно интересен при оценке состояния и тенденций развития мира в его политико-экономическом и других аспектах [3].

В этом методе задействованы планеты, отдаленные от Солнца, которые, как считается, символизируют длительные периоды (движутся медленно) в развитии человечества. К таким планетам относятся Юпитер, Сатурн, Уран, Нептун и Плутон. Если из перечисленных планет составить пары, то получится в общей сложности 10 единиц.

Для каждой пары планет в любой момент времени может быть определено угловое расстояние между планетами, составляющими пару. А.-Ж. Гушон заметил: если такие расстояния посчитать на начало года, а затем все их сложить, то получим некоторое число, характеризующее данный год. Если определить такое число для каждого года, а затем все числа отложить на графике, то получим некую кривую. В общем и целом, он показывает главные тренды глобальной напряженности, роста и упадка с довольно высокой точностью [2].

Например, для XX в. наиболее заметные и длительные «спады» на графике будут соответствовать периодам международных кризисов. Такие экстремумы на графике точно указывают: периоды I и II Мировых войн, Карибского кризиса, войны во Вьетнаме, а также мирового экономического кризиса начала 80-х годов, когда реальной войны не было, но «холодная война» шла полным ходом.

А. Барбо подвел теоретическую базу под открытие А.-Ж. Гушона, показав, что движение фазовой точки графика есть не что иное, как текущие пульсации «Великого Года», открытого Платоном. Он считал, что развитие мира происходит циклами, или

«годами», длительностью по тридцать шесть тыс. лет каждый. В начале такого цикла все планеты располагаются в сверхсоединении в одной точке Зодиакального круга.

Чем ниже опускается кривая графика, тем меньшее значение имеет сумма угловых расстояний в парах планет, тем ближе планеты к исходному сверхсоединению, тем ближе мир приближается к хаосу. И наоборот, чем выше график, тем больше расстояние между планетами, тем больше в нем оптимизма и порядка.

Если начало года отражает весь год, то начало существования чего-то или кого-то отражает жизнь этого субъекта или объекта. Государство – очень сложно организованное «существо», живущее своей жизнью и подчиняющееся законам – земным и космическим. На него тоже влияют циклы высших планет, а значит, можно построить и график изменения индекса Барбо [4].

Список литературы

1. Белкин В. А. Циклы цен на нефть и магнитных бурь: механизм и факты сильных связей (1861–2015 гг.) [Электронный ресурс] // В. А. Белкин / Челябинск: Челябинский гуманитарий №3 (32). 2015. – С. 32–45. – Режим доступа: http://timing-solution.livejournal.com/11570.html.

2. Белкин В. А. Большие циклы солнечной активности как основа больших циклов конъюнктуры (Электронный ресурс) // В. А. Белкин / Челябинск: Челябинский гуманитарий. Экономика. №4 (17). 2011. – С. 13-24. – [Режим доступа]: https://cyberleninka.ru/article/n/bolshie-tsikly-solnechnoy-aktivnosti-kak-osnova-bolshih-tsiklov-konyunktury.

3. Модели Spectrum на основе вэйвлет-циклов с использованием астрономии [Электронный ресурс]. – Режим доступа: http://www.timingsolution.ru/stat/All%20about%20 Spectrum%20Models%20Step%20By%20Step%20guide.htm#A3.

4. Модуль: Bradley barometer. [Электронный ресурс]. – Режим доступа: https://timing-solution.livejournal.com/.

5. Разумов И. К. Корреляция исторических ритмов с циклами верхних соединений планет и Солнца [Электронный ресурс] // И. К. Разумов, В. А. Петров / – М.: Сознание и физическая реальность, №4. 2012. – С. 37-55. – [Режим доступа]: http://www.nostradam.ru/research/I.Razumov.V.Petrov.Historical%20rhythms.htm.

6. Чижевский А. Л. Земное эхо солнечных бурь: 2-е изд. – М.: Мысль, 1976. – 340 с.

7. The Bradley Siderograph and the Advanced Astro Indicator [Электронный ресурс]. – Режим доступа: https://bradleysiderograph.com/historical-correlation-analysis-for-the-advanced-astro-indicator/.

Сведения об авторе

Жмурко Даниил Юрьевич, кандидат экономических наук, доцент, преподаватель кафедры информатики и математики Краснодарский университет МВД России; e-mail: danis1982@list.ru.

Иванов Вячеслав Юрьевич,
Волков Антон Григорьевич

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ ФИКСАЦИИ АУТЕНТИЧНЫХ ФОТОСНИМКОМ НА БАЗЕ СМАРТФОНА С ОС ANDROID

Серьезной проблемой, появившейся после перехода на цифровую съемку, стала возможность редактирования полученных фотографий без использования труднодоступного оборудования. Многие люди умеют использовать программные продукты,

применяемые для редактирования изображений. Это создает угрозу фальсификации фотографий при формировании доказательной базы как при рассмотрении гражданских дел, так и уголовных. По причине быстрого роста числа так называемых цифровых доказательств, которые зачастую образуются с использование современных телефонов, смартфонов и так далее возникла необходимость разработать программный комплекс, который бы позволил пользователю сделать фотографию, и в последующем легко подтвердить ее аутентичность.

Цифровая фотография, в отличии от аналоговой, где носителем данных является фотопленка или же фотобумага (в случае проявленных фотографий), может находиться на более большом перечне носителей: жесткие магнитные диски, магнитно-ленточные накопители, различные чипы флэш памяти. Хотя данный вид съемки и получил широкое распространение ввиду своих неоспоримых плюсов: скорость съемки, отсутствие высоких профессиональных требований к фотографу, простота и скорость получения результатов, компактность аппаратуры, в случае рассмотрения данных фотоснимков в суде могут возникать некоторые проблемы. Связанно это с тем, что цифровая фотография относительно легко может быть отредактирована без применения специальных технических средств.

В настоящее время арбитражные суды принимают в качестве доказательств фото, сделанные на телефон. Как правило, суды признают фотографии надлежащими доказательствами, если возможно установить дату, время и место фотосъемки. Сведения о дате, времени и месте могут быть получены посредством анализа фотографии, сопоставления с другими доказательствами по делу, либо из технической информации к фотографии в цифровой форме (включая геотеги), а также из самого телефона, если фотография не удалена или может быть восстановлена.

Если цифровая фотография имеет набор атрибутов, позволяющих установить дату, место и способ ее получения, а также механизм проверки подлинности данных атрибутов, то в данном случае возможно обойтись без назначения судебной экспертизы, что позволило бы значительно снизить как нагрузку на сотрудников экспертно-криминалистических подразделений, так и общую продолжительность рассмотрения дел в суде.

Следовательно, необходимо сформировать набор требований к цифровой фотографии, соблюдение которых, позволило бы сказать, что данная фотография является аутентичной и может быть использована в качестве доказательства в суде.

Исходя из вышеизложенного, данные требования будут содержать в себе:

1. Возможность достоверно установить время, дату и место получения цифрового изображения.

2. Возможность установить устройство, на которое производилась фотосъемка.

3. Возможно подтвердить подлинность данных, изложенных в п 1, 2 данного списка.

Описание функциональных модулей системы.

Общая структура представляет собой:

1. Сайт – Интернет-ресурс, предоставляющий информацию о сохраненных фотографиях.

2. Мобильное приложение – интерфейсное приложение для смартфона Android. Приложение взаимодействует с сервером API, для сохранения сделанных фотографий

Краткий алгоритм работы мобильного приложения:

1. При нажатии кнопки съемки в первый раз на устройстве, приложение должно получить разрешение от пользователя на использование геопозиции, доступ к внутреннему хранилищу и к камере.

2. Если какое-либо из разрешений не получено, а равно отсутсвует связь с

сервером APi то съемка фото должна быть невозможна и выведено уведомление пользователю, с предложением исправить проблему (заново запросить разрешения, предложить проверить интернет соединение либо подождать, пока доступ к серверу не будет восстановлен).

3. После того как пользователь сделает снимок, к нему добавляются мета данные (Дата, Время, Геолокация), файл предохраняется во внутреннее хранилище приложения, после чего высчитывается контрольная сумма по алгоритму SHA512, отправляется на API сервер, от которого необходимо получить положительный ответ, если же ответ не был получен, то пользователю выводится уведомление, а фотография вместе с сопутствующей информацией не сохраняется, после чего(при положительном ответе) вся вышеизложенная информация сохраняется во внутреннюю БД приложения (SQLite).

4. Экран «Галерея» открывается при нажатии на кнопку «галерея» в верхней части приложения или путем свайпа влево (длинное движение пальцем в направление от правого края экрана к левому).

5. Пользователю отображаются карточки со сделанными фотографиями и дополнительной информацией/функционалом.

Сайт предназначается для поиска уже загруженных пользователями фотографий.

Поиск производится по хэш сумме. При наличии фотографии искомой контрольной суммой в базе данных сайта, пользователю отображается сама фотография, ее дата съемки, данные о местоположении на момент съемки и элемент управления, предназначенный для поиска другой фотографии/перехода на страницу со строкой поиска.

Литература

1. Федеральный закон «О полиции» от 07.02.2011 N 3-ФЗ
2. Федеральный закон от 31 мая 2001 г. N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»
3. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ
4. Постановление Пленума Верховного Суда РФ от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам»
5. Приказ МВД России от 29.06.2005 N 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»
6. Приказ МВД России от 11 января 2009 г. N 7 «Об утверждении наставления по организации экспертно- криминалистической деятельности в системе МВД России».
7. «Книга по фототехнической и видеотехнической экспертизе» Г.П. Шамаев, Москва, Норма: ИНФРА-М, 2017, стр. 528

Сведения об авторах

Иванов Вячеслав Юрьевич, кандидат технических наук, доцент, начальник кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя.

Волков Антон Григорьевич, слушатель факультета подготовки специалистов в области информационной безопасности Московского университета МВД России имени В.Я. Кикотя.

Иванов Игорь Петрович

ВОЗМОЖНОСТИ МАТЕМАТИЧЕСКИХ МЕТОДОВ И СОВРЕМЕННЫХ ЦИФРОВЫХ РАЗРАБОТОК В ПРОГНОЗИРОВАНИИ И ПРЕДОТВРАЩЕНИИ ПРЕСТУПЛЕНИЙ

Прогнозирование и выработка принятия верных управленческих решений составляет фундаментальную основу в любой сфере деятельности. Сотрудникам органов внутренних дел прогнозирование и выявление закономерностей совершения преступлений помогает находить и выбирать наиболее оптимальные методы борьбы с преступностью. В процессе прогнозирования можно использовать два подхода:

- индуктивный – от частного к общему;
- дедуктивный – от общего к частному.

Поисковое прогнозирование определяет состояние объекта исследования в будущем и настоящем, выявляет полученные в результате опыта закономерности и позволяет планировать изменение ситуации в будущем.

Преступность – очень сложный феномен. На протяжении своего существования человечество пытается постичь его сущность. Постепенно человечество пришло к убеждению, что преступность как специфическое явление следует изучать специально, ибо для того, чтобы вести борьбу с преступностью, необходимо познать ее.

Данное явление является стихийным и собирательным. В связи с особенностями трактования термина преступность различными авторами, одинаковые элементы были собраны в одно определение: «преступность – это негативное социально-правовое явление, имеющее свои закономерности, количественные и качественные характеристики, влекущее отрицательные, вредные для общества последствия и требующее специфических государственных и общественных антикриминальных мер воздействия». Другими словами, каждое преступление складывается из различных общественно опасных посягательств, которые совершаются разными людьми, а те уже, руководствуются собственными мотивами и выбирают собственные методы для достижения поставленной цели.

В недалеком прошлом, в органах внутренних дел для прогнозирования и изучения преступности и явлений, в теории криминологии основное место занимали специальные математические методы: экстраполяция, моделирование и экспертные оценки.

Рассмотрим более подробно основные методики прогнозирования преступности и возможности их применения в органах внутренних дел.

Метод экстраполяции заключается в изучении тренда изменения показателей прогнозируемого объекта, в выявлении закономерностей их развития преобладающих в прошлом, и определении его развития в будущем, при условии, что обстоятельства, оказывающие корреляционные связи не претерпят сильных изменений. Тренд – это линия указывающая направление движения показателей. Линия тренда должна описывать, как можно точнее показатели конкретного изучаемого явления и отстоять от них на минимальную сумму квадратов расстояния. Данный показатель определяется на основе учета среднеквадратичных отклонений фактических данных от расчетных значений тренда.

Методы экстраполяции по оценкам проведения аналитической деятельности могут давать положительные результаты для изучения ближайшего будущего и имеют малый эффект при составлении долгосрочных прогнозов. При увеличении прогнозируемого периода увеличивается качество и количество ошибок. Поэтому данный метод позволяет абстрагироваться только от мелких и несущественных свойств прогнозируемого явления.

Прогнозы преступности, полученные с помощью методов экстраполяции, позволяют обнаружить неблагоприятные тенденции развития изучаемых явлений. Построение тренда – это один из самых простых способов прогнозирования преступности. Более детальное изучение и проведение анализа преступности, возможно, проводить с помощью других методов.

Метод моделирования – это способ построения математической модели образа криминологического объекта, содержащий в себе его основные существенные характеристики и свойства. При построении модели необходимо определить математическую закономерность поведения изучаемых факторов и их тенденций будущего развития, чем при построении простой экстраполяции. Разработка модели данных должна быть проще прототипа, так как в ней происходит процесс абстрагирования от второстепенных или не коррелируемых характеристик. Метод моделирования относится к числу основных методов аналитической деятельности. Поэтому для проведения данных исследований, необходим профессиональный опыт в данном направлении деятельности и знание доказательных методов используемых в эксперименте. «Прогноз начинается с продолжения в будущее какого-либо явления, а кончается воспроизведением этого явления в более или менее упрощенном виде в модель, так как в действительности такого явления пока не существует». Другими словами, модель становится аналогом исследуемого объекта. Достоинством данного метода заключается в том, что во время построения математической модели можно сосредоточить внимание только на самых важных характеристиках изучаемых явлений. Одним из свойств

Метод экспертных оценок основывается на наличии практического опыта и теоретических знаний об изучаемых явлениях и заключается в обобщении мнений экспертов. Практические данные, не являются значимыми, так как они не поддаются формализации. Процедура экспертных оценок зависит от качественной разработки анкетных материалов, по которым происходит оценка значимости и ранжирования объектов исследования. Качественная обработка результатов анкетирования экспертов – залог успешного проведения указанного метода. Отрицательной характеристикой данного метода считается – отсутствие гарантии достоверности ответа респондента. Результатом выводов является обобщенное заключение экспертов, базирующееся на их практическом и научном опыте или профессиональном мастерстве, полученном во время профессиональной деятельности.

Итогом результата экспертных оценок является формирование индивидуального мнения или общего вывода на основе обработки ответов группы экспертов. При проведении опроса могут возникать недостатки, основанные на спецификации ситуации опроса. При этом гарантия достоверности результатов снижается.

Кроме основных методов прогнозирования применяют частные методы: частотный анализ, корреляционный анализ, выборочный анализ, факторный анализ и другие.

Все перечисленные методы основываются на изучении не только самого изучаемого явления, но и других факторов, находящихся во взаимосвязи между ними.

Для прогнозирования в современном мире применяются новейшие технологии обработки больших массивов данных, разрабатываются мощные процедуры обработки информации на основе нейросети, методика обоснованной теории, применение методов искусственного интеллекта, увеличение количества интернет вещей.

Перенимая опыт зарубежных коллег, при решении рассмотренных вопросов, можно привести положительные факты применения современных It-технологий при расследовании и предотвращении преступлений.

Процесс Хоукса, разработанный в 1970 году, эффективен и в настоящее время. Позволяет прогнозировать места ограблений и перестрелок между преступниками на основе машинной обработке данных.

Программа PredPol при помощи специально разработанных алгоритмов позволила снизить количество совершаемых преступлений. Сотрудникам полиции ежедневно на карту поступала информация о предполагаемых преступлениях. Наличие сотрудников полиции в указанных местах позволяли по горячим следам раскрывать совершенные преступления, либо преступления не совершались в результате присутствия сотрудников полиции в указанном районе.

Технологии, направленные на прогнозирование будущих преступлений, проходят испытания и приносят свои выгоды не в виртуальном, а в реальном мире. Одну из ведущих ролей для предсказаний преступности сегодня играют специалисты в области информационных технологий.

В современном мире, характеризующимся стремительным развитием информационных технологий, больших данных и нейросетей, неопределенность будущего становится лишь чисто математической проблемой. Статистический анализ и другие методы способны уже сейчас вычислять паттерны поведения людей, а разрабатываемые алгоритмы позволяют определять вероятность появления событий, основываясь на данных совершенных в прошлом. Прогнозирование позволяет человечеству избегать грядущих кризисов и катаклизмов, а полицейским – раскрывать, предотвращать преступления и уменьшать «латентность преступности».

Литература

1. Аванесов, Г.А. Теория и методология криминологического прогнозирования. М., 1972.

2. Забаев, И.В., Неформализованные данные: методы сбора и анализа. [Электронный ресурс]. – Режим доступа: https://ecsocman.hse.ru/data/2012/08/20/1265223821/3абаев.pdf

3. Правовая статистика: Практикум по специальности 030505.65 – Правоохранительная деятельность / И.П. Иванов, В.А. Кемпф – Барнаул: БЮИ МВД России, 2011. – 45 с.

4. Правовая статистика: учебное пособие. / И.П. Иванов. – Барнаул, БЮИ МВД России, 2013. – 110 с.

Сведения об авторе

Иванов Игорь Петрович, кандидат педагогических наук, доцент, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: iv_on_off@mail.ru

Коимшиди Георгий Феофилактович,
Саркисян Армен Жораевич

АИС «АНАЛИЗ И ПРОГНОЗ ПРЕСТУПНОСТИ» НА ПЛАТФОРМЕ EXCEL КАК ЭЛЕМЕНТ РАБОЧЕГО МЕСТА КРИМИНОЛОГА

В России в конце прошлого века лидерами в анализе и прогнозе преступности были НИИ Академии МВД СССР (ныне Академии Управления МВД России). А с 90-х годов – ВНИИ МВД России, которое в начале каждого года стало проводить комплексный анализ состояния преступности в Российской Федерации и его прогноз [1]. В системе МВД России с 1991 г. ежегодный анализ преступности за пять лет предоставлял ГИАЦ МВД России [2]. С 2003 г. анализ и прогноз преступности ежегодно стал проводиться в Генеральной прокуратуре – НИИ проблем укрепления законности и правопорядка при Генеральной прокуратуре Российской Федерации (ныне НИИ Университета прокуратуры Российской Федерации) [3].

Методы анализа и прогноза преступности достаточно добротно разработаны и уже вошли в многочисленные учебники ведущих криминологов России, например, Долговой А.И. [4], Лунеева В.В. [5] и многих других.

Информационным обеспечением анализа и прогноза преступности, в основном, являются формы статистической отчетности ГИАЦ МВД России (ежегодные, ежеквартальные и ежемесячные) [7].

Во ВНИИ МВД России для информационного обеспечения ежегодного комплексного анализа преступности за прошедшие годы на платформе Excel были разработаны АИС по различным формам учета: 494 (ранее 451), 493 (450), 492 (458), 491 (453) и др. АИС представляют собой двухконтурные Банки Данных. Первый контур – база данных (БД) и второй – система управления базой данных (СУБД). Это два файла в формате Excel. Рассмотрим для примера АИС по форме 494 «Оперативная статистическая информация о состоянии преступности и расследовании преступлений». Первый контур АИС (БД) – файл Excel, на страницах которого систематизируется информация о показателях преступности в регионах. На каждой странице собираются данные из некоторых столбцов различных разделов формы 494. Название страницы соответствует названию выбранного столбца из формы. В табл. 1 представлен фрагмент листа: данные о количестве зарегистрированных преступлений за отчетный период (нарастающим итогом).

Таблица 1

Количество зарегистрированных преступлений (нарастающим итогом)

		янв.08	фев.08	мар.08	апр.08	май.08
111	1	94	182	261	346	428
171	1	3046	6365	10213	13678	17149
172	1	851	1832	2938	3836	4711
511	1	2485	5104	7463	9942	12137
571	1	3723	7773	11714	15618	19556
…						
1200	1	259548	540464	848536	1134996	1409888
9501	1	60320	121919	188920	250483	309561
…						

Первый столбец листа БД – идентификатор региона в формате ГИАЦ, второй – номер одной из строк (вид преступления), а следующие столбцы – значения показателя за соответствующий отчетный период: 3 столбец – за январь 2008 г., 4 – за январь-февраль 2008 г. и т.д. На каждый вид преступления отводится 94 строки: 85 для субъектов Российской Федерации, 1 – для Российской Федерации и 8 – для федеральных округов.

СУБД – это файл в формате Excel, на каждой странице которого можно получить информацию о состоянии преступности определенного вида в регионах России. Связь СУБД с БД осуществляется с помощью двух функций из предлагаемых платформой Excel: АДРЕС() – адрес ячейки в БД, где хранится значение требуемого данного, и ДВССЫЛ() – ссылка на адрес нужной ячейки. Для построения таблиц, графиков, получения других рассчитываемых показателей преступности, а также для типологии субъектов Российской Федерации по качественному показателю преступности используются еще три функции: логическая ЕСЛИ() – для получения того или иного значения в случае выполнения или не выполнения заданного условия, РАНГ() – для определения ранга региона по выбранному показателю в массиве субъектов Российской Федерации, и ПОИСКПОЗ() – для определения относительной позиции в массиве элемента, соответствующего указанному значению. А также для расчёта требуемого показателя ис-

пользуются различный статистические формулы, которые берутся из учебников по статистике, например, Лунеева В.В. [5].

Система позволяет строить графики динамики количества зарегистрированных, раскрытых, нераскрытых преступлений, выявленных лиц, погибших лиц или получивших тяжкий вред здоровью всей преступности или отдельных ее видов в России, в федеральном округе или в выбранном субъекте Российской Федерации. На рис. 1 представлена динамика количества зарегистрированных преступлений в Краснодарском крае. При этом можно перейти на страницу, где будет даны графики ежемесячной динамики выбранного показателя (в том числе и в виде гистограммы).

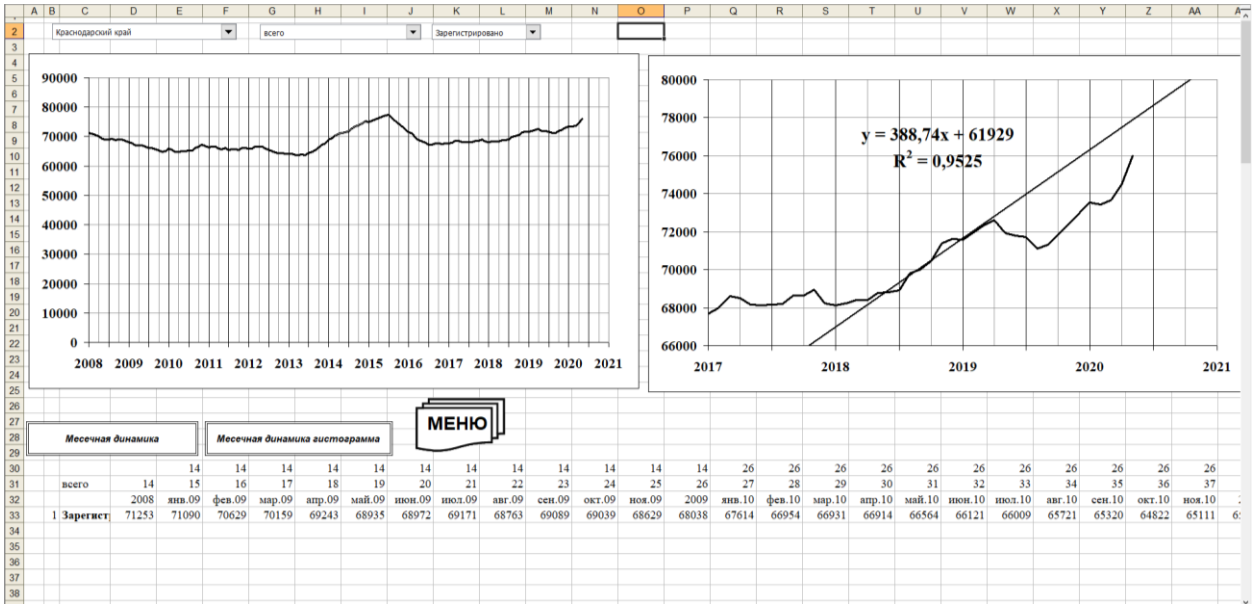


Рис. 1. Лист СУБД с графиками динамики преступности.

Для сравнения динамики коэффициентов преступности в регионе в СУБД есть листы с графиками динамики этого показателя (рис. 2).

Из рис. 2 видно, что коэффициент преступности в Южном федеральном округе меньше, чем в России в целом, а в Краснодарском крае – меньше, чем в округе. Однако, в апреле 2021 г. разница между ними заметно уменьшилась.

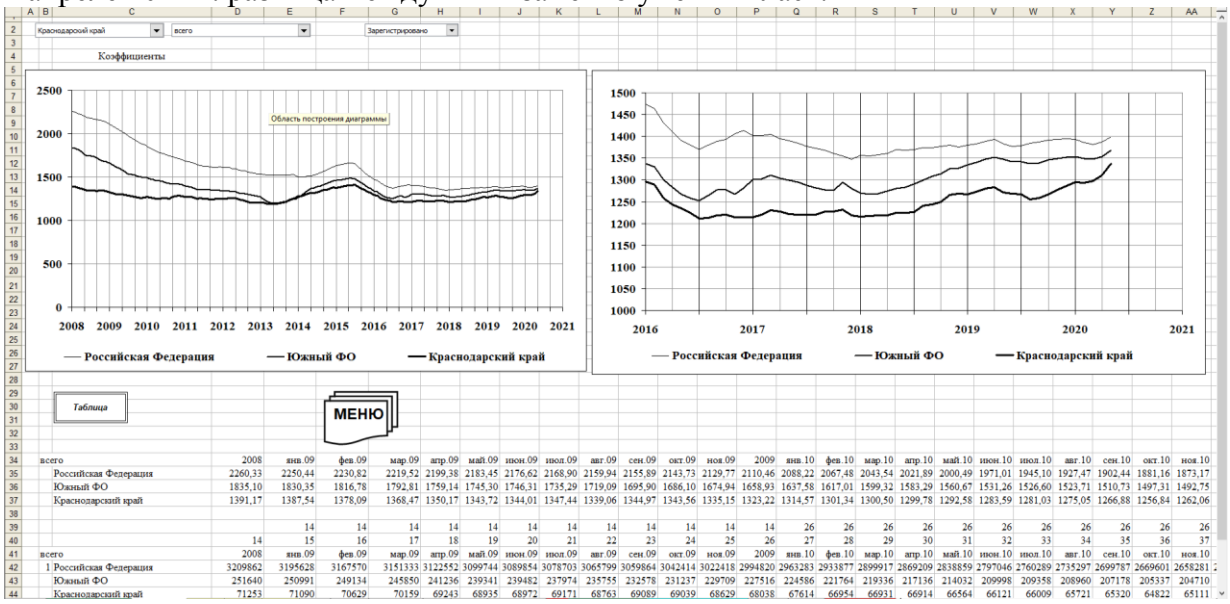
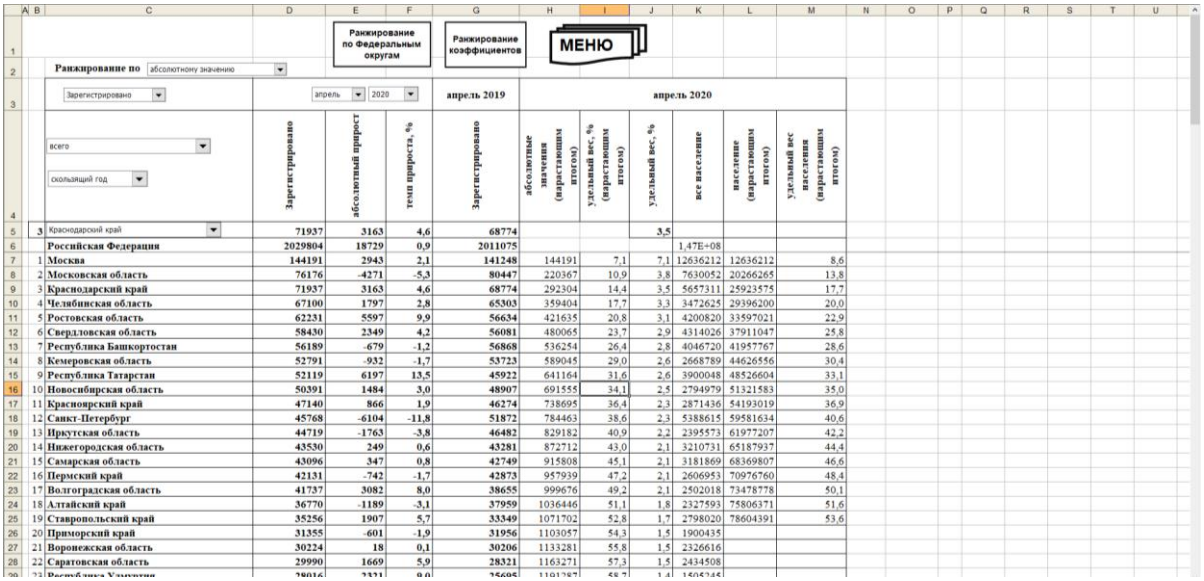


Рис. 2. Лист СУБД с графиками динамики коэффициентов преступности.

В системе возможно ранжировать субъекты Российской Федерации по абсолютным показателям: по их абсолютным значениям, а также по абсолютному или относительному приросту (рис. 3). По состоянию на 1 мая 2021 г. за 12 прошедших месяцев более трети (34,1 % – см. ячейку I16) преступлений зарегистрировано в 10 субъектах Российской Федерации.



Ранжирование по Федеральным округам | Ранжирование коэффициентов | МЕНЮ

Ранжирование по: абсолютному значению

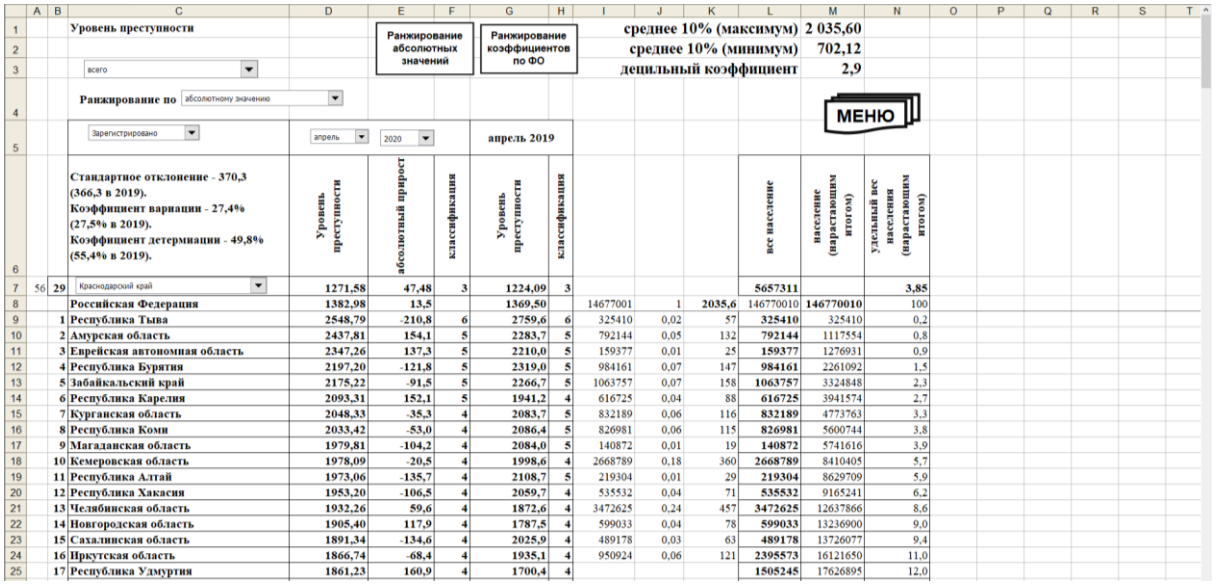
Зарегистрировано | апрель | 2020

			Зарегистрировано	абсолютный прирост	темп прироста, %	Зарегистрировано	абсолютные значения (нарастающим итогом)	удельный вес, % (нарастающим итогом)	удельный вес, %	все население	население (нарастающим итогом)	удельный вес населения (нарастающим итогом)
			всего			апрель 2019	апрель 2020					
			скользящий год									
3		Краснодарский край	71937	3163	4,6	68774			3,5			
		Российская Федерация	2029804	18729	0,9	2011075				1,47E+08		
1		Москва	144191	2943	2,1	141248	144191	7,1	7,1	12636212	12636212	8,6
2		Московская область	76176	-4271	-5,3	80447	220367	10,9	3,8	7630052	20266265	13,8
3		Краснодарский край	71937	3163	4,6	68774	292304	14,4	3,5	5657311	25923575	17,7
4		Челябинская область	67100	1797	2,8	65303	359404	17,7	3,3	3472625	29396200	20,0
5		Ростовская область	62231	5597	9,9	56634	421635	20,8	3,1	4200820	33597021	22,9
6		Свердловская область	58430	2349	4,2	56081	480065	23,7	2,9	4314026	37911047	25,8
7		Республика Башкортостан	56189	-679	-1,2	56868	536254	26,4	2,8	4046720	41957767	28,6
8		Кемеровская область	52791	-932	-1,7	53723	589045	29,0	2,6	2668789	44626556	30,4
9		Республика Татарстан	52119	6197	13,5	45922	641164	31,6	2,6	3900048	48526604	33,1
10		Новосибирская область	50391	1484	3,0	48907	691555	34,1	2,5	2794979	51321583	35,0
11		Красноярский край	47140	866	1,9	46274	738695	36,4	2,3	2871436	54193019	36,9
12		Санкт-Петербург	45768	-6104	-11,8	51872	784463	38,6	2,3	5388615	59581634	40,6
13		Иркутская область	44719	-1763	-3,8	46482	829182	40,9	2,2	2395573	61977207	42,2
14		Нижегородская область	43530	249	0,6	43281	872712	43,0	2,1	3210731	65187937	44,4
15		Самарская область	43096	347	0,8	42749	915808	45,1	2,1	3181869	68369807	46,6
16		Пермский край	42131	-742	-1,7	42873	957939	47,2	2,1	2606953	70976760	48,4
17		Волгоградская область	41737	3082	8,0	38655	999676	49,2	2,1	2502018	73478778	50,1
18		Алтайский край	36770	-1189	-3,1	37959	1036446	51,1	1,8	2327593	75806371	51,6
19		Ставропольский край	35256	1907	5,7	33349	1071702	52,8	1,7	2798020	78604391	53,6
20		Приморский край	31355	-601	-1,9	31956	1103057	54,3	1,5	1900435		
21		Воронежская область	30224	18	0,1	30206	1133281	55,8	1,5	2326616		
22		Саратовская область	29990	1669	5,9	28321	1163271	57,3	1,5	2434508		

Рис. 3. Лист СУБД – ранжирование субъектов Российской Федерации по абсолютным показателям (по абсолютным значениям и по абсолютному или относительному приросту).

Есть возможность ранжировать субъекты Российской Федерации по коэффициентам преступности (рис. 4).

Система автоматически рассчитывает средний уровень (2 035,6; ячейка M1) преступлений на 100 тыс. населения в субъектах Российской Федерации, где проживает 10 % населения страны и у них самые высокие коэффициенты преступности. И средний уровень (702,1; ячейка M2) в регионах, где проживает 10 % населения страны и у них самые низкие коэффициенты преступности. Их соотношение – Децильный коэффициент 2,9 (ячейка M3) соответствует нормальному распределению.



Уровень преступности

Ранжирование абсолютных значений | Ранжирование коэффициентов по ФО

среднее 10% (максимум) 2 035,60
среднее 10% (минимум) 702,12
децильный коэффициент 2,9

всего

Ранжирование по: абсолютному значению

МЕНЮ

Зарегистрировано | апрель | 2020

Стандартное отклонение - 370,3 (366,3 в 2019).
Коэффициент вариации - 27,4% (27,5% в 2019).
Коэффициент детерминации - 49,8% (55,4% в 2019).

				Уровень преступности	абсолютный прирост	классификация	Уровень преступности	классификация				все население	население (нарастающим итогом)	удельный вес населения (нарастающим итогом)
				апрель 2019			апрель 2020							
56	29		Краснодарский край	1271,58	47,48	3	1224,09	3				5657311		3,85
			Российская Федерация	1382,98	13,5		1369,50		14677001	1	2035,6	146770010	146770010	100
	1		Республика Тыва	2548,79	-210,8	6	2759,6	6	325410	0,02	57	325410	325410	0,2
	2		Амурская область	2437,81	154,1	5	2283,7	5	792144	0,05	132	792144	1117554	0,8
	3		Еврейская автономная область	2347,26	137,3	5	2210,0	5	159377	0,01	25	159377	1276931	0,9
	4		Республика Бурятия	2197,20	-121,8	5	2319,0	5	984161	0,07	147	984161	2261092	1,5
	5		Забайкальский край	2175,22	-91,5	5	2266,7	5	1063757	0,07	158	1063757	3324848	2,3
	6		Республика Карелия	2093,31	152,1	5	1941,2	4	616725	0,04	88	616725	3941574	2,7
	7		Курганская область	2048,33	-35,3	4	2083,7	5	832189	0,06	116	832189	4773763	3,3
	8		Республика Коми	2033,42	-53,0	4	2086,4	5	826981	0,06	115	826981	5600744	3,8
	9		Магаданская область	1979,81	-104,2	4	2084,0	5	140872	0,01	19	140872	5741616	3,9
	10		Кемеровская область	1978,09	-20,5	4	1998,6	4	2668789	0,18	360	2668789	8410405	5,7
	11		Республика Алтай	1973,06	-135,7	4	2108,7	5	219304	0,01	29	219304	8629709	5,9
	12		Республика Хакасия	1953,20	-106,5	4	2059,7	4	535532	0,04	71	535532	9165241	6,2
	13		Челябинская область	1932,26	59,6	4	1872,6	4	3472625	0,24	457	3472625	12637866	8,6
	14		Новгородская область	1905,40	117,9	4	1787,5	4	599033	0,04	78	599033	13236900	9,0
	15		Сахалинская область	1891,34	-134,6	4	2025,9	4	489178	0,03	63	489178	13726077	9,4
	16		Иркутская область	1866,74	-68,4	4	1935,1	4	950924	0,06	121	2395573	16121650	11,0
	17		Республика Удмуртия	1861,23	160,9	4	1700,4	4				1505245	17626895	12,0

Рис. 4. Лист СУБД – ранжирование субъектов Российской Федерации по коэффициентам преступности (по абсолютным значениям или по абсолютному приросту).

В Российской Федерации 1 383,0 (ячейка D3) преступлений на 100 тыс. населения. В ячейке С6 (рис. 4) приведены основные статистические характеристики совокупности субъектов Российской Федерации по уровню всей преступности по состоянию на 1 мая 2021 г.: стандартное отклонение (370,3), коэффициент вариации (27,4 %) и коэффициент детерминации (49,8 %). Последний – результат дисперсионного анализа, который выявил, что разнообразие субъектов Российской Федерации по уровню преступности почти на 50 % обусловлено их социально-географическим различием.

На этом листе СУБД также приводится типология субъектов Российской Федерации по уровню преступности (столбцы F и H). Группа 6 – это регионы, которые по правилу трех сигм нарушают статистическую однородность всей совокупности субъектов Российской Федерации. Они вне типологии. Группа 5 –высокие значения показателя. Группа 4 – значения показателя выше среднего. Группа 3 – средние значения показателя. Группа 2 – значения показателя ниже среднего. Группа 1 – низкие значения показателя.

Следует отметить, что по заказу потребителя достаточно легко добавить в систему еще один лист с необходимой для него любой информации, которую можно получить из БД, и в удобной форме.

Для разработки подобных АИС в штате криминологов достаточно иметь одного с математическим образованием, а также на курсах информатики обучать их созданию. Трудности – регулярное получение соответствующих статистических форм из ГИАЦ МВД России.

Одной из основных проблем ведения таких АИС – ввод первичной информации. Регулярно получая данные из ГИАЦ МВД России, в БД можно создать автоматизированный перевод данных из базы любой формы ГИАЦ. Однако, эти формы очень часто реформируются и после них необходимо перерабатывать БД АИС «Анализ и прогноз преступности».

В перспективе документооборот во всех сферах, в том числе и в МВД России будет переходить на цифровой формат. Надо отметить, что в медицине это уже широко используется. Создается Единая Медицинская Информационная Система (ЕМИАС). Эта система позволит любому врачу в режиме онлайн изучить электронную медицинскую карту пациента. В настоящее время следует и в правоохранительных органах начать разработку аналога такой системы. Кроме того, надо уже сейчас предусмотреть возможность перехода от ручного заполнения карточек первичного учета к методам программной обработки цифрового массива документов – это повысит достоверность и надежность учета, исключит субъективные ошибки и, главное, возможность получения информации в режиме онлайн. Отпадет необходимость составлять и реформировать формы государственной статистической отчетности – каждый пользователь такой системы самостоятельно лично под свои ведомственные интересы будет разрабатывать необходимые ему формы.

Литература

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2019 года и тенденции ее развития: Аналитический обзор / М.В. Гончарова, М.М. Бабаев, С.А. Невский и др. М.: ФГКУ «ВНИИ МВД России», 2020, – 94 с.

2. Преступность и правонарушения (2010-2015): Статистический сборник. М.: ФКУ «ГИАЦ МВД России», 2015, – 180 с.

3. Состояние законности и правопорядка в Российской Федерации и работа органов прокуратуры 2018 год: Информационно-аналитическая записка. М.: ФГКУ «Университет прокуратуры Российской Федерации», 2018, – 145 с.

4. Криминология: Учебник для вузов / Под общ. ред. д.ю.н., проф. А.И. Долговой. – 3-е изд., перераб. и доп. – М.: Норма, 2005. - 912 с.

5. Лунеев В.В. Юридическая статистика: Учебник для вузов – 3-е изд., перераб. и доп., с изм. – М.: Юристъ, 2013. - 448 с.

6. Форма статистической отчетности ГИАЦ МВД России № 451 Состояние преступности в России за январь-декабрь 2020 года: Статистический сборник. М.: ФКУ «ГИАЦ МВД России», 2021. - 55 с.

Сведения об авторах

Коимшиди Георгий Феофилактович, кандидат технических наук, доцент, ведущий научный сотрудник Федерального государственного казенного учреждения «Всероссийский научно-исследовательский институт МВД России», e-mail: koim@mail.ru.

Саркисян Армен Жораевич, кандидат юридических наук, доцент, руководитель редакционно-издательского отдела Московской академии Следственного комитета Российской Федерации, доцент кафедры «Уголовное право, уголовный процесс и криминалистика» Российского университета транспорта; e-mail: 7700153@gmail.com.

Кропачев Сергей Юрьевич
Крыгин Сергей Владимирович

Использование Windows 10 Timeline при расследовании компьютерных инцидентов

Аннотация: Статья посвящена рассмотрению возможностей, предоставляемых Windows 10 Timeline при выявлении, раскрытии и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Авторы анализируют особенности применения для получения криминалистически значимой информации при расследовании компьютерных инцидентов. Отдельно рассматриваются вопросы применяемого программного обеспечения для оптимизации работы с данной утилитой.

Ключевые слова: информационная безопасность, компьютерный инцидент, криминалистический анализ, кибербезопасность, кибератака.

В настоящее время мы являемся очевидцами того, как стремительно развиваются информационные технологии, захватывая новые сферы жизни и деятельности общества. Не стала исключением и экономика, в которой информационно-телекоммуникационные технологии сформировали современные управленческие системы во всех отраслях, использующих передовые знания для устойчивого развития и получения преимущества на рынках.

Прорывное развитие технологий цифрового мира повлекло за собой то, что преступное сообщество с энтузиазмом начало использовать их в своих целях, тем более что некоторые возможности оказались весьма привлекательны для злоумышленников, например, анонимизация криптовалют. Даная технология хорошо освоена и широко используется в криминальной деятельности, связанной с незаконным оборотом наркотических веществ или отмывании доходов, полученных преступным путем.

Периодически в новостях, распространяемых средствами массовой информации, появляются сообщения о взломах киберпреступниками информационных систем крупных компаний и корпораций и получении несанкционированного доступа к базам данных пользователей, в том числе и к персональным данным клиентов этих организаций.

На фоне массового перехода значительного количества компаний на удаленный формат работы, количество компьютерных инцидентов увеличилось практически вдвое по сравнению с предыдущими периодами, при этом порядка 86% атак были направле-

ны на организации. Количество атак с применением вредоносного программного обеспечения увеличилось в два раза, при этом постоянно совершенствуются способы сокрытия нелегального проникновения и воздействия на объекты атаки. На первом месте по частоте применения оказались вирусы-шифровальщики, их доля составила 45% от общего количества выявленного вредоносного программного обеспечения. Зафиксированы кибератаки на объекты критически значимой инфраструктуры, такие как электростанции, системы водоснабжения, и даже медицинские учреждения подвергались атакам киберпреступников [1].

Все указывает на то, что необходимо тщательным образом обратить внимание на изучение технологий формирования цифровых следов, чтобы разработать методы их контроля, выявления следов преступной деятельности и использования полученных результатов в следственной практике при расследовании уголовных дел.

Под инцидентом информационной безопасности (information security incident) мы будем понимать появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности [2].

В дальнейшем, инцидент уже может перерасти в преступление, совершенное с использованием информационно-телекоммуникационных технологий, при наличии всех обстоятельств, необходимых для правильной квалификации деяния. К ключевым обстоятельствам можно отнести:

- время и место совершения, особенно фиксация момента подключения/отключения зафиксированное в системных журналах;
- наличие цифровых следов пребывания в операционной системе, оставленных злоумышленником, используемые им учетные записи и его действия.

Для получения такой информации специалисты-эксперты используют различные программные инструменты от разных производителей, но мы остановимся на таком инструменте, как Windows 10 Timeline, представляющем собой встроенную в Windows 10 утилиту, восстанавливающую хронологию событий с учетом специфики работы операционной системы Windows.

При расследовании компьютерного инцидента применяется такой вид анализа, как создание временной шкалы, представляющей собой файл или таблицу с информацией о событиях, расположенных в хронологическом порядке.

Всего можно выделить две основных способа создания временной шкалы:

1. Timeline - основывается на анализе временных изменений метаданных файлов в файловой системе, то есть анализ опирается на файловую систему хранилища данных.

2. Super Timeline – помимо изменений временных метаданных файлов также анализирует изменения, связанные с артефактами в операционной системе.

Чаще всего для временного анализа используются программные средства сторонних разработчиков, отличающиеся по предоставляемому функционалу и ограничениям, так, например, процесс снятия образа жесткого диска с последующим сбором и анализом информации (парсингом) бесплатной программой Autopsy может затянуться на несколько суток. Естественно, что ни о каком оперативном реагировании не может быть и речи, тогда как в случае кибератаки важна скорость своевременной реакции по ее отражению и фиксированию информации о действиях злоумышленника до ее возможного удаления.

Соответственно, в условиях необходимости оперативного реагирования, предполагая сохранение на данный момент неизменности анализируемой среды для дальнейшего использования, например в качестве доказательства в судебном процессе, рассмотрим возможности, предоставляемые Windows Timeline 10 для просмотра истории событий на компьютере, подвергшемся кибератаке.

Windows 10 Timeline впервые была введена в обновлении Windows 10 (1803) и позволяет посмотреть последнюю линейную активность пользователя, то есть открытые документы, запущенные программы, просмотренные видео и изображения, в течение тридцати суток, не требуя прав администратора.

Открыть просмотр недавних событий в Windows 10 Timeline можно нажав сочетание клавиш Win + Tab, или значок на панели задач рабочего стола, рядом со значком поиска (рис.1).

Рис.1.

На появившемся экране будут доступны миниатюры программ или документов, которые были открыты недавно, а справа доступна временная шкала для их просмотра в хронологической последовательности (рис.2).

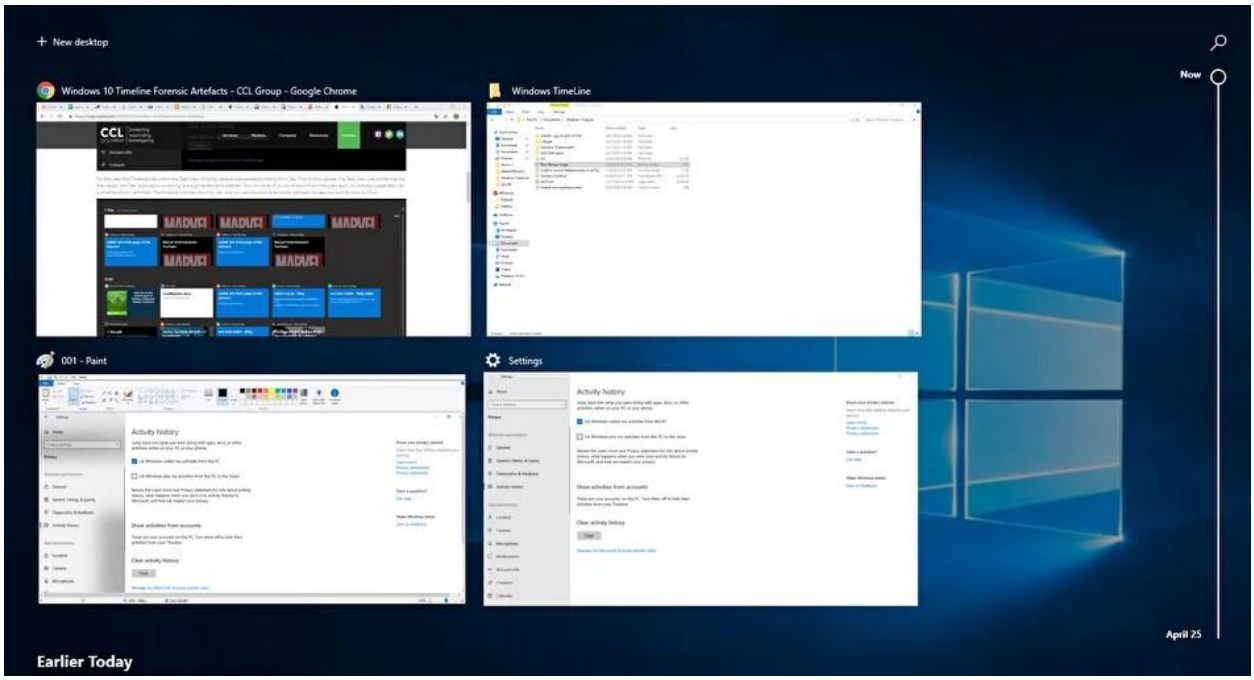


Рис.2.

Необходимо учитывать такой немаловажный фактор, что не все недавно открытые приложения будут отображаться на временной шкале, но при включенной по умолчанию настройке синхронизации с Microsoft некоторые данные, сохраненные в Microsoft Cloud, доступны более 30 суток.

Если в истории недавних действий не находятся искомые данные, то их можно посмотреть в журнале активности действий «ActivitiesCache.db», который размещается по адресу: C:\Users\profilename\AppData\Local\ConnectedDevicesPlatform\L.profile name\

Данный журнал представляет собой SQL - базу, в которой есть следующие таблицы «Activity», «ActivityOperation», «Activity_PackageId», «AppSettings», «DataEncryptionKeys», «ManualSequence», «Metadata».

Просмотр информации, хранящейся в данной SQL – базе можно осуществить с помощью бесплатного инструмента DB Browser for SQLite, который и применялся для исследования в рамках данной статьи или использовать специализированные криминалистические утилиты.

Для достижения целей криминалистического анализа наибольший интерес представляют таблицы «Activity» и «Activity_PackageId».

В таблице «Activity» находятся несколько временных меток по каждому событию (рис.3):

- «StartTime» и «ENDTime» показывают время начала запуска и завершения использования приложения, соответственно;
- «ExpirationTime» указывает время до которого информация о событии будет хранится в журнале;
- «LastModifiedTime» показывает момент последнего изменения записи о действиях пользователя;
- «LastModifiedOnClient» заполнется только тогда, когда пользователь сам изменил файл.

Необходимо учитывать тот факт, что время может быть отображено в формате EpochTime, например такое значение 1622926773, будет соответствовать следующему значению в формате Unix - Saturday, June 5, 2021 11:59:33 PM GMT+03:00.

Activity		CREATE TABLE [Activity]([Id] GUID PRIMAR
Id	GUID	"Id" GUID NOT NULL
AppId	TEXT	"AppId" TEXT NOT NULL
PackageIdHash	TEXT	"PackageIdHash" TEXT
AppActivityId	TEXT	"AppActivityId" TEXT
ActivityType	INT	"ActivityType" INT NOT NULL
ActivityStatus	INT	"ActivityStatus" INT NOT NULL
ParentActivityId	GUID	"ParentActivityId" GUID
Tag	TEXT	"Tag" TEXT
Group	TEXT	"Group" TEXT
MatchId	TEXT	"MatchId" TEXT
LastModifiedTime	DATETIME	"LastModifiedTime" DATETIME NOT NULL
ExpirationTime	DATETIME	"ExpirationTime" DATETIME
Payload	BLOB	"Payload" BLOB
Priority	INT	"Priority" INT
IsLocalOnly	INT	"IsLocalOnly" INT
PlatformDeviceId	TEXT	"PlatformDeviceId" TEXT
DdsDeviceId	TEXT	"DdsDeviceId" TEXT
CreatedInCloud	DATETIME	"CreatedInCloud" DATETIME
StartTime	DATETIME	"StartTime" DATETIME
EndTime	DATETIME	"EndTime" DATETIME
LastModifiedOnClient	DATETIME	"LastModifiedOnClient" DATETIME
GroupAppActivityId	TEXT	"GroupAppActivityId" TEXT

Рис.3.

Таблица «Activity_PackageId» хранит записи о запускаемых приложениях, указывает путь к исполняемым файлам, показывает, когда и каким пользователем запускались, а также срок до которого будут храниться эти записи.

1560	BLOB	[{"application":"F:\\Софт\\Драйвера\\Принтер\\LBP3010_3018_3050_R150_V110_W64_uk_EN_1\\...	pH4VElQCk/...	ECB32AF3-1440-4086-94E3-53...	6
1561	BLOB	[{"application":"C:\\Users\\ \\AppData\\Local\\Temp_tc\\steghide\\steghide.exe","platform":"x_exe_path"},...	pJsvxH3gLPVDOswX24/...	ECB32AF3-1440-4086-94E3-53...	5
1562	BLOB	[{"application":"D:\\Office\\deploy.exe","platform":"x_exe_path"},{"application":"D:\\Office\\...	qg7vb09AcgD/...	ECB32AF3-1440-4086-94E3-53...	5

Помимо журнала активности «ActivitiesCache.db», в этом же каталоге, где он и располагается, могут находиться файлы с расширением .cdp, котрые содержат информацию о моменте последней синхронизации с Microsoft Cloud и id пользователя (рис.4).

Как и любая другая база данных SQLite, она характеризуется следующими двумя вспомогательными файлами: 'ActivitiesCache.db-shm' и 'ActivitiesCache.db-wal', которые тоже могут представлять интерес для поиска информации

Часто встречаются случаи, когда злоумышленник целенаправленно удаляет записи о своей активности в системе, таким образом затирая цифровые следы. В этом случае тоже можно получить дополнительную информацию об удаленных записях посред-

ством анализа свободного пространства базы данных, свободных блоков (списков) и WAL-файла, но это уже потребует более серьезного криминалистического анализа.

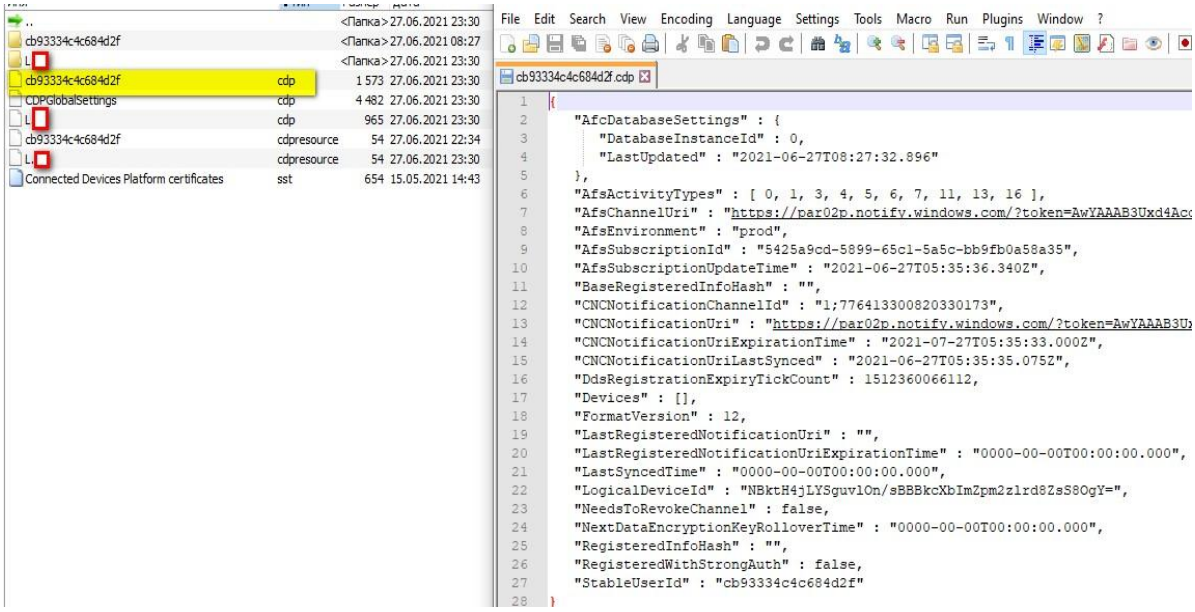


Рис.4

Несомненно, что временной анализ активности Windows 10 Timeline отличается от классических вариантов временного анализа, но также очевидно, что проигрывает по возможностям программам судебной экспертизы, например такой как Belkasoft Evidence Center.

Таким образом, используя Windows 10 Timeline, мы можем получить необходимую информацию, провести первичный анализ активности на компьютере, подвергшемся воздействию, что позволяет оперативно реагировать на действия злоумышленника, чтобы не дать ему возможности удалить свои цифровые следы, зафиксировав информацию, которая позволит более успешно провести дальнейшее расследование. Windows 10 Timeline, значительно облегчает операции по восстановлению хронологии событий, а также предоставляет дополнительную информацию о файлах, запущенных на данном компьютере, в том числе удаленных.

Литература

1. Актуальные киберугрозы: итоги 2020 года. Positive Technologies [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/#id1 (дата обращения – 10.06.2021).

2. ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Электронный фонд правовых и нормативно-технических документов. [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200068822 (дата обращения – 11.06.2021).

3. Расследование инцидентов информационной безопасности : учебное пособие / И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с.

4. Технологии расследования компьютерных инцидентов. Бутин А.А. Академический журнал ACADEMY № (11)38 2018 / Режим доступа: https://elibrary.ru/item.asp?id=36476091 (дата обращения – 10.06.2021

Сведения об авторах

Кропачев Сергей Юрьевич, преподаватель кафедры математики, информатики и информационных технологий Нижегородской академии МВД России.

Крыгин Сергей Владимирович, заместитель начальника кафедры математики, информатики и информационных технологий Нижегородской академии МВД России, кандидат юридических наук, доцент.

Лаптев Владимир Николаевич

МЕСТО И РОЛЬ ИНФОРМАЦИИ В ОБЕСПЕЧЕНИИ УСПЕШНОГО ФУНКЦИОНИРОВАНИЯ И РАЗВИТИЯ ОТКРЫТЫХ СИСТЕМ

Для гибкого приспособления деятельности открытой системы (ОС) к изменениям внешней среды (оперативной обстановке) необходимо создание адаптивной матрицы типовых знаний (МТЗ) /см. предыдущую статью/. Все входящие в нее строки $Y_m(x_n)$ способны при $Y_k(x_n)=Y_m(x_n)$ автоматически работать в типичных ситуациях, а при $Y_k(x_n)\neq Y_m(x_n)$ – адаптироваться к изменениям внешней среды (С).

Входящие в нее числовые величины представлены в универсальном безразмерном виде (в долях единицы) для их корректного математического сравнения и использования.

Как правило, $M=N$, а N – общее количество равных частей $\Delta x_n=1/2N$ отрезка [0,1], получаемых методом дихотомии. $Y_k(x_n)$ и $Y_m(x_n)$ – однотипные безразмерные значения текущей k и типовых m дискретных функций $Y_m(x_n)$ МТЗ, пригодных для однозначной идентификации $Y_k(x_n)$.

В формуле (1) слева показана непрерывная функция многих переменных $Y(x_1,x_2, \dots , x_N)$, а справа – набор *двумерных* единичных квадратов 1×1, в которых дробление отрезков [0, 1] осуществляется методом дихотомии (строгим делением пополам каждого последующего отрезка в этом интервале).

$$Y(x_1, x_2, \dots, x_N) = \sum_{n=1}^{2N+1}\left(g_n \sum_{m=1}^{N}\left(h_{mn}(x_m)\right)\right) = \sum_{n=1}^{2N+1}\left(\log_2 \sum_{m=1}^{N}\left(h_{mn}(x_m)\right)\right). \quad (1)$$

где $x = (x_1, \dots, x_N)$, $0 \le x_n \le 1$.

Монотонные дискретные отображения столбцов $h_{mn}(x_n)$, имеющих одинаковое основание $\Delta x_n=(x_{n+1}-x_n)/N$, не зависят от конкретной функции $Y(x_1,x_2, \dots , x_N)$. Эта означает, что для реализации функций многих переменных вполне достаточно операций суммирования и композиций универсальной функции одной переменной

В ее состав входят все n дискретных параметров сигнала внешнего воздействия $Y_{km}(x_{km})$, которые уравновешиваются n дискретными параметрами сигнала противодействия $Y_{mn}(x_{mn})$ со стороны ОС.

Дискретные параметры – это конкретные числовые значения характеристик x_{km}, измеряемых датчиками ОС (у нас ОВД) по каждому интегрированному сигналу $Y_m(x_n)$ ($Y_k(x_n)$).

В мозгу человека все значения $h_{mn}(x_{mn})\Delta x_{mn}$ и $h_{mn}(x_{mn})\Delta x_{mn}$ в $Y_m(x_n)$ и $Y_k(x_n)$ строго упорядочены и разделяются на:

1) внешние, поступающие извне;

2) внутренние, отражающие состояния ОС и снабжение его ФЭ ресурсами (для поддержания гомеостата и должного поведения);

3) целевые (сигналы управления, обеспечивающие достижение желаемого $+Кр_m$), изменяющие характер взаимосодействия $ОС_m \leftrightarrow С_k$ от $Y_m(x_n) \neq Y_k(x_n)$ до $Y_m(x_n) = Y_k(x_n)$.

Элементами МТЗ размера МТЗ $N\times N$ являются N уникальных строк $Y_m(x_n)$:

$$Y_m(x_n) = \sum_{n=1}^{N} |h_{mn}(x_n \Delta x_n)| \quad (2)$$

При выполнении условия (3)

$$|Y_k(x_n) - Y_m(x_n)| \le \varepsilon \text{ и } |\Delta x_n| = n|x_{n+1}-x_n|/N \le \delta., \quad (3)$$

где ε и δ – допустимые на практике погрешности совпадения значений стоп-кадра взаимодействия открытой системой $ОС_m \leftrightarrow С_k$ и Δx_n.

При выполнении условия (3), считается, что текущий стоп-кадр $Y_k(x_n)$, отражает совпадение этого текущего интегрального внешнего воздействия окружающей среды (извне), с интегральным противодействием ему $Y_m(x_n)$, со стороны ОС. В этом случае ОС автоматически запускает механизм синхронной (параллельной) работы q функциональных элементов ($ФЭ_q$), уравновешивающих текущее интегральное воздействие извне $Y_k(x_n)=Y_m(x_n)$ и осуществляется достижения позитивного конечного результата $+Кр_m$, – выживание ОС. В случае, когда $Y_k(x_n)\neq Y_m(x_n)$ выживание ОС остается под вопросом, ибо в этом случае она может и не выжить, то есть погибнуть.

Сумма площадей $|h_{mn}(x_n)\Delta x_n|$ для каждой функции $Y_{mn}(x_n)$ – это уникальные интегральные значения, однозначно идентифицирующие m-й стоп-кадр. Условия (3) позволяют четко различать стоп-кадры $Y_m(x_n)$ и $Y_k(x_n)$ как математические модели, имеющие разные уникальные интегральные числовые (значения) – качества.

Именно такая достоверная информация позволяет человеку (живой ОС), как обученному автомату, однозначно идентифицировать или не идентифицировать типовой для него текущий стоп-кадр $Y_m(x_n)$ при выполнении условия $Y_m(x_n)\approx Y_k(x_n)$ (с допустимыми при этом погрешностями ε и δ). В случае такой идентификации взаимодействия, на базе резонанса и дискретного преобразования Фурье (ДПФ), МАУ ОС (ее сотрудников) автоматически вычисляет спектр собственных круговых частот ω_{m0}, ω_{m1}, …, ω_{mq} $ФЭ_{mq}$ и запускает m-й поведенческий акт ($ПА_m$), т. е. синхронную совместную работу q его ФЭ (исполнительных органов), обеспечивающую выживание ОС. МТЗ, базирующаяся на таком информационно-когнитивном МАУ ОС, пополняется новыми типовыми знаниями $З_m$, необходимыми для успешного выживания ОВД в динамически изменяющейся оперативной обстановке С.

Правильное понимание места и роли информации в повседневной деятельности любого сотрудника (ОС) позволяет им реально грамотно использовать свои знания, умения и навыки (ЗУНы), как в личной жизни, так и в своей профессиональной деятельности. Только такой подход позволил человечеству обеспечить свое успешное выживание и развитие в изменяющемся мире.

В соответствии с ФЗ «Об информации, информационных технологиях и защите информации» эти термины трактуются как:

а) информация – сведения (сообщения, данные) независимо от формы и представления;

б) информационные технологии – процессы, методы поиска, сбора, хранения, обработки, представления, распределения информации и способы осуществления таких процессов и методик;

в) информационные системы – как совокупность содержащейся в базах данных (БД) информации;

г) информационно-технологические системы – технологические системы передачи данных по линиям связи, информация, доступ к которой осуществляется через ЭВМ.

Защита информации (теперь информационная безопасность) – это принятие правовых, организационных и технологических мероприятий, направленных на:

1) пресечение уничтожения, модернизации уникальной информации, ее блокировки, копирования, распространения, несанкционированного доступа, а также от иных неправомерных действий;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализация прав на доступ к информации.

И.С. Ожегов определяет сущность информации как – «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством; сообщения, осведомляющие о положении дел, о состоянии чего-нибудь».

Однако такое определение сущности информации не представлена ее главная характеристика. А именно качественное отражение ОС конкретного стоп-кадра ее взаимодействия с изменяющейся внешней средой $ОС_m \leftrightarrow С_k$, в котором обе его части могут совпадать или не совпадать (с допустимой при этом погрешностью ε). уникального (неповторимого) свойства любого конкретного объекта, позволяющее четко однозначно отличать качественно разные ОС.

Здесь необходимо отметить, что большинство людей не понимают, что только цифровое представление моделей $Y_m(x_n)$ и $Y_k(x_n)$ обеспечивает их единообразное и корректное сличение за счет того, что любое цифровое представление чисел в двоичной системе исчисления обладает уникальным свойством – однозначно отражает их качество и является основанием формальной логики. Последняя, с помощь конкретных логических операций, позволяет строить строгие математические модели, обладающие разными качествами и формальными возможностями.

В этой связи под информацией мы понимаем строго упорядоченные цифровые наборы, обладающие уникальными логическими и цифровыми качествами, позволяющие строить с их помощью качественно различные модели формальной логики и цифровые комбинации, обладающие уникальным свойствами.

Комплексное использование творческим человеком информации в рамках схемы знания (типовые модели) – умения (алгоритмы их успешной реализации) – навыки (автоматическая реализация компьютерами этих алгоритмов в РМВ) на практике иллюстрирует следующая схема взаимодействия ОС с изменяющейся природой (рис. 1).

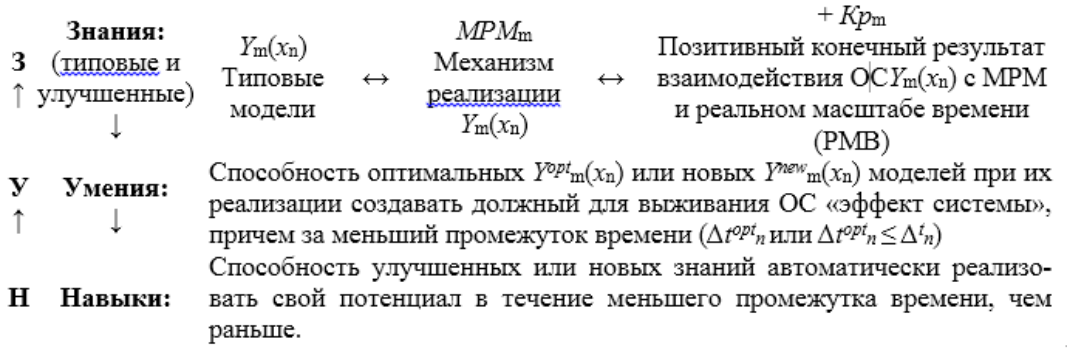


Рис. 1. Взаимосвязи знаний, умений и навыков в творческой деятельности человека.

В этой схеме знания представляют собой гармоничное взаимодействие типовых моделей $Y_m(x_n)$ с адекватными им механизмами их реализации. При этом взаимодействии обеспечивается сбалансированность воздействия извне противодействием («эффектом системы») со стороны ОС. Умения – это потенциальная способность ОС реализовывать типовые $Y_m(x_n)$, оптимальные $Y^{opt}{}_m(x_n)$ и новые $Y^{new}{}_m(x_n)$ модели, позволяющие ей при грамотном использовании «эффекта системы» успешно выживать в изменяющемся мире. Навыки – это умения, доведенные до автоматизма на базе уточненной $МТЗ^{opt}$ или новой, кардинально улучшенной $МТЗ^{new}$ (с новыми типовыми моделями $Y^{opt}{}_m(x_n)$ и $Y^{new}{}_M(x_N)$).

Из положений конкретной математики и практики применения компьютерных программ при реализации указанных выше математических моделей четко прослеживается необходимость правильного повсеместного использования отдельными сотрудниками и коллективами триады

знания – умения – навыки

в науке, обучении и деятельности ОВД, однозначно трактуемом как ЗУНы.

Блок знания – эта область использования искусственного интеллекта (ИИ) как комплекса технологических решений, удачно имитирующих познавательные и прикладные (исполнительные) функции человека (включая самообучение и поиск решений без заранее заданного алгоритма), позволяющего ему, при решении проблем и задач оптимизации, получать результаты, сопоставимые с результатами совместной интеллектуальной и исполнительной (совместной) человеческой деятельности, доведенной до автоматизма, требуемого для его выживания в конкретном типовом текущем стоп-кадре его взаимодействия с изменяющейся внешней средой.

Блок умения включает в себя угаданную сотрудником (коллективом) информационно-коммуникационную связь (структуру) взаимосодействия ОС (ОВД) с внешней средой (С), четко описанного для нового конкретного стоп-кадрового взаимодействия $ОС_m \leftrightarrow С_k$ на языке математической (то есть формальной) логики. Это позволяет человеку (коллективу творческих людей), успешно четко формализовать процесс выполнения конкретных индивидуальных и совместных коллективных действий сотрудников ОВД, а затем (с помощью программирования) эффективно автоматизировать эти формализованные действия, процессы и сервисы обработки данных, автономного поиска новых решений.

Блок навыки позволяет убедиться в способности сотрудника или ОВД в целом находить оптимальные и принципиально новые пути решения задач и проблем, связанных с их успешной адаптацией к изменениям внешней среды (оперативной обстановки), причем в реальном масштабе времени. Комплексное автоматическое использование таких ЗУН-ов как отдельным сотрудником, так и коллективом ОВД. Их постоянное развитие приводит к успешной адаптации деятельности отдельных сотрудников и коллектива ОВД в целом, к постоянно изменяющейся текущей оперативной обстановке в автоматическом режиме.

Такое непрерывное развитие ЗУН-ов сотрудников ОВД способствует реальному переводу революционных идей, моделей, технологий в разряд типовых, но уже с качественно новыми возможностями. Человек, как самая совершенная ОС, обладающая ЕИ и ИИ, с помощью компьютерных сетей весьма эффективно автоматизирует решение типовых задач и проблем. Он открывает для себя новые возможности, совершенствуя ЗУН. Только гармоничное взаимосодействие естественного и искусственного интеллектов способно обеспечить устойчивое выживание ОС (в том числе и ОВД) в изменяющейся внешней социально-экономической среде.

Литература

1. Аршинов Г.А. Анализ оборота капитала и цены на готовую продукцию в интегрированных объединениях АПК / Г.А. Аршинов, С.В. Лаптев, В.Г. Аршинов // Новые технологии. – 2018. – № 4. – С. 96–101.

2. Аршинов Г.А Анализ современных форм интеграции сельскохозяйственных товаропроизводителей и перерабатывающих предприятий АПК / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2016. – № 123. – С. 1392–1421.

3. Аршинов Г.А. Анализ условий образования эффективных объединений предприятий молочного подкомплекса АПК /, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2017. – № 132. – С. 128–155.

4. Аршинов В.Г. Математическое моделирование интеграционных процессов в АПК / В.Г. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: сб. статей II Всероссийской научно-практической конференции. – 2006. – С. 5–6.

5. Аршинов Г.А. Математическое моделирование экономической деятельности перерабатывающих предприятий / Г. А. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: материалы IX Всероссийской научно-практической конференции; отв. ред. С.А. Вызулин, Е.В. Михайленко, Ю.Н. Сопильняк. – Краснодар: КубГАУ, 2013. – С. 24–27.

6. Аршинов Г.А. Математическое моделирование отношений партнеров в современных формах интеграции сельскохозяйственных товаропроизводителей и перерабатывающих предприятий / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2017. № 130. – С.1137–1159.

7. Аршинов Г.А. Математическое моделирование экономической деятельности перерабатывающих предприятий / Г.А. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: материалы IX Всероссийской научно-практической конференции; отв. ред. С.А. Вызулин, Е.В. Михайленко, Ю.Н. Сопильняк. – Краснодар: КубГАУ, 2013. – С. 24–27.

8. Аршинов Г.А. Совершенствование акустических методов диагностики скрытых микродефектов и эксплуатационная надежность вязкоупругих элементов конструкций / Г.А. Аршинов, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. № 154. – С. 84–93.

9. Аршинов Г.А. Оценка экономической и эксплуатационной надежности строительных сооружений на основе исследования волновых характеристик нелинейных вязкоупругих стержневых элементов конструкций / Г. А. Аршинов, С. В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. – № 153. – С. 113–122.

10. Аршинов Г.А. Причины, препятствующие созданию эффективных объединений предприятий молочного подкомплекса АПК / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2016. № 123. – С. 1422–1443.

11. Аршинов Г.А. Стратегия и тактика использования МАУ ОС в деятельности АПК / Г.А. Аршинов, В.И. Лойко, С. В. Лаптев // Трансформация социально-экономического пространства России и мира: сб. статей Международной научно-практической конференции / под ред. Г.Б. Клейнера, Х.А. Константиниди, В.В. Сорокожердьева, З.М. Хашевой. – 2020. – С.131–135.

12. Аршинов Г.А. Уточнение акустических методов регистрации мик-родефектов материала на основе исследования нелинейных волн дефор-маций в вязкоупругих стержнях / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2020. № 162. – С.37–53.

13. Аршинов В.Г. Функция скорости спроса и оборот вложенного капитала в интеграционных структурах АПК / В.Г. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: сб. статей II Всероссийской научно-практической конференции. 2006 – С.7–9.

14. Информационная безопасность: учеб. пособие / В.И. Лойко, В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с.

15. Лаптев В.Н. Разработка адаптивной матрицы типовых знаний для инвестиционного управления АПК / В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев, Т.В. Лукьяненко, Е.В. Фешина // Политематический сетевой электронный научный журнал Кубанского

государственного аграрного универ-ситета. – Краснодар: КубГАУ, 2020. – № 164. – С. 36–54.

16. Лаптев С.В. Постановка курса «Web-технологии в идентификации систем» / С.В. Лаптев // Качество современных образовательных услуг – основа конкурентоспособности вуза. Сб. статей по материалам межфакультетской учебно-методической конференции. / Отв. за вып. М.В. Шаталова. – Краснодар: КубГАУ, 2016. – С.298–300.

17. Лаптев С.В. Нелинейные дисперсионные волны в вязкоупругих тонкостенных конструкциях: дисс. канд физ.-мат. наук / С.В. Лаптев. – Саратов: СГУ, 2000. – 132 с.

18. Лаптев С.В. Разработка информационных систем на базе web-технологий: учеб. пособие / С.В. Лаптев, В.Н. Лаптев, Г.А. Аршинов – Краснодар: КубГАУ, 2021. – 175 с.

19. Степанов В.В. Нелинейная математическая модель ценообразования продукции перерабатывающего предприятия / В.В. Степанов, Г.А. Аршинов, С.В. Лаптев, И.А. Мануйлов // Автоматизированные информационные и электроэнергетические системы: материалы II Межвузовской научно-практической конференции. – Краснодар: КубГТУ, 2012. – С.38–40.

Сведения об авторе

Лаптев Владимир Николаевич, кандидат технических наук, доцент, доцент кафедры комьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: lvn4828@yandex.ru.

Лаптев Владимир Николаевич

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИАЛЕКТИКИ ПРИРОДЫ И ИХ МЕСТО В ФУНКЦИОНИРОВАНИИ И РАЗВИТИИ ОВД

С позиций законов диалектики природы [1, 24-25] успешное функционирование и развитие открытых систем (ОС) (в том числе и ОВД) обеспечивает выживание ОС в изменяющейся внешней среде через их адаптацию к этим изменениям, приводящую к уравновешиванию внешних воздействий среды адекватным им ответным противодействием.

Технология гармоничного взаимосодействия ОС с изменяющейся внешней средой (С) определяет место и роль информации в этом процессе [1]. Поиск ОС противодействия, соответствующего внешнему воздействию, приводит либо к применению одного из множества известных, либо к построению неизвестного нового противодействия, позволяющего ОВД добиться желаемого позитивного конечного результата (+Кр) – выживания в процессе адаптации.

Непрерывный процесс внешнего воздействия на ОС (у нас ОВД) можно представить дискретным набором упорядоченных стоп-кадров, среди которых могут быть повторяющиеся, причем ОС действует в типовых стоп-кадрах одинаково, а в нетиповых – по-разному.

Для человека +Кр – это сохранение целостности организма в условиях текущего внешнего стоп-кадра, соответствующего приращению времени Δt_k, за счет уравновешивания векторного воздействия $\boldsymbol{C_k}$ внешней среды адекватным ответным векторным противодействием $\boldsymbol{OC_m}$.

Поэтому в основу выживания человека (у нас ОВД) природа заложила механизм адаптивного управления (МАУ), запускающий выполнение таких одинаковых в типовых и разных в нетиповых стоп-кадрах взаимодействий, $\boldsymbol{OC_m \leftrightarrow C_k}$ при которых выполнялось условие баланса $\boldsymbol{OC_m = C_k}$.

Использование стоп-кадровой модели баланса $\boldsymbol{OC_m = C_k}$ позволяет четко разделять все модели взаимодействия $\boldsymbol{OC_m \leftrightarrow C_k}$ на типичные и нетипичные.

Для выживания ОВД необходимо, чтобы коллективная (синхронная) работа q задействованных ОС ее функциональных (исполнительных) элементов обеспечила создание «эффекта системы» $\boldsymbol{OC_m}$, при котором выполняется условие $\boldsymbol{OC_m=C_k}$. Это достигается за счет правильного модельного отражения в мозгу человека реального стоп-кадрового процесса $\boldsymbol{OC_m \leftrightarrow C_k}$ и создания ОВД адекватного противодействия $\boldsymbol{C_m}$, при котором $\boldsymbol{OC_m=C_k}$.

С этих позиций окружающий мир – это единство двух противоположностей: **пустоты** (вакуум) и твердых **частиц** (неделимых на части свободных элементов) отдельных или их «сгустков» (открытых систем), взаимодействующих между собой и с окружающей их внешней средой через пустоту (вакуум). Открытыми системами можно в этом случае считать человека, семью, трудовой коллектив, страну.

Таким образом, ОС – это конечное множество функциональных элементов (ФЭ), связанных между собой и способных в разных ситуациях контакта с внешней средой, обмениваясь с ней веществом, энергией и сигналами, способна адаптироваться к ее изменениям.

Необходимо описать МАУ произвольной ОС, способный изменять ее состояния так, чтобы действующие векторные импульсы внешней среды $\boldsymbol{C_k}$ с допустимой погрешностью $\boldsymbol{\varepsilon}$ компенсировались адекватными интегральными ответными импульсами $\boldsymbol{C_m}$ со стороны ОС.

Такой МАУ успешно реализуется природой в человеке, причем в типичных для человека-творца ситуациях работает автоматически (максимально реализуя возможности искусственного интеллекта – ИИ), а в неординарных ситуациях – творчески путем поиска и реализации человеком (с помощью его естественного интеллекта) новых способов поэтапной автоматизации управления ОС на базе совершенствования взаимосодей-ствия искусственного (формализованного) и естественного (творческого) начала.

Решение проблемы адаптации ОВД к внешним воздействиям состоит в разработке механизма адаптивного управления (МАУ) ОВД, способного автоматически запускать известные действия ОВД в типичных ситуациях и оказании помощи в поиске необходимых неизвестных ответных реакций (по аналогии с присущими человеку творческими способностями), определяющих выживание ОВД в нетипичных ситуациях [20].

В этом случае необходимо применение современных математических методов. Слово «математика» означает «точные знания». Математическое описание явлений и объектов основывается на диалектике непрерывного и дискретного и отображается в виде различных «жестких» (неизменных) и «мягких» (поддающихся изменениям) математических моделей.

Главными законами природы сегодня считаются [1, 2-14, 27-29]:

– закон пространственно-временного континуума развития материи (стоп-кадрового взаимодействия $\boldsymbol{OC}_{\mathrm{m}} \leftrightarrow \boldsymbol{C}_{\mathrm{k}}$) и

– законы диалектики природы (трактуемые Гегелем как законы мышления):

1) взаимного проникновения противоположностей (точнее их сбалансированного взаимосодействия);

2) перехода количества в качество и обратно (в каждом стоп-кадре);

3) отрицания-отрицания (кардинального уточнения взаимосодейст-вия противоположностей при невыполнении требований первых двух законов).

Из первого закона диалектики вытекает последовательное квантование или стоп-кадровое сбалансированное взаимосодействия противоположностей (природы и человека), из второго – четкое различие стоп-кадров разного качества, а из третьего – отсутствие баланса между воздействием извне и противодействием ему со стороны ОС.

Стабильное существование живых существ и искусственных ОС определяется выполнением законов диалектики природы в реальном масштабе времени (РМВ), т. е. в каждом стоп-кадре [1-2, 15-18, 27–29].

Природа, базируясь на принципе первичности материи и вторичности сознания, сформировала в человеческом организме механизм гибкого взаимодействия его разума – естественного интеллекта и тела – исполнительного органа. Первый сформировался как орган моделирования сбалансированного взаимодействия человека с изменяющейся внешней средой, а второй – как орган, гибко уравновешивающий все воздействия извне.

Человек научился различать типичные ($\boldsymbol{OC}_m=\boldsymbol{C}_k$) и не типичные ($\boldsymbol{OC}_m\neq\boldsymbol{C}_k$) ситуации процесса $\boldsymbol{OC}_m\leftrightarrow\boldsymbol{C}_k$. В типичных ситуациях он действует автоматически, а в нетипичных – ищет способы нахождения новых автоматизмов, делающих нетипичные для него ситуации типичными.

Человек осуществляет эти действия по схеме: 1) фиксация нарушений баланса, 2) применение известных или построение новых моделей, устраняющих эти нарушения; 3) выполнение этих совместных действий в реальном масштабе времени (РМВ) [17].

Конечная цель любой ОС – ее выживание в любом текущем стоп-кадре за счет уравновешивания линейного или нелинейного воздействия извне $\boldsymbol{C_k}$ адекватным ему противодействием $\boldsymbol{OC_m}$, в виде позитивного конечного результата (+Кр).

Если это воздействие типичное, т. е. $Y_k(x_n)=Y_m(x_n)$, то автоматически включается «жесткая» модель $Y_m(x_n)$. В случае нетипичного воздействия ОС запускает одну из «мягких» моделей с ожиданием, что ее реализация может реально спасти ОС от гибели [1–8].

До настоящего времени считалось, что автоматизация поведения человека имеет предел – невозможность полной формализации всех практических действий. На самом деле в жизни человека имеет место поэтапная формализация его деятельности. Встречаясь с проблемой, человек всегда ее решал, т. е. обеспечивал свое выживание в изменяющемся мире.

Уникальная способность человека поэтапно формализовать, а затем автоматизировать свои действий за счет разработки конкретных моделей и адекватных технологий их реализации дала ему возможность лучше всех живых существ адаптироваться к изменениям окружающего его мира [17–18].

Однако далеко не всеми осознана необходимость органического единства естественного интеллекта (ЕИ) – творческих способность человека и искусственного интеллекта (ИИ) – с его высочайшими скоростями компьютерных вычислений. Их гармоничное взаимосодействие является самой надежной современной научно-технической базой развития человечества.

Для выявления места и роли информации в успешном функционировании и развитии ОВД (как специфичной ОС) необходимо:

1. Выявить проблему, решение которой обеспечит существенное улучшение управления деятельностью ОВД и описать технологию решения этой проблемы (вопроса не имеющего пока решения).

2. Установить математические модели взаимодействия ОС (у нас ОВД) с постоянно изменяющейся внешней средой (С) в типичных и нетипичных для нее ситуациях.

3. Определить роль информации в математических моделях взаимодействия ОВД с изменяющейся внешней средой и технологию ее эффективного применения в их деятельности.

4. Использовать МАУ ОВД и описать информационные процессы, происходящие в нем.

5. Описать формализованную схему устойчивого функционирование и развитие ОВД.

В теории функциональных систем (ТФС) [1] П.К. Амосов доказал необходимость использования в качестве системообразующего фактора +Кр деятельности организма человека в изменяющейся внешней среде в течение временного интервала Δt_n, отведенного на обработку информации и реализацию должной реакции соответственно текущему стоп-кадру.

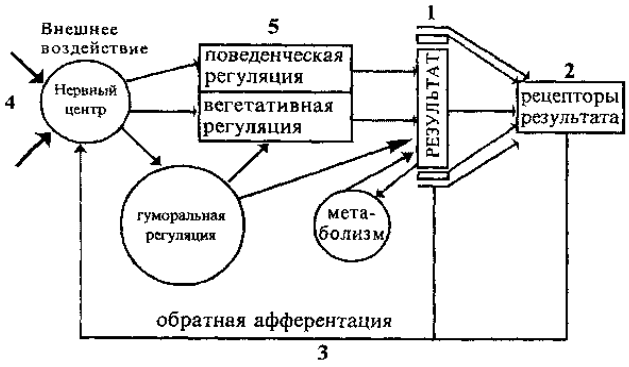


Рис. 1. Схема функциональной системы организма человека.

Функциональные системы (ФС) организма человека – это динамические, саморегулирующиеся центрально-периферические структуры его организации, обеспечивающие своей деятельностью полезные для метаболизма организма и его приспособления к окружающей среде результаты.

Для достижения полезного +Кр ФС организма человека избирательно объединяют q ФЭ разных уровней (ткани органов, механизмы нервной и гуморальной регуляции). Их синхронное взаимодействие обеспечивают должную адаптивную устойчивость +Кр и сбалансирование взаимодействие $\boldsymbol{OC_m=C_k}$ в целом (рис. 1).

На этом рисунке обозначены: 1 – полезный $Y_m(x_n)$ приспособительный результат ОС; 2 – рецепторы результата; 3 – сигналы, идущие от рецепторов результата в центральную нервную систему (ЦНС) организма (обратная связь); 4 – ЦНС как скопления нейронов, их отростков, тесно связанных между собой, спинным и головным мозгом, который создает текущие стоп-кадровые модели $Y_k(x_n)$ и сравнивает их с типовыми стоп-кадровыми моделями $Y_m(x_n)$, хранящимися в памяти человека; 5 – коллективная синхронная работа q функциональных элементов, обеспечивающая выживание ОС в течение временного интервала Δt_n [1, 23–25].

Структура и работа функциональной системы (ФС) организма человека представлена на рисунке 2.

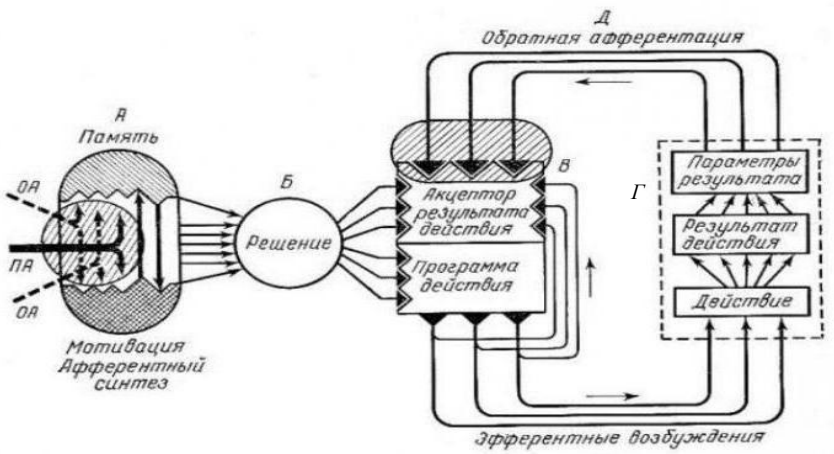


Рис. 2. Структура и работа ФС организма человека.

На нем А – это блок построения текущей модели взаимодействия ОС с внешней средой $Y_k(x_n)$; *Б* – блок сравнения $Y_k(x_n)$ с типовыми моделями $Y_m(x_n)$, хранящимися в памяти человека; *В* – блок разработки программы синхронной работы *q* функциональных элементов (ФЭ) для достижения $+Кр_m$; *Г* – блок фиксации наличие или отсутствия баланса $\boldsymbol{OC_m=C_k}$.

При получении ожидаемого конечного результата выполняется переход к очередному *(k+1)-му* стоп-кадру взаимодействия $OC_m \leftrightarrow C_{k+1}$, иначе запускается механизм поиска $Y^{opt}{}_k(x_n)$ или $Y^{new}{}_k(x_n)$ моделей выживания ОС за счет творческих способностей человека [33–35]. Архитектоника целенаправленного поведенческого акта человека в типовых и нетиповых для него ситуациях представлена на рисунке 3, на котором показано, как из блока акцептор результата поведения в блок афферентного (входного) синтеза подается текущий стоп-кадр $Y_k(x_n)$ взаимодействия $\boldsymbol{OC_m \leftrightarrow C_k}$. Туда же от рецепторов результата поведения и внутренних потребностей организма передаются параметры типовых воздействий внешней среды и внутренних потребностей организма $Y_m(x_n)$. Здесь используются следующие обозначения: ОА – обстановочная, ПА – пусковая афферентации (инфор-мация о состоянии окружающей среды и внутренних органов организма человека в текущем стоп-кадре их взаимодействия) [1].

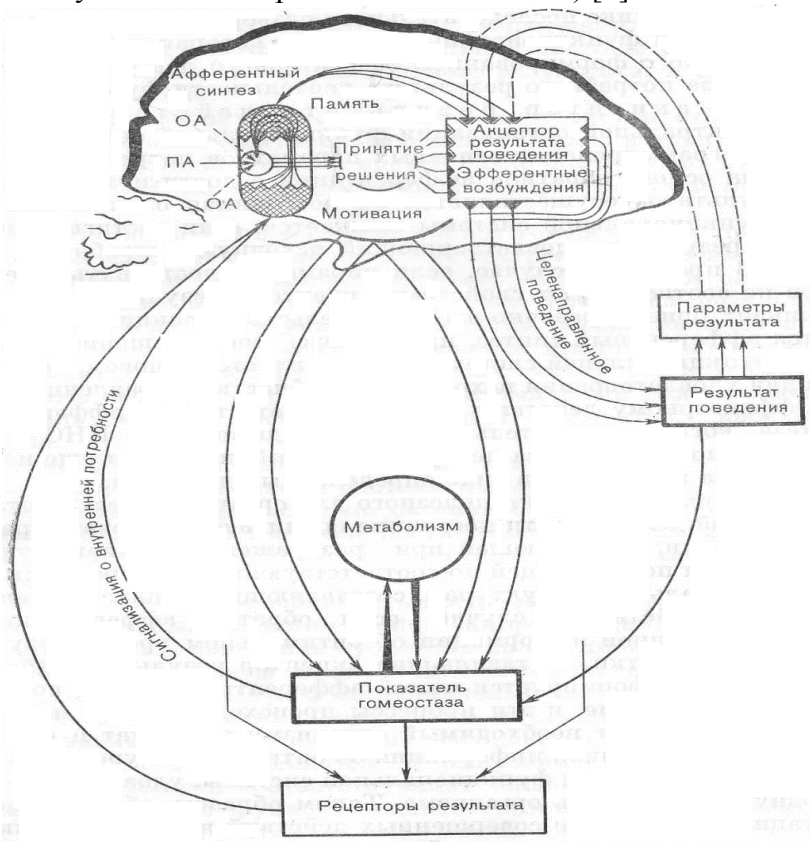


Рис. 3. Взаимодействие функциональной системы гомеостатического и поведенческого уровней в организме человека.

В блоке принятия решения сигналы $Y_m(x_n)$ и $Y_k(x_n)$ сравниваются. При их совпадении с допустимой погрешностью с ($|Y_k(x_n)–Y_m(x)| \leq \varepsilon$) в блоке эфферентные (выходные) возбуждения вычисляются резонансные частоты $\omega_1, \omega_2, ..., \omega_q$ $ФЭ_q$ для импульса $Y_m(x_n)$, создающие на организм человека «эффект системы» $\boldsymbol{OC_m}$, уравновешивающий воздействие внешней среды $\boldsymbol{C_k}$ в текущем стоп-кадре. Затем происходит переход к следующему *(k+1)* стоп-кадру взаимодействия ОС с окружающей средой С.

При несовпадении $Y_k(x_n)$ *с* $Y_m(x_n)$ мозг либо 1) оптимизирует матрицу типовых знаний (МТЗ), либо 2) заново ее пересчитывает, формируя одну/или несколько моделей

$Y^{opt}{}_m(x_n)$, или создает новую МТЗ, где все $Y^{new}{}_m(x_n)$ формируются заново. Процессы автоматической реализации $Y_m(x_n)$, отладки $Y^{opt}{}_m(x_n)$ или пересчета $Y^{new}{}_m(x_n)$ включают следующие этапы: а) афферентный поиск типовой $Y_m(x_n)$, формирование $Y^{opt}{}_m(x_n)$ или синтез $Y^{new}{}_m(x_n)$; б) принятие решения – поиск в памяти человека аналога $Y_k(x_n)$, вычисления, $Y^{opt}{}_m(x_n)$ или $Y^{new}{}_m(x_n)$; в) их сличение с $Y_k(x_n)$ с допустимой при этом погрешностью ε; г) синтез резонансных частот $\omega_1, \omega_2, \ldots, \omega_q$, обес-печивающих синхронную коллективную работу q ФЭ$_q$; д) обратная афферентация – сравнение полученного конечного результата с желаемым результатом $\boldsymbol{OC}_m=\boldsymbol{C}_k$.

В основе теории функциональных систем П. К. Анохина лежат следующие постулаты [1]:

1) +Кр – ведущий объективный показатель деятельности ФС;

2) саморегуляции или динамической самоорганизации ФС;

3) изоморфизма (однотипной организации) ФС разного уровня;

4) представления непрерывного взаимодействия $\boldsymbol{OC}_m \leftrightarrow \boldsymbol{C}_k$ в виде последовательности взаимодействий стоп-кадров $Y_n(x_n) \leftrightarrow Y_k(x_n)$;

5) избирательного объединения ФЭ в должную ФС;

6) синхронной работы ФЭ с должным «эффектом системы»;

7) иерархии, консерватизма и пластичности в деятельности ФС;

9) избирательное улучшение (созревание) ФЭ и ФС в процессе жизнедеятельности организма человека.

С этих позиций МАУ ОВД представляет собой устройство, обеспечивающее: а) работу рецепторов; б) получение нужного для выживания ОВД +Кр; в) передачу входных сигналов от рецепторов в орган управления и обратно – сигналов управления к исполнительным органам ОВД; г) создание нужного для выживания ОВД должного «эффекта системы».

П.К. Анохин подчеркивал, что каждый организм представляет собой динамическое сочетание устойчивости и изменчивости. Изменчивость организма (у нас ОВД) определяет его приспособительные реакции, например, гомеостаз – жизнеспособность организма практически в любых условиях, на которые он в состоянии адекватно реагировать.

Взаимодействие ОС с постоянно изменяющейся внешней средой (С) в типичных (устойчивых) и нетипичных (неустойчивых) ситуациях представлено на рисунке 4 в виде алгоритмической модели работы механизма адаптивного управления ОС. Он обеспечивает создание нужного для ее выживания в конкретном m-м стоп-кадре «эффекта системы» [1, 27–28].

На рисунке 4 в правом верхнем углу указана матрица типовых знаний (МТЗ), а в нижнем левом – иерархические оргструктуры из q функциональных элементов (ФЭ$_q$), синхронная, работа которых создает нужные для выживания ОС «эффекты системы» $+Кр_m=\boldsymbol{OC}_m=\boldsymbol{C}_k$. При совпадении $Y_m(x_n)$ с $Y_k(x_n)$ ОС выживает в текущем k-м стоп-кадре ее взаимодействия с изменяющейся внешней средой ($\boldsymbol{C}$).

МТЗ состоит из m строк типовых функций $Y_1(x_n), \ldots, Y_m(x_n), \ldots, Y_M(x_n)$ от n переменных x_n, которые сравниваются с текущей функцией $Y_k(x_n)$. При выполнении условия $|Y_k(x_n)-Y_m(x)| \leq \varepsilon$, в блоке ДПФ (дискретное преобразование Фурье) вычисляются собственные круговые частоты $\omega_1, \omega_2, \ldots, \omega_q$ для $Y_m(x_n)=Y_k(x_n)$, создающие «эффект системы» $\boldsymbol{OC}_m$, уравновешивающий воздействие внешней среды $\boldsymbol{C}_k$ на ОС в текущем k-м стоп-кадре [17].

Здесь же введены обозначения: Фк – фиксация или не фиксация параметров внешнего текущего воздействия на ОС; Оц – оценка параметров внешнего текущего воздействия на ОС; Оц – оценка параметров внешнего (из среды) и внутренних (от ОС) воздействий или возврат в блок Фк; Кд – кодирование параметров воздействия или воз-

врат в блок Оц; $Y_k(x_n)$ – построение типовой модели текущего стоп-кадра или возврат в блок Кд; Ид – идентификация модели типового текущего стоп-кадра $Y_k(x_n)$ путем его сравнения с типовыми $Y_m(x_n)$ из МТЗ (при совпадении $Y_m(x_n)=Y_k(x_n)$ переход в блок Авт – автоматики, иначе возврат в блок Кд); Авт – блок автоматики, где ОС принимается решение о формальном, т. е. автоматическом создании нужного «эффекта системы» за счет перехода в блок ДПФ, иначе переход в блок ФЛ – формальной логики; ДПФ – блок автоматического вычисления спектра круговых частот $\omega_1, \omega_2, ..., \omega_q$, обеспечивающих за счет синхронной работы q ФЭ$_q$ должный для выживания ОС «эффект системы», иначе возврат блок Авт; Об – общая передача спектра команд управления $\omega_1, \omega_2, ..., \omega_q$ исполнительным элементам и обеспечение ими за счет коллективной работы требуемого «эффект системы», иначе возврат в блок Авт; блок +Кр – оценка полученного +Кр, если он получен управленческий кадр окончен, иначе переход к блоку Об [17].

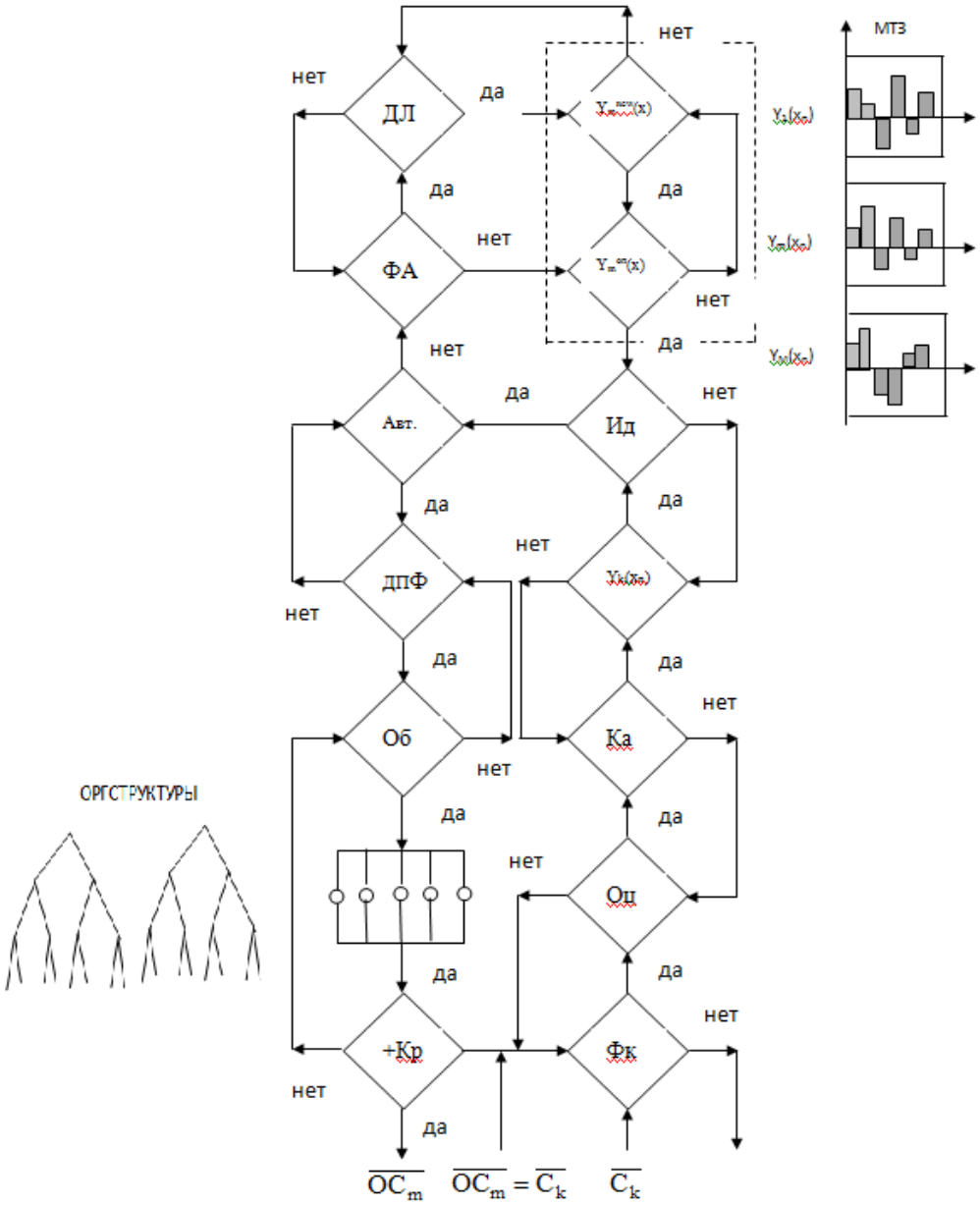


Рис. 4. Концептуальная алгоритмическая модель работы МАУ ОС.

Все указанные в верхнем абзаце блоки используются для автоматической реализации типовых моделей поведении ОС. Однако в организме человека природа отрабо-

тала еще два варианта его выживания. Первый вариант основывается на частичном улучшении некоторых типовых моделей $Y_m(x_n)$ за счет их оптимизации – создания моделей $Y_m^{opt}(x_n)$. Второй вариант реализует полный пересчет МТЗ, $Y_m(x_n)$, т. е. создание новой МТЗ, где все модели $Y_m^{new}(x_n)$ обладают принципиально новыми уникальными качествами [13–15, 17].

Поясним суть оптимизации и построения новой МТЗ. Оптимизация МТЗ представляет собой промежуточный вариант ее обновления. ФЛ – блок формальной логики, где выясняется, можно ли формально улучшить одну или несколько функций $Y_m(x_n)$. Если можно, то осуществляется переход в блок $Y_m^{opt}(x_n)$, иначе возврат в блок Авт; ДЛ – блок диалектической логики, где устанавливается возможность кардинального улучшения МТЗ и осуществляется переход к блоку $Y_m^{new}(x_n)$, иначе возврат в блок $Y_m^{opt}(x_n)$; $Y_m^{new}(x_n)$ – блок пересчета всей МТЗ на базе новейших достижений науки и техники, иначе возврат в $Y_m^{opt}(x_n)$ [17].

Таким образом, с помощью творческого использования возможностей формальной и диалектической логики через практическое подтверждение новых возможностей $МТЗ_{opt}$ и $МТЗ_{new}$ человек непрерывно развивает свои интеллектуальные способности [27]. Результат реализация модели $Y_k(x_n)$ предполагает два варианта взаимодействия $ОС_m \leftrightarrow С_k$:

$$Y_k(x_n) = Y_m(x_n) \quad (1)$$

$$Y_k(x_n) \neq Y_m(x_n). \quad (2)$$

В случае (1) ОС выживает, а (2) – она может погибнуть, если не найдет способа, обеспечивающего ее адаптацию к новым условиям. Однако в случае (2) естественный интеллект (разум человека) в рамках законов диалектики природы нашел поэтапный способ достижения (1) за счет усиления им своего творческого потенциала (путем обязательной проверки его мощи в деле).

Это подтверждено А.Н. Колмогоровым и Э.В. Евреиновым. Первый в 1957 г. доказал теорему [18], а Э.В. Евреинов практически подтвердил, что модель коллектива вычислителей не имеет ограничений по производительности (таблица 1) [16].

Таблица 1

Сравнение моделей вычислителя и коллектива вычислителей

Модель вычислителя	**Модель коллектива вычислителя**
Последовательное выполнение операций; Фиксированная логическая структура вычислений	Параллельное выполнение операций; Переменная логическая структура вычислений
Конструктивная неоднородность элементов и связей	Конструктивная однородность элементов и связей
Имеет ограничение по росту производительности ВТ	Не имеет ограничений по производительности ВТ

Она позволяет понять, почему выживание ОС возможно лишь при выполнении условия $Y_k(x_n)=Y_m(x_n)$.

Модель коллектива вычислителей является главным инструментом, обеспечивающим прорыв в росте высокоскоростных вычислений. Установлено, что нужный по производительности «эффект системы» $Y_m(x_n)$ в ОС достигается одним и тем же способом, а именно – синхронной (параллельной) работой ее исполнительных (функциональных) элементов (ФЭ) [11].

Теорема Колмогорова утверждает, любая непрерывная функция от N переменных $Y(x)=Y(x_1, x_2,..., x_N)$, определенная на N-мерном единичном кубе, может быть представлена в виде суммы $2N+1$ суперпозиций непрерывных и монотонных отображений единичных отрезков [19]:

$$Y(x_1, x_2, ..., x_N) = \sum_{n=1}^{2N+1}\left(g_n \sum_{m=1}^{N}(h_{mn}(x_m))\right) = \sum_{n=1}^{2N+1}\left(\log_2 \sum_{m=1}^{N}(h_{mn}(x_m))\right) \quad (3)$$

где $x = (x_1, ..., x_N)$, $0 \le x_n \le 1$.

Слева в формуле (1.3) стоит непрерывная произвольная функция, определенная на многомерном кубе, а непрерывные функции g_n и $h_{mn}(x_m)$ определены на отрезках [0,1]. Монотонные непрерывные отображения h_{mn} могут иметь достаточно сложную структуру, но не зависят от конкретной функции $Y(x)$ (здесь это логарифмическая функция $y=log_2x$). Эта теорема означает, что для реализации функций многих переменных достаточно операций суммирования и композиции функций одной переменной.

В качестве характеристики, определяющей уникальность каждой функции $Y(x_n)$, выберем упорядоченный набор интегральных сумм на отрезке [0,1]

$$\sum_{n=1}^{N} h_{mn}(\xi_n)\Delta x_n, \quad (4)$$

который рассматриваем как информацию о виде функции $Y(x_n)$.

В [15] доказано, что «конкретная математика» расшифровывается как КОНтинуальная и дисКРЕТНАЯ математика, т. е. как единство непрерывной и дискретной математик. Ее назначение – научить технике грамотного оперирования с дискретными объектами, аналогичной технике для непрерывных объектов. Авторы книги на конкретных примерах обучают математическим методам исследования дискретно-непрерывных систем.

Е.В. Луценко [23-26] разработал системную теорию информации и технологию ее применения, названную им автоматизированным системно-когнитивным анализом (АСК-анализ), которую реализовал в программном комплексе «Эйдос». Она успешно используется им при управлении ОС в типовых ситуациях, математически описываемых матрицей типовых знаний (МТЗ), формируемой системой «Эйдос». С ее помощью с заданной точностью можно распознать типовые ситуацию и запустить соответствующий конкретный механизм выживания системы.

МТЗ позволяет устанавливать реальные связи и их силу для всех ее параметров. С помощью этой системы можно получать новые знания и использовать их для достижения нужного +Кр [17].

Из описания работы математических моделей взаимодействия ОС с изменяющейся внешней средой в типичных $Y_k(x_n) = Y_m(x_n)$ и в нетипичных $Y_k(x_n) \neq Y_m(x_n)$ ситуациях (рисунок 4) вытекает следующий вывод.

Мозг человека – орган, единообразно создающий текущие $Y_k(x_n)$ и типовые модели $Y_m(x_n)$ взаимодействия человека с изменяющейся внешней средой. Тело человека – исполнительный орган, обеспечивающий синхронную работу различных функциональных элементов ОС с нужным для нее «эффектом системы».

При однозначной идентификации $Y_k(x_n)=Y_m(x_n)$ на базе модели $Y_m(x_n)$ автоматически запускается процесс вычисления собственных круговых частот $\omega_1, \omega_2, \ldots, \omega_q$, задействованных q нужных ФЭ$_q$. Тем самым достигается их синхронная (коллективная) работа, создающая «эффект системы», определяющий выживание ОС в очередной типовой ситуации.

В противном случае мозг конструирует $Y^{opt}{}_m(x_n)$ или новые $Y^{new}{}_m(x_n)$ и пытается быстро апробировать их на практике для дальнейшего использования. Таким образом, мозг создает новые возможности организма и обеспечивает его растущие потребности. В результате творческого развития уточняется МТЗ.

Программный комплекс, автоматизирующий работу МАУ ОС в указанном направлении, предполагается реализовать на базе компьютерной системы «Эйдос-АСА», которая будет включать себя программу быстрого преобразования Фурье (БПФ)

[26-28]. Она позволит вычислять собственные круговые частоты ω_{m1}, ω_{m2}, …, ω_{mq}, используемые в МАУ ОВД и обеспечит получение нужных для выживания ОВД «эффектов системы» в типичных и не типичных для них ситуациях.

Литература

1. Анохин П.К. Избранные труды. Принципиальные вопросы общей теории функциональной системы / П К. Анохин. – М.: Наука, 1978. – 400 с.

2. Аршинов Г.А. Анализ оборота капитала и цены на готовую продукцию в интегрированных объединениях АПК / Г. А. Аршинов, С.В. Лаптев, В.Г. Аршинов // Новые технологии. – 2018. – № 4. – С. 96–101.

3. Аршинов Г.А Анализ современных форм интеграции сельскохозяйственных товаропроизводителей и перерабатывающих предприятий АПК / Г. А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2016. – № 123. – С. 1392–1421.

4. Аршинов Г.А. Анализ условий образования эффективных объединений предприятий молочного подкомплекса АПК /, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2017. – № 132. – С. 128–155.

5. Аршинов В.Г. Математическое моделирование интеграционных процессов в АПК / В. Г. Аршинов, С. В. Лаптев // Математические методы и информационно-технические средства: сб. статей II Всероссийской научно-практической конференции. – 2006. – С. 5–6.

6. Аршинов Г.А. Математическое моделирование экономической деятельности перерабатывающих предприятий / Г. А. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: материалы IX Всероссийской научно-практической конференции; отв. ред. С.А. Вызулин, Е.В. Михайленко, Ю.Н. Сопильняк. – Краснодар: КубГАУ, 2013. – С. 24–27.

7. Аршинов Г.А. Математическое моделирование отношений партнеров в современных формах интеграции сельскохозяйственных товаропроизводителей и перерабатывающих предприятий / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2017. № 130. – С.1137–1159.

8. Аршинов Г.А. Математическое моделирование экономической деятельности перерабатывающих предприятий / Г.А. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: материалы IX Всероссийской научно-практической конференции; отв. ред. С.А. Вызулин, Е.В. Михайленко, Ю.Н. Сопильняк. – Краснодар: КубГАУ, 2013. – С. 24–27.

9. Аршинов Г.А. Совершенствование акустических методов диагностики скрытых микродефектов и эксплуатационная надежность вязкоупругих элементов конструкций / Г.А. Аршинов, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. № 154. – С. 84–93.

10. Аршинов Г.А. Оценка экономической и эксплуатационной надежности строительных сооружений на основе исследования волновых характеристик нелинейных вязкоупругих стержневых элементов конструкций / Г. А. Аршинов, С. В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2019. – № 153. – С. 113–122.

11. Аршинов Г.А. Причины, препятствующие созданию эффективных объединений предприятий молочного подкомплекса АПК / Г.А. Аршинов, В.И. Лойко, В.Г. Ар-

шинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2016. № 123. – С. 1422–1443.

12. Аршинов Г.А. Стратегия и тактика использования МАУ ОС в деятельности АПК / Г.А. Аршинов, В.И. Лойко, С. В. Лаптев // Трансформация социально-экономического пространства России и мира: сб. статей Международной научно-практической конференции / под ред. Г.Б. Клейнера, Х.А. Константиниди, В.В. Сорокожердьева, З.М. Хашевой. – 2020. – С.131–135.

13. Аршинов Г.А. Уточнение акустических методов регистрации микродефектов материала на основе исследования нелинейных волн деформаций в вязкоупругих стержнях / Г.А. Аршинов, В.И. Лойко, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГАУ, 2020. № 162. – С.37–53.

14. Аршинов В.Г. Функция скорости спроса и оборот вложенного капитала в интеграционных структурах АПК / В.Г. Аршинов, С.В. Лаптев // Математические методы и информационно-технические средства: сб. статей II Всероссийской научно-практической конференции. 2006 – С.7–9.

15. Грэхмен Р. Конкретная математика: Основания информатики / Р. Грэхмен, Д. Кнут, О. Паташник. – М.: Мир, 2006. – 703 с.

16. Евреинов Э. В. Однородные вычислительные системы, структуры и среды / Э. В. Евреинов. – М.: Радио и связь, 1981. – 208 с.

17. Информационная безопасность: учеб. пособие / В.И. Лойко, В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с.

18. Колмогоров А. Н. О представлении непрерывных функций нескольких переменных в виде суперпозиций непрерывных функций одного переменного и сложения / А. Н. Колмогоров // Доклады АН СССР, 1957. – Т. 114. – С. 953–956.

19. Лаптев В.Н. Разработка адаптивной матрицы типовых знаний для инвестиционного управления АПК / В.Н. Лаптев, Г.А. Аршинов, С.В. Лап-тев, Т.В. Лукьяненко, Е.В. Фешина // Политематический сетевой элект-ронный научный журнал Кубанского государственного аграрного универ-ситета. – Краснодар: КубГАУ, 2020. – № 164. – С. 36–54.

20. Лаптев С.В. Постановка курса «Web-технологии в идентификации систем» / С. В. Лаптев // Качество современных образовательных услуг – основа конкурентоспособности вуза. Сб. статей по материалам межфакультетской учебно-методической конференции. / Отв. за вып. М.В. Шаталова. – Краснодар: КубГАУ, 2016. – С.298–300.

21. Лаптев С.В. Нелинейные дисперсионные волны в вязкоупругих тонкостенных конструкциях: дисс. канд физ.-мат. наук / С.В. Лаптев. – Саратов: СГУ, 2000. – 132 с.

22. Лаптев С.В. Разработка информационных систем на базе web-технологий: учеб. пособие / С.В. Лаптев, В.Н. Лаптев, Г.А. Аршинов – Краснодар: КубГАУ, 2021. – 175 с.

23. Луценко Е. В. Автоматизированный системный анализ в управлении активными объектами: монография / Е. В. Луценко. – Краснодар: КубГАУ, 2002. – 605 с.

24. Луценко Е. В. Автоматизированный системный анализ как средство пересинтеза модели активного объекта управления при прохождениии им точки бифуркации / Е. В. Луценко, В. Н. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2007. – № 30. – С. 1–19.

25. Луценко Е. В. Системно-когнитивное моделирование в АПК / Е. В. Луценко, В. Н. Лаптев, А. Э. Сергеев. – Краснодар: КубГАУ, 2018. – 517 с.

26. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ № 490 от 10 октября 2019 г.

27. Сато Ю. Без паники! Цифровая обработка сигналов. / Ю. Сато; пер. с японского Т. Г. Селиной. – М.: Додэка-XXI, 2010. – 176 с.

28. Степанов В.В. Нелинейная математическая модель ценообразования продукции перерабатывающего предприятия / В.В. Степанов, Г.А. Аршинов, С.В. Лаптев, И.А. Мануйлов // Автоматизированные информационные и электроэнергетические системы: материалы II Межвузовской научно-практической конференции. – Краснодар: КубГТУ, 2012. – С.38–40.

29. Энгельс Ф. Диалектика природы. избр. соч. / Ф. Энгельс. в 9 т.–Т. 5. – М.: Политиздат, 1986. – С. 372–613.

Сведения об авторе

Лаптев Владимир Николаевич, кандидат технических наук, доцент, доцент кафедры комьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: lvn4828@yandex.ru.

Медведев Виталий Александрович,
Аристов Роман Викторович

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, КАК ПЕРСПЕКТИВНЫЙ МЕТОД БОРЬБЫ С ПРЕСТУПНОСТЬЮ

В настоящее время наблюдается увеличение преступлений, совершаемых с использованием информационных технологий. Безусловно, это связано с тем, что 21 век, это век информационных технологий. Согласно официальной статистике МВД России за 2020 год число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4% (510396 тыс.), в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%. Существуют трудности в раскрытии такого вида преступлений. Согласно статистике МВД России, в 2020 году осталось не раскрыто 83,9 % (379830) таких преступлений. Также очень сложно доказать вину подозреваемых в совершении данных преступлений, например, при мошенничестве в сети интернет. Для решения проблемы проводятся научные исследования в данной области. Одним из приоритетных направлений научных исследований, согласно Концепции научного обеспечения деятельности органов внутренних дел Российской Федерации, на период до 2030 года, а также Сводному перечню проблем деятельности органов внутренних дел Российской Федерации, требующих научного разрешения, является совершенствование системы раскрытия и расследования преступлений в сфере компьютерных технологий.

Исходя из проведенных исследований, можно сделать однозначный вывод в необходимости реорганизации органов внутренних дел с целью увеличения сотрудников технической направленности, а также внедрения технического прогресса в работу сотрудников полиции. Увеличения специалистов по компьютерным технологиям в органах внутренних дел позволит увеличить раскрываемость преступлений в сфере высоких технологий. Соответственно, в настоящее время, необходимо уделять особое внимание подготовке квалифицированных кадров в области защиты информации и защиты персональных данных.

Также необходимо создание отдельных подразделений по борьбе с интернет мошенничеством (например, фишингом – подмена сайта для получения персональных данных или взлом социальных сетей в корыстных целях) на районном уровне. Ведь борьба с киберпреступностью в данный момент, это прерогатива отдела «К», но коли-

чество преступлений, с использованием информационных технологий только растет, и в настоящий момент отдел «К» просто не может заниматься всеми преступлениями.

Нельзя обойти стороной и необходимость внедрения в работу полиции технического прогресса. Например, внедрение в процесс расследования преступления элементов искусственного интеллекта, такого как, нейронная сеть, которая сможет определять в автоматическом режиме источник интернет атаки или фактический адрес устройства, откуда осуществлялось интернет мошенничество по средствам привязки к телекоммуникационным вышкам и интернет провайдерам. После полученной информации сотруднику полиции будет уже гораздо легче осуществлять поиск преступников.

В настоящий момент, федеральная служба безопасности использует программное обеспечение, на основе нейронных сетей, для распознавания лиц, при использовании видеонаблюдения городской инфраструктуры. Или поиска потенциальных подозреваемых на основе фоторобота. Доступ к данному программному обеспечению необходимо предоставить органам внутренних дел для поиска лиц, подозреваемых в совершении преступлений, в рамках их юрисдикции.

Также нейронные сети можно использовать для расследования преступлений общеуголовной направленности, совершенных без использования компьютерных технологий. Например, в США активно ведется работа по наполнению базы данных ДНК человека. Искусственный интеллект используется для поиска родственников, посредством сдачи анализа ДНК тестов и сравнения полученных результатов с базой данных. В США в настоящее время достаточно просто сдать анализ ДНК и уже система сама начнет процесс сравнения с имеющимися материалами в базе данных, с выводом соответствующих результатов с указанием процентного родственного совпадения. Основное условие, это то, что результаты анализов ДНК потенциальных родственников тоже должны находиться в данной базе. Но с точки зрения развития медицины в целом, и методов анализа в частности, такой проблемы в США не стоит. Они автоматически пополняют базу данных при определенных медицинских исследованиях. Согласие человека на это не требуется. Вначале основной целью создания такой базы данных было поиск родственников для сдачи донорской крови или даже пересадки органов от близких родственников, которые могут даже и не знать о своем родстве. Но также полиция использует данную базу для сравнения найденных следов ДНК с места преступления. Безусловно, наполнение данной базы занимает длительное время, но данный метод, в конечном результате, приводит к увеличению раскрываемости преступлений.

Безусловно, внедрение элементов искусственного интеллекта в деятельность органов внутренних дел может повлечь за собой отрицательные последствия, такие как возможность технической ошибки или возможность внесения изменений в работу системы или хищение персональных данных злоумышленниками в случаи плохого обеспечения информационной безопасности или халатности сотрудников. Но стоит заметить, что внедрение технического прогресса в деятельность органов внутренних дел в первую очередь приведет к увеличению раскрываемости преступлений, профилактики и предупреждения преступлений на примере компьютерных систем прогнозирования повторного совершения преступления по фотографии и психологическому портрету осужденного. Также нет необходимости значительного увеличения сотрудников ОВД. Но искусственный интеллект не должен заменить сотрудника полиции, он должен стать лишь его помощником в борьбе с преступностью.

Литература

1. Демина Р.Е. Совершенствование организации и использования криминалистических учетов МВД России для успешного раскрытия преступлений // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 44-47.

2. Ковалев С.А. Использование криминалистического компьютерного моделирования при планировании расследовании преступлений/ С.А. Ковалев //Юридические науки. – С. 111 – 123.

3. Малюгина А.В., Ануфриева А.Н. Возможности оптимизации и совершенствования деятельности полиции России, связанные с применением технологических инноваций (анализ зарубежного опыта) // European Journal of Natural History. 2020. № 4. С. 78-84.

4. Платонов В.А. Использование информационных технологий в раскрытии и расследовании преступлений/ В.А. Платонов // Юридические науки. – С. 52 – 54.

5. Рак И.П. Информационные технологии в деятельности правоохранительных органов // Инновационная наука. 2016. № 2-3. С. 132-135.

Сведения об авторах

Медведев Виталий Александрович, преподаватель кафедры социально-экономических и гуманитарных дисциплин Ленинградского областного филиала Санкт-Петербургского университета МВД России; e-mail: smit-vint@yandex.ru.

Аристов Роман Викторович, кандидат философских наук, доцент кафедры социально-экономических и гуманитарных дисциплин Ленинградского областного филиала Санкт-Петербургского университета МВД России; e-mail: 20arv20@mail.ru.

Михайленко Евгений Владимирович

ТЕХНОЛОГИИ ПОДГОТОВКИ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ ГЕНЕРАЦИИ И ПРОВЕРКИ ПРАКТИЧЕСКИХ ЗАДАНИЙ ПО ТЕМЕ «СРАВНЕНИЯ»

В статье описываются процедуры подготовки программных продуктов для генерирования и верификации практических заданий по теме «Сравнения» раздела «Теория чисел», изучаемой курсантами Кранодарского университета МВД России, обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере. Описываемые приложения рассчитаны на использование среды офисного пакета Microsoft Office, в настоящее время являющегося наиболее распространенным в России, однако все рассуждения, касающиеся методов и технологий создания указанных программных продуктов, легко могут быть перенесены на другие информационно совместимые программные пакеты, такие как, например, OpenOffice или LibreOffice [1, 12]. Кроме того, разработанные в среде Microsoft Office программные продукты в большинстве случаев без потерь будут открываться и работать в указанных системах.

Выбор среды программирования обоснован мощным математическим аппаратом Visual Basic for Application (VBA), доступность широких возможностей использования различных шрифтов, графических форм и объектов, простотой, логичностью синтаксиса и семантики встроенного языка программирования [2, 3, 8]. Удобство использования выбранного программного продукта заключается также и в том, что перечень заданий, подготовленный в виде документа или таблицы, не требует специальной обработки для вывода на печать [5, 13].

Суть разрабатываемых программных комплексов заключается в использовании приложений интегрированных пакетов Microsoft Office, OpenOffice или LibreOffice, где на заранее подготовленную форму в виде документа, электронной таблицы или презентации автоматически по специальному алгоритму, реализованному в виде макросов,

выводятся сгенерированные данные в виде комбинации чисел, символов, строк, таблиц или графических объектов [9, 10, 11].

Разрабатывая аогоритмы компьютерных программ, не всегда удается построить прорстой и лаконичный вычислительный процесс. Часто для формирования заданий необходимо использовать массивы числовых и текстовых данных, разветвляющиеся и циклические структуры, учитывать ряд ограничений и связей [6. 14].

Особенность генерирования таких заданий заключается в совместной обработке специальным образом структурированных числовых массивов, содержащих различные данные [4, 7]. Рассмотрим примеры заданий из программного комплекса «Сравнения». В задании 1 (рис. 1) требуется выписать все целые числа из указанного промежутка $[n_1; n_2]$, сравнимые с числом *a* по модулю *b*.

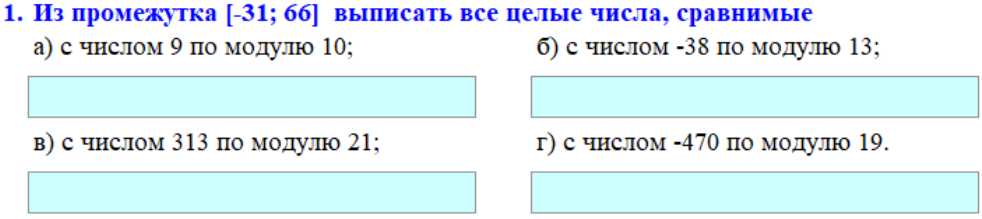


Рис. 1. Задание 1 программного комплекса «Сравнения».

Уже в заголовке мы видим сгенерированные значения начала и конца промежутков, кроме того, нам необходимо определить значения числа *a* и модуля *b* в четырех пунктах задания. Рассмотрим генерацию и проверку пункта 1.а (рис. 2).

```
Do                                      'Генерируем a, b, n1, n2
  a = Rnd(v) * 10 + 8
  b = Rnd(v) * 10 + 8
  n1 = Rnd(v) * 20 - 40
Loop Until a <> b And n1 Mod b <> 0 And n1 Mod a <> 0
n2 = n1 + b * 9 + 7

t = ""                                  'Находим решение t
s1 = a Mod b
For i = n1 To n2
  s2 = i Mod b: If s2 < 0 Then s2 = s2 + b
  If s1 = s2 Then t = t + st(i) + ", "
Next i
t = NoSpase(Mid(t, 1, Len(t) - 2))
                                        'Читаем ответ
tz = NoSpase(Cells(11, 2))              'и сравниваем с решением
If t = tz Then mark = mark + 1 Else Call krest(11, 2)
```

Рис. 2. Генерация и проверка задания 1.а.

Для генерации условия в цикле с постусловием Do .. Loop Until мы определяем значения числа *a*, модуля *b* и начала промежутка $[n_1; n_2]$ таким образом, чтобы числа *a* и *b* были различны, а n_1 не делилось ни на *a* ни на *b*. Конец промежутка n_2 задается позже завершения цикла и устанавливается большим значения *a* на величину $9b+7$.

Решение находим в цикле с параметром *i*, в котором мы находим s_1 – остаток от деления *a* на *b*, затем перебирая по порядку все целые числа из промежутка $[n_1; n_2]$, добавляем в список *t*, только те, для которых остаток от деления на *b* равен s_1. Из ответа выполненного задания мы убираем все пробелы и сравниваем его с нашим рассчитанным результатом.

В задании 2 программного комплекса программного комплекса «Сравнения» (рис. 3) требуется разбить выведенное множество чисел на классы вычетов по данному модулю. Отметим, для этого задания необходимо сгенерировать последовательности целых чисел и модуль, однако классы вычетов $\overline{0}$, $\overline{3}$, $\overline{4}$, $\overline{7}$, предложенные в задаче являются фиксированными.

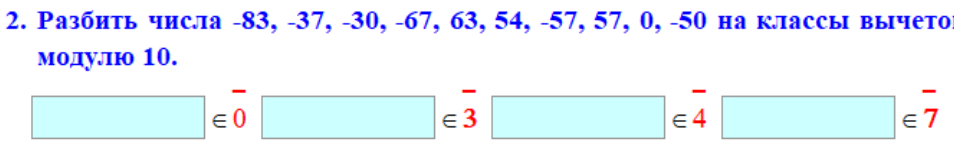


Рис. 3. Разбить представленные числа на классы по данному модулю.

Рассмотрим код генерации параметров задания (рис. 4).

```
Do                                  'Генереруем массив чисел
  t = ""
  s0 = 0: s3 = 0: s4 = 0: s7 = 0:
  For i = 1 To 10
    Do
      mX(i) = Rnd(v) * 200 - 100
      j = 0
      For k = 1 To i - 1
        If mX(i) = mX(k) Then j = j + 1
      Next
      r = mX(i)
      Do While r < 0
        r = r + b
      Loop
    Loop Until j = 0 And (r Mod b = 0 Or r _
              Mod b = 3 Or r Mod b = 4 Or r Mod b = 7)
    If r Mod b = 0 Then         'Помещаем числа в класс 0
      s0 = s0 + 1: mT0(s0) = mX(i)
      For k = 1 To s0 - 1
        If mT0(s0) < mT0(k) Then Call swap(mT0(s0), mT0(k))
      Next k
    End If
    If r Mod b = 3 Then         'Помещаем числа в класс 3
      s3 = s3 + 1: mT3(s3) = mX(i)
      For k = 1 To s3 - 1
        If mT3(s3) < mT3(k) Then Call swap(mT3(s3), mT3(k))
      Next k
    End If
    If r Mod b = 4 Then         'Помещаем числа в класс 4
      s4 = s4 + 1: mT4(s4) = mX(i)
      For k = 1 To s4 - 1
        If mT4(s4) < mT4(k) Then Call swap(mT4(s4), mT4(k))
      Next k
    End If
    If r Mod b = 7 Then         'Помещаем числа в класс 7
      s7 = s7 + 1: mT7(s7) = mX(i)
      For k = 1 To s7 - 1
        If mT7(s7) < mT7(k) Then Call swap(mT7(s7), mT7(k))
      Next k
    End If
    t = t + st(mX(i)) + ", "
  Next i
Loop Until s0 > 1 And s3 > 1 And s4 > 1 And s7 > 1
```

Рис. 4. Генерация задания 2 программного комплекса «Сравнения».

Как мы видим из представленного кода программы, что каждый из десяти элементов массива mX, генерируемых по выше предложенному алгоритму, мы помещаем в один из классов s0, s3, s3 или s7. Элементы в соответствующих массивах mT0, mT3, mT4, mT7 упорядочиваются по мере поступления элементов. Генерация может происходить неоднократно, поскольку для завершения основной итерации должно быть выполнено условие, смысл которого заключается в том, что ни один из представленных классов не должен оказаться пустым.

Рассмотрим технологии проверки данного задания (рис. 5). Процесс проверки задания сводится к последовательному формированию в цикле For .. Next с параметром i каждого из четырех решений: t0, t3, t4 и t7. Решения выписываются из заполненных массивов mT0, mT3, mT4, mT7. Затем считываем решения tz из выполненных заданий, убираем пробелы и сравниваем их с нашими решениями.

```
t0 = ""                                  'Находим решение t0
For i = 1 To s0
  t0 = t0 + st(mT0(i)) + ", "
Next i
t0 = NoSpase(Mid(t0, 1, Len(t0) - 2))
            'Читаем ответ и сравниваем с решением (Класс "0")
tz = NoSpase(Cells(18, 2))
If t0 = tz Then mark = mark + 1 Else Call krest(18, 2)
            'Находим решение t3
t3 = ""
For i = 1 To s3
  t3 = t3 + st(mT3(i)) + ", "
Next i
t3 = NoSpase(Mid(t3, 1, Len(t3) - 2))
            'Читаем ответ и сравниваем с решением (Класс "3")
tz = NoSpase(Cells(18, 6))
If t3 = tz Then mark = mark + 1 Else Call krest(18, 6)
            'Находим решение t4
t4 = ""
For i = 1 To s4
  t4 = t4 + st(mT4(i)) + ", "
Next i
t4 = NoSpase(Mid(t4, 1, Len(t4) - 2))
            'Читаем ответ и сравниваем с решением (Класс "3")
tz = NoSpase(Cells(18, 10))
If t4 = tz Then mark = mark + 1 Else Call krest(18, 10)
            'Находим решение t7
t7 = ""
For i = 1 To s7
  t7 = t7 + st(mT7(i)) + ", "
Next i
t7 = NoSpase(Mid(t7, 1, Len(t7) - 2))
            'Читаем ответ и сравниваем с решением (Класс "7")
tz = NoSpase(Cells(18, 14))
If t7 = tz Then mark = mark + 1 Else Call krest(18, 14)
```

Рис. 5. Фрагмент кода проверки задания 2 программного комплекса «Сравнения».

Задания 3 и 4 программного комплекса «Сравнения» посвящены составлению полной и приведенной систем вычетов по заданному модулю. На рисунке 2.1.16 представлены сгенерированные формы заданий.

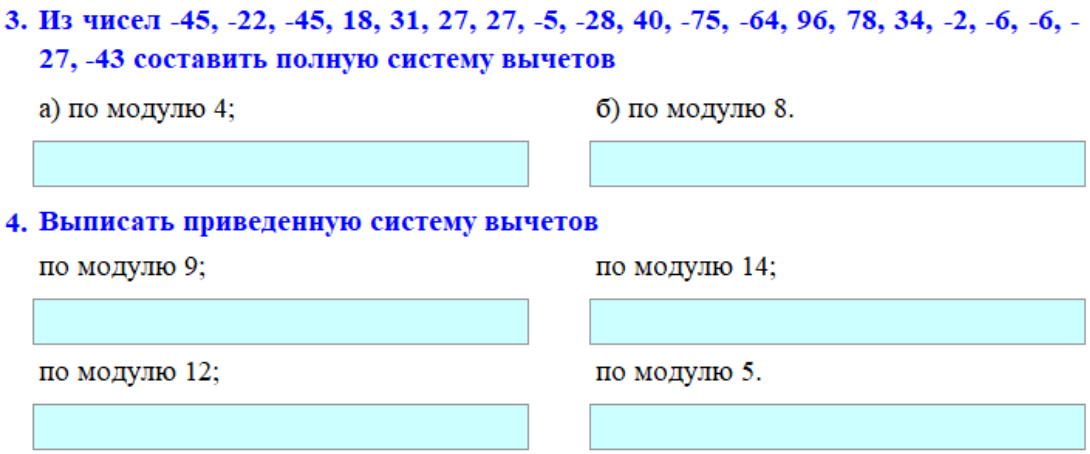


Рис. 6. Сгенерированные формы заданий 3 и 4.

Рассмотрим процесс генерации и проверки только четвертого задания. На рисунке 7 представлен код генерации задания 4 «Выписать приведенную систему вычетов».

```
'4. Выписать приведенную систему вычетов
Do
  b1 = Rnd(v) * 8 + 4
  b2 = Rnd(v) * 8 + 8
  b3 = 2 ^ (Int(Rnd(v) * 2 + 1)) * 3 ^ (Int(Rnd(v) * 2 + 1))
  b4 = 2 ^ (Int(Rnd(v) * 2 + 1)) * 3 ^ (Int(Rnd(v) * 2)) * _
            5 ^ (Int(Rnd(v) * 2)) * 7 ^ (Int(Rnd(v) * 2))
Loop Until b1 <> b2 And b1 <> b3 And b1 <> b4 And b2 <> b3 _
            And b2 <> b4 And b3 <> b4 And b3 > 10 _
            And b3 < 30 And b4 > 10 And b4 < 30
```

Рис. 7. Генерация задания 4 «Выписать приведенную систему вычетов».

Здесь в цикле Do .. Loop Until последовательно формируются четыре значения: b1, b2, b3 и b4, представляющих соответственно модули чисел из задания. Если первые два числа b1 и b2 формируются случайным образом из диапазонов от четырех до двенадцати и от восьми до шестнадцати и могут быть простыми числами, то значения b3 и b4 составляются из произведения простых чисел: 2, 3, 5 и 7 в соответствующих степенях. В постусловии цикла полученные значения проверяются на совпадения, кроме того, должны быть выполнены требования для диапазонов величин b3 и b4.

Во время проверки заданий (рис. 8) нам необходимо рассчитать приведенную систему для каждого модуля.

Приведенная система для модулей b1, b2, b3 и b4 формируется в строчных переменных t1, t2, t3 и t4 соответственно. Зная, что каждая приведенная система начинается с единицы, определим их начальные значения, как «1,». В цикле с параметром For .. Next будем перебирать все значения от двух до $bx-1$. В списки попадут только числа, взаимно простые с нашими модулями.

```
t1 = "1, "                          'Расчитываем первый ответ
For i = 2 To b1 - 1
  If НОД(i, b1) = 1 Then t1 = t1 + st(i) + ", "
Next i
t1 = NoSpase(Mid(t1, 1, Len(t1) - 2))

tz = NoSpase(Cells(28, 2))          'Читаем ответ и сравниваем с решением t1
If t1 = tz Then mark = mark + 1 Else Call krest(28, 2)

t2 = "1, "                          'Расчитываем второй ответ
For i = 2 To b2 - 1
  If НОД(i, b2) = 1 Then t2 = t2 + st(i) + ", "
Next i
t2 = NoSpase(Mid(t2, 1, Len(t2) - 2))

tz = NoSpase(Cells(28, 11))          'Читаем ответ и сравниваем с решением t2
If t2 = tz Then mark = mark + 1 Else Call krest(28, 11)

t3 = "1, "                          'Расчитываем третий ответ
For i = 2 To b3 - 1
  If НОД(i, b3) = 1 Then t3 = t3 + st(i) + ", "
Next i
t3 = NoSpase(Mid(t3, 1, Len(t3) - 2))

tz = NoSpase(Cells(31, 2))          'Читаем ответ и сравниваем с решением t3
If t3 = tz Then mark = mark + 1 Else Call krest(31, 2)

t4 = "1, "                          'Расчитываем четвертый ответ
For i = 2 To b4 - 1
  If НОД(i, b4) = 1 Then t4 = t4 + st(i) + ", "
Next i
t4 = NoSpase(Mid(t4, 1, Len(t4) - 2))

tz = NoSpase(Cells(31, 11))          'Читаем ответ и сравниваем с решением t2
If t4 = tz Then mark = mark + 1 Else Call krest(31, 11)
```

Рис. 8. Код проверки задания «4. Выписать приведенную систему вычетов».

Задания «5 Найти значение функции Эйлера» и «6. Решить сравнения» завершают программный комплекс «Сравнения» (рис. 9).

Рис. 9. Задания 5 и 6 программного комплекса «Сравнения».

Процесс генерации аргументов функции Эйлера по структуре похож на определение модулей из четвертого задания (рис. 10). Первые три значения b1, b2 и b3 берутся из указанных в коде интервалов, а переменные b4, b5 и b6 представляют собой произ-

ведение простых чисел в соответствующих степенях. Полученные значения проверяются на совпадения и указанные диапазоны.

```
Do
  b1 = Rnd(v) * 8 + 8
  b2 = Rnd(v) * 20 + 20
  b3 = Rnd(v) * 30 + 30
  b4 = Rnd(v) * 40 + 40
  b5 = 2 ^ (Int(Rnd(v) * 5 + 1)) * 3 ^ (Int(Rnd(v) * 4)) * _
           5 ^ (Int(Rnd(v) * 3)) * 7 ^ (Int(Rnd(v) * 2))
  b6 = 2 ^ (Int(Rnd(v) * 5 + 1)) * 3 ^ (Int(Rnd(v) * 4)) * _
           5 ^ (Int(Rnd(v) * 3)) * 7 ^ (Int(Rnd(v) * 2)) * _
           11 ^ (Int(Rnd(v) * 2)) * 13 ^ (Int(Rnd(v) * 2))
Loop Until b1 <> b2 And b1 <> b3 And b1 <> b4 And b1 <> b5 And b1 <> b6 _
       And b2 <> b3 And b2 <> b4 And b2 <> b5 And b2 <> b6 _
       And b3 <> b4 And b3 <> b5 And b3 <> b6 _
       And b4 < b5 And b5 < b6 _
       And b5 < 10000 And b6 < 10000
```

Рис. 10. Генерация задания «5. Найти значение функции Эйлера».

Процесс проверки пятого задания весьма лаконичен (рис. 11). Все представленные ответы сравниваются с со значение функции Euler(x), представленной в приложении 2.

```
If Val(Cells(35, 4)) = Euler(b1) Then mark = mark + 1 Else Call krest(35, 4)
If Val(Cells(35, 10)) = Euler(b2) Then mark = mark + 1 Else Call krest(35, 10)
If Val(Cells(35, 16)) = Euler(b3) Then mark = mark + 1 Else Call krest(35, 16)
If Val(Cells(37, 4)) = Euler(b4) Then mark = mark + 1 Else Call krest(37, 4)
If Val(Cells(37, 10)) = Euler(b5) Then mark = mark + 1 Else Call krest(37, 10)
If Val(Cells(37, 16)) = Euler(b6) Then mark = mark + 1 Else Call krest(37, 16)
```

Рис. 11. Код проверки задания «5 Найти значение функции Эйлера».

Наиболее интересен алгоритм генерирования и проверки задания «6. Решить сравнения». В начальном фрагменте программы для генерации (рис. 12) мы определяем модули для каждого из представленных сравнений. В этой части программного кода осуществляется проверка на идентичность значений и диапазонных ограничений.

```
Do
  b1 = Rnd(v) * 5 + 2
  b2 = Rnd(v) * 5 + 4
  b3 = Rnd(v) * 5 + 8
  b4 = Rnd(v) * 5 + 10
  b5 = Rnd(v) * 5 + 20
  b6 = 2 ^ (Int(Rnd(v) * 2 + 1)) * 3 ^ (Int(Rnd(v) * 2 + 1))
  b7 = 2 ^ (Int(Rnd(v) * 2 + 1)) * 3 ^ (Int(Rnd(v) * 2 + 1))
  b8 = 5 ^ (Int(Rnd(v) * 2 + 1)) * 7 ^ (Int(Rnd(v) * 2))
  b9 = 3 ^ (Int(Rnd(v) * 2 + 1)) * 5 ^ (Int(Rnd(v) * 2))
Loop Until b1 <> b2 And b1 <> b3 And b1 <> b4 And b1 <> b5 And b1 <> b6 _
       And b2 <> b3 And b2 <> b4 And b2 <> b5 And b2 <> b6 _
       And b3 <> b4 And b3 <> b5 And b3 <> b6 And b4 <> b5 _
       And b6 <> b7 And b8 <> b9 _
       And b6 < 30 And b7 < 40 And b8 < 60 And b9 < 60 _
       And b6 > 10 And b7 > 10 And b8 > 10 And b9 > 10
```

Рис. 12. Начальный фрагмент генерации задания «6. Решить сравнения».

Однако далее процесс формирования параметров задач и определения решений существенно отличается. Следует различать алгоритмы по трем типам: «только одно решение», «более одного решения» и «решений нет».

Тип сравнения «только одно решение» получается, если коэффициент при неизвестном и модуль взаимно просты. На рисунке 13 представлен код генерации такого задания.

```
'1 один корень
Do
  a = Rnd(v) * 8 + 2
  c = Rnd(v) * 8 + 2
  b1 = Rnd(v) * 5 + 3
Loop Until НОД(a, b1) = 1 And a <> c
Cells(41, 2) = a
Cells(41, 4) = c & " (mod " & b1 & ");"
```

Рис. 13. Код генерации сравнения типа «только одно решение».

Для сравнения второго типа «более одного решения» необходимо, чтобы наибольший общий делитель коэффициента при неизвестном и модуля был больше единицы, а свободный член делился на него (рис. 14).

```
'6 количество корней от двух до шести
Do
  a = Rnd(v) * 20 + 5
  b6 = Rnd(v) * 10 + 8
  d = НОД(a, b6)
  c = d * Int(Rnd(v) * 5 + 2)
Loop Until d > 1 And d < 7 And a <> c And a <> b6 And b6 <> c
Cells(45, 14) = st(a)
Cells(45, 16) = c & " (mod " & b6 & ");"

Do
  r1 = Int(Rnd(v) * 3)
  r2 = Int(Rnd(v) * 3)
  r3 = Int(Rnd(v) * 3)
Loop Until r1 = 2 Or r2 = 2 Or r3 = 2
```

Рис. 14. Код генерации сравнения типа «более одного решения».

И, наконец, сравнения третьего типа «решений нет» формируются в случае, если наибольший общий делитель коэффициента при неизвестном и модуля сравнения будет больше единицы, а свободный член на него не делится. Поскольку было бы неразумно делать у одних и тех же заданий ответ «решений нет», это будет известно всем обучаемым, то данный тип сравнения следует комбинировать с задания первого или второго типа в одном номере (рис. 15).

```
'9 несколько решений  или решений нет

If r3 = 0 Or r3 = 1 Then
  Do                    'r3 = 0, 1 несколько решений
    a = Rnd(v) * 20 + 5
    b9 = Rnd(v) * 10 + 8
    d = НОД(a, b9)
    c = d * Int(Rnd(v) * 10 + 2)
  Loop Until d > 1 And a <> c And a <> b9 And b9 <> c
                  Else
  Do                    'r3 > 1 решений нет
    a = Rnd(v) * 20 + 5
    b9 = Rnd(v) * 10 + 8
    d = НОД(a, b9)
  Loop Until d > 1 And a <> b9
  Do
    c = Rnd(v) * 20 + 2
  Loop Until c Mod d <> 0 And a <> c And b9 <> c
End If

Cells(49, 14) = st(a)
Cells(49, 16) = c & " (mod " & b9 & ")."
```

Рис. 15. Код генерации сравнения комбинированного типа.

Например, в пункте 9 шестого задания в случае r3=0 или r3=1 формируется задание с несколькими решениями, а при значении параметра r3>1 создается задание третьего типа «решений нет». Программа генерации составлена так, чтобы хотя бы одно из трех последних сравнений не имело решения.

При проверке решений мы используем значения, полученные при генерации задания. Например, при проверке решения девятого сравнения необходимо учитывать, что при решении мы можем получить несколько решений либо «решений нет». В этом случае мы простым перебором значений от нуля до $b9-1$, подставляя $b9$ в сравнение, проверяем истинность полученного выражения, тем самым формируя список решений сравнения. Если список содержит какие-либо значения, то решение записывается в виде строкового выражения: $t9+"(\mathrm{mod}"+st(b9)+")"$. В случае пустого списка решением является строка «решенийнет». Отсутствие пробела в ответе обусловлено тем, что из результата выполнения работы после считывания также удаляются все пробелы.

```
t9 = ""                                 'Находим решение девятого уравнения
For x = 0 To b9 - 1
  If a * x Mod b9 = (c + 10 * b9) Mod b9 Then t9 = t9 + st(x) + ", "
Next x
If t9 <> "" Then t9 = NoSpase(Mid(t9, 1, Len(t9) - 2))
If t9 <> "" Then t9 = t9 + "(mod" + st(b9) + ")" Else t9 = "решенийнет"
tz = NoSpase(Cells(51, 14))             'Читаем ответ и сравниваем с решением t3
If t9 = tz Then mark = mark + 1 Else Call krest(51, 14)
```

Рис. 16. Проверка сравнения комбинированного типа.

Описываемый в статье программный продукт успешно используются в учебном процессе Краснодарского университета МВД России при изучении дисциплины математика для проведения практических занятий с курсантами, обучающимися по специальностям 38.05.01 Экономическая безопасность и 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Литература

1. Булгаков, В.В. Структурно-методическая модель компьютерной программы контроля теоретических знаний курсантов /В.В. Булгаков // Открытое образование (Научный журнал). – М.: Российский экономический университет имени Г.В. Плеханова, 2018. – Том 22, №3. С. 4 – 13.

2. 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.

3. Лаптев, В.Н. Методы разработки тестовых заданий 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, 2015. – №09(113). С. 826 – 840. – IDA [article ID]: 1131509061. – Режим доступа: http://ej.kubagro.ru/2015/09/pdf/61.pdf, 0,938 у.п.л.

4. 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.

5. Лаптев, В.Н. О технологиях разработки программных приложений для генерирования и проверки практических заданий 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, 2020. – №01(155). С. 164 – 177. – IDA [article ID]: 1552001013. – Режим доступа: http://ej.kubagro.ru/2020/01/pdf/13.pdf, 0,875 у.п.л.

6. Лаптев, В.Н. О технологиях разработки программных приложений для генерирования и проверки практических заданий 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, 2020. – №02(156). С. 143 – 158. – IDA [article ID]: 1562002008. – Режим доступа: http://ej.kubagro.ru/2020/02/pdf/08.pdf, 1 у.п.л.

7. Михайленко, Е.В. О разработке программных приложений для генерации и проверки заданий к практикуму по разделу «Дискретная математика» дисциплины математика // Е.В. Михайленко // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2019. С. 20 – 27.

8. Михайленко, Е.В. К вопросу об использовании информационных технологий приорганизации самостоятельной работы обучающихся / Е.В. Михайленко, И.Н. Старостенко // Проблемы современного педагогического образования. – Сборник научных трудов. – Ялта: РИО ГПА, 2019. – Вып. 65. – Ч. 1. С. 257 – 262.

9. Михайленко, Е.В. Общие принципы автоматизации подбор заданий и проверки выполненных курсантами работ по математическим дисциплинам /Е.В. Михайленко // Математические методы и информационно-технические средства: материалы XIV Всерос. науч.-практ. конф., 21 июня 2019 г. / редкол.: И. Н. Старостенко, Е. В. Михайленко, С.К. Ефремов, А. А. Хромых. – Краснодар: Краснодарский университет МВД России, 2019. С. 122 – 127.

10. Крыгин, С.В. Особенности преподавания дисциплин информационного цикла при реализации программ дополнительного профессионального образования /С.В. Крыгин С.В., С.Н. Сухов // Передовой опыт и проблемы профилизации учебной, учебно-методической и научно-исследовательской деятельности в образовательных организациях системы МВД России: доклады участников Всерос. Науч.-практ. конф. – Нижний Новгород: Нижегородская академия МВД России, 2019. С. 156 – 162.

11. Жукова, П.Н. Использование информационных технологий в системе ведомственного образования на современном этапе (на примере БЕЛ ЮИ МВД России имени И.Д. Путилина) /П.Н. Жукова, А.Н. Прокопенко, А.А. Гуржий // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 4-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2018. С. 3 – 12.

12. Старостенко, И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

13. Старостенко, И.Н. Место и роль электронного обучения в образовательном процессе / И.Н. Старостенко // Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности. –

Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2016. –С. 17-23.

14. Старостенко, И.Н. Актуальные вопросы информатизации образования / И.Н. Старостенко // Общество и право. – Краснодар: Краснодарский университет МВД России, 2017. – №4 – С. 274-277.

Сведения об авторе

Михайленко Евгений Владимирович, кандидат физико-математических наук, доцент, заместитель начальника кафедры информатики и математики Краснодарского университета МВД России; e-mail: evmikhaylenko@mail.ru.

Нестеренко Иван Сергеевич

ОСОБЕННОСТИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В УСЛОВИЯХ ПАНДЕМИИ В ОБРАЗОВАТЕЛЬНЫХ СИСТЕМАХ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В процессе развития информационного общества большое значение имеют проблемные вопросы, касающиеся организации образовательного процесса в вузе. Современная система высшего образования должна быть способна не только вооружать знаниями обучающихся, но и вследствие постоянного и быстрого обновления информации формировать потребность в непрерывном самостоятельном овладении необходимыми и востребованными умениями и навыками самообразования, компетенциями, а также самостоятельной и творческой деятельности в течение всей активной жизни человека.

Для реализации данной концепции непрерывного образования достаточно актуальным становится дистанционное образование обучающихся всех возрастных категорий. Это обуславливается ещё и тем, что в нынешних карантинных условиях, дистанционная форма обучения является единственным приемлемым «спасительным» выходом из сложившейся кризисной ситуации для большинства образовательных систем. Поскольку посредством данной формы обучения курсанты и слушатели не только получают информацию, необходимую им для профессионального становления в той или иной сфере, но и приспосабливаются к самостоятельному процессу получения знаний, что во время пандемии является ценным навыком. Дистанционное обучение предопределяет главные условия эффективного образования, а именно его непрерывность и системность. Преимуществом дистанционного обучения выступает то обстоятельство, при котором любой курсант, применительно к образовательным организациям МВД РФ, находясь в отдалении от преподавателя, взаимодействует с ним, не упуская информации, являющейся значимой для последующего усвоения и закрепления им учебного материала.

В статье 16 Федерального Закона «Об образовании в Российской Федерации» (с изменениями, вступившими в силу с 1.09.2020 года), под дистанционным обучением понимается электронное обучение, которое в свою очередь представляет собой совокупный комплекс образовательной деятельности, где для большей степени эффективности применяются продукты научно-технического прогресса.

Дистанционное обучение обусловлено следующими факторами:

- большая территория государства;
- концентрация научно-технических центров в крупных населенных пунктах;
- появление новых потребностей у населения в непрерывном образовании;

- доминирование информационных технологий в образовательной сфере в период пандемии;

- миграция населения.

Наряду с вышеперечисленными факторами стоит добавить распространение эпидемии COVID-19 и введение карантина на территории страны. Данный фактор имеет особо важное значение, поскольку экстренное введение карантина позволило обнажить много различного рода проблем в системе образования всех уровней.

Ранее дистанционное обучение отождествляли с заочным обучением, однако это совсем две разные формы обучения. Выделить дистанционную форму в отдельную систему по сравнению с классическим вариантом заочной формы образования позволяет наличие ряда особенностей:

1) в дистанционной форме образования организуется непрерывный и интенсивный диалог между курсантом и преподавателем;

2) учебно-методический материал для данной формы образования позволяет усилить его деятельностную основу;

3) на основе адекватного учебно-методического материала осуществляется эффективное управление учебным процессом, которое становится возможным благодаря современным средствам коммуникаций;

4) при использовании дистанционной формы образования проявляется индивидуальный учебный компонент по сравнению с традиционным фронтальным обучением. Дистанционная форма – это форма личностно- ориентированного обучения с соответствующими прогрессивными педагогическими технологиями;

5) в дистанционной форме обучения проще организовать совместную работу с курсантами и слушателями: вебинары, конференции, семинары и обсуждения, вплоть до разработки обучающимися совместных проектов;

6) при дистанционной форме обучения сводятся к минимуму переезды, уменьшаются затраты сил, средств и времени;

7) дистанционная форма предоставляет возможность любому человеку обучаться в любом образовательном учреждении, у любого преподавателя вне зависимости от места его жительства и места расположения образовательного учреждения.

От традиционных же форм обучения дистанционное обучение отличают следующие характерные черты:

- гибкость – возможность заниматься в удобное для себя время, в удобном месте и темпе, когда обучающемуся предоставляется нерегламентированный отрезок времени для освоения учебной дисциплины;

- модульность – возможность из набора независимых учебных курсов формировать учебный план, отвечающий индивидуальным или групповым потребностям;

- параллельность – обучение без отрыва от производства, параллельное с профессиональной деятельностью;

- асинхронность – подразумевается, что в процессе обучения преподаватель и курсант могут реализовывать технологию преподавания и учения независимо во времени, т.е. по удобному для каждого расписанию и в удобном темпе;

- охват – одновременное обращение ко многим источникам учебной информации (электронным библиотекам, банкам данных, и т.д.) большого количества обучающихся;

- экономичность – эффективное использование учебных площадей, технических средств, транспортных средств;

- технологичность – применение в образовательном процессе вуза новейших достижений телекоммуникационных технологий, способствующих продвижению человека в мировое постиндустриальное информационное пространство;

- новая роль педагога – дистанционное обучение расширяет и обновляет роль преподавателя, который должен координировать образовательную деятельность, постоянно усовершенствовать преподаваемые им курсы, повышать свою квалификацию в соответствии с нововведениями и инновациями.

Н.В. Волженин систему дистанционного обучения (СДО) понимает совокупность организационных, телекоммуникационных, педагогических и научных ресурсов, вовлеченных в создание и практическое осуществление образовательных программ с использованием дистанционной технологии обучения. Организационно СДО состоит из координирующих органов, исследовательских организаций, базовых учебных заведений дистанционного обучения (ответственных за дистанционное обучение структурных подразделений), сети вузов и учебных центров дистанционного образования.

Реализация дистанционного обучения в Краснодарском университете МВД России среди лиц как постоянного, так и переменного состава, приняло особую актуальность в условиях распространения вируса «COVID-19». Начиная с 27 марта 2020 года, для образовательных организаций МВД РФ было принято решение о необходимости роспуска всех курсантов и слушателей по местам жительства, в которых они непосредственно зарегистрированы. Как следствие, обучение в период всего карантина осуществлялось дистанционно посредством специально созданной электронной образовательной среды, которая включала в себя следующие компоненты:

- система управления учебным процессом (СУУП) «Магеллан», с помощью которого преподаватели и обучающиеся находятся в курсе расписания, возможных замен. Удобство от пользования «Магелланом» состоит также в реализации обратной связи, обусловленной тем, что курсанты могут в любой момент времени увидеть полученную на учебном занятии оценку;

- корпоративный портал «Битрикс24», предназначение которого заключается в том, что с помощью него производится организация внутренней работы вуза МВД РФ. Характерной чертой «Битрикс24» является то, что курсанты и слушатели, располагая индивидуальными данными, необходимыми для входа в систему, могут свободно пользоваться электронными лекциями, которые представлены как в текстовом, так и видео формате. Также, посредством «Битрикс24», преподаватели способны в экстренном порядке уведомить обучающихся о той или иной перестановке занятий, не учтенной в расписании;

- электронная библиотека вуза, предусматривает беспрепятственный доступ представителей как постоянного, так и постоянного состава к литературе, необходимой для изучения конкретной дисциплины;

- СУО «Moodle» представляет собой платформу, способствующую организации дистанционного обучения, избегая, при этом, значительного ущерба, выраженного в виде пробелов знаний, обучающихся по той или иной дисциплине. Данная платформа является, своего рода, личным кабинетом каждого преподавателя и курсанта, где последний, в свою очередь, может проследить степень готовности заданий, заранее размещенных профессорско-преподавательским составом. Кроме этого, посредством данной платформы курсанты и слушатели могут в свободном порядке воспользоваться лекционным материалом, который, по усмотрению преподавателя, выкладывается в «Moodle».

Большинство респондентов (91,5%) достаточно быстро освоили продукты информационно-образовательной среды, под которой понимается работа в системе «Moodle», где курсанты получали и загружали задания. 8% респондентов разобрались не сразу и только у 1,5 % респондентов возникли трудности с использованием данной платформы. Данные свидетельствуют об эффективности использования данной платформы для дистанционного обучения в условиях пандемии.

Хотелось бы заострить внимание на видео-конференцсвязи, посредством которой проводились первоначально все занятия (Zoom, TrueConf). Стоит отметить, что по результатам опроса, проведенного в ноябре 2020 года среди курсантов и слушателей вуза МВД РФ, 45% опрошенных отдавали предпочтение именно Zoom, объясняя это удобством пользования, выраженного в возможности курсантов и слушателей, не имеющих ноутбуки или компьютеры, подключиться к семинарскому или практическому занятию, тем самым, избежав пропуска по неизвестной причине. Данная программа просуществовала недолго, вскоре ее эксплуатация была запрещена в электронно-образовательных платформах, применяющихся в образовательных системах МВД. Также, 35% опрошенных высказались о преимуществе такого электронного девайса, который носил название «TrueConf». Преимущество данного видео-сервиса также заключалось в проведении дистанционных занятий, максимально приближенным к реальным условиям. Следующим, на этапе становления дистанционного обучения в образовательной организации МВД РФ, следует выделить облачную платформу для проведения вебинаров BigBlueButton (далее «BBB»), систему, которая получила самый низкий процент голосов среди опрошенных, численно равный 16%. На наш взгляд, подобная разница достаточна справедлива, поскольку «BBB», по сравнению с двумя вышеупомянутыми видео-платформами, обладает значительными недостатками. Во-первых, посещение семинарских или практических занятий с телефона фирмы IPhone, не поддерживается. Во-вторых, видеосвязь, осуществляемая посредством «BBB», зачастую зависает, что исключает нормальный ритм проведения занятий, поскольку приходится тратить время на то, чтобы перезагрузить компьютер или ноутбук в случае возникшего системного сбоя. Среди опрошенных, были респонденты, которые затруднились дать ответ на заданный вопрос, процентная составляющая их была равна 4% от общего числа всей выборки.

Как правило, у большинства людей складывается мнение о том, что прохождение обучения в дистанционной форме проще, чем в очной (в нашем исследовании 92% респондентов хотели бы продолжить обучатся в данном режиме). Достаточно двоякий вывод, ведь с одной стороны, дистанционное обучение действительно легче дается обучающимся, ведь они располагают возможностью самостоятельно планировать время, им не приходится осуществлять затраты на проезд. С другой стороны – сложность дистанционного обучения заключается в процессе самоорганизации курсантов и слушателей, так как процесс обучения в дистанционном формате расслабляет последних, позволяет им откладывать выполнение того или иного задания в долгий ящик. Дистанционное обучение – это направление, которое надо развивать, поскольку оно достаточно эффективно в условиях, диктуемых нынешними реалиями жизни.

Литература

1. Алексеев В.М., Ильченко С.В. Особенности современного дистанционного обучения контрактных управляющих // Актуальные проблемы гуманитарных и естественных наук. 2016. № 9-1. С. 168-171.

2. Каширин А.Н. Организационно-педагогические условия развития инновационно-образовательных процессов в колледже: дис.канд.пед.наук: 13.00.01/ Каширин А.Н. Тамбов, 2007.

3. Лишманова Н.А., Пимичева М.А. Дистанционное обучение и его роль в современном мире // Научнометодический электронный журнал «Концепт». – 2016. – Т. 11. – С. 2216–2220. – URL: http://ekoncept.ru/2016/86472.htm.

4. Полат Е.С, Моисеева М.В., Петров А.Е. Педагогические технологии дистанционного обучения / Под ред. Е.С. Полат. – М., «Академия», 2006.

5. Приказ МВД РФ от 23.06.2006 N 497 «О внедрении Системы дистанционных образовательных технологий в образовательных учреждениях МВД России».

6. Тихонов А.Н., Иванников А.Д. Технологии дистанционного обучения [Текст] // А.Н. Тихонов, А.Д. Иванников. Высш. образование в России – 1994. № 3.

7. Фролова Т.М. Оптимизация учебно-методического обеспечения образовательного процесса в вузе МВД России на основе современных информационных технологий: дис. канд. пед. наук: 13.00.01 / Фролова Т.М.

8. Шерстяных А.С. Дистанционное образование: проблемы организации учебного процесса // Вестник Сибирского юридического института: научно-практический журнал. – Красноярск: СибЮИ МВД России, 2009.

9. http://novaum.ru/public/p374.

Сведения об авторе

Нестеренко Иван Сергеевич, кандидат педагогических наук, доцент кафедры информатики и математики Краснодарского университета МВД России.

Прокопенко Алексей Николаевич,
Жукова Полина Николаевна,
Гусев Юрий Михайлович

К ВОПРОСУ О ПОДГОТОВКЕ СОТРУДНИКОВ ПОЛИЦИИ, РАСКРЫВАЮЩИХ ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Активное использование информационных технологий в жизни людей, внедрение цифровых технологий во все аспекты жизни общества, принципиально изменяет в последнее десятилетие весь мир. Данный процесс получил название цифровой трансформации и особенно активно происходит в финансовой и бизнес сферах. Также наблюдается почти полное перемещение определенных видов преступной деятельности в киберпространство. К ним относятся создание и распространение детской порнографии, торговля оружием и людьми, незаконный оборот наркотиков, вовлечение лиц в экстремистскую и террористическую деятельность, финансовое мошенничество и другие виды преступной деятельности. В последние годы активно развивается мошенничество с использованием сотовой связи, а также средств IP-телефонии.

До короновирусной пандемии количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ), постоянно росло, примерно на 30-40% в год. Однако, с 2018 года наметился просто лавинообразный рост такого типа преступлений. Это связано, как с нерегулируемостью многих направлений деятельности в киберпространстве, так и с анонимностью большинства действий.

Наметившаяся тенденция была выявлена в МВД России, и министр В.А. Колокольцев на коллегии министерства 1 ноября 2019 года обратил внимание на новые угрозы в Интернет, а также перемещения преступных деяний в сеть [1]. Соответственно, было принято решение о создании в структуре министерства подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием ИТТ, общей численностью более четырех тысяч человек. Поскольку подразделения были созданы по отраслевому принципу в пределах тех штатных единиц, которые имеются в центральном аппарате министерства и территориальных органах внутренних дел, то возникла необходимость подготовки сотрудников [2].

Кроме того, Владимиром Владимировичем Путиным на расширенной коллегии МВД России 26 февраля 2020 года была дополнительно поставлена задача по сниже-

нию количества противоправных действий в Интернет, в том числе по незаконному распространению наркотиков [3].

Поскольку большая часть сотрудников, специализирующихся на противодействии преступлениям, совершаемым с использованием ИТТ, являются оперативными сотрудниками с базовым юридическим образованием, они не готовы к выполнению поставленных руководством страны и министерства задач. В этой связи для уже действующих сотрудников проводятся курсы повышения квалификации или переподготовка. Можно выделить, например, обучение, организованное ДГСТ МВД России, проводимое Университетом Банка России в полностью дистанционном формате, которое прошли тысячи сотрудников полиции.

Однако, для сотрудников, которые поступают на службу, представляется необходимым получение специальных знаний технического характера на этапе профессиональной подготовки или высшего образования.

В этих целях в октябре 2020 года Департаментом государственной службы и кадров было принято решение о подготовке сотрудников по различным специальностям, связанным с противодействием преступлениям, совершаемым с использованием ИТТ. Преимущественно данные специалисты должны иметь юридическое образование по специальности 40.05.02 Правоохранительная деятельность для специализации – оперативно-разыскная деятельность органов внутренних дел. При этом получение технических знания является для них дополнительной составляющей в рамках узкой специализации.

Белгородскому юридическому институту МВД России имени И.Д. Путилина поручено участвовать в подготовке сотрудников полиции указанной специализации по очной форме обучения для узкой специализации противодействие незаконному обороту наркотиков в сфере информационно-телекоммуникационных технологий. Также институтом планируется проведение повышений квалификации для действующих оперативных сотрудников полиции по направлению выявление и раскрытие преступлений, совершаемых с использованием ИТТ.

В ходе подготовки к реализации новой узкой специализации коллективами кафедр информационно-компьютерных технологий и оперативно-розыскной деятельности были подготовлены предложения в проект учебного плана, а совместно с факультетом переподготовки и повышения квалификации – проекты программ повышения квалификации. Также была разработана и утверждена программа повышения квалификации «Противодействие незаконному обороту наркотиков в сфере информационно-телекоммуникационных технологий» в объеме 60-ти часов по которой планируется обучение профессорско-преподавательского состава и сотрудников института.

В этой связи мы предлагаем коллегам из других образовательных организаций МВД России ознакомится с предложенным нами подходом по обучению оперативных сотрудников, противодействующих преступлениям в сфере ИТТ.

Запланированные для изучения учебные дисциплины информационного блока представлены в таблице 1. Ряд учебных дисциплин изучается всеми обучающимися по специальностям 40.05.01 Правовое обеспечение национальной безопасности и 40.05.02 Правоохранительная деятельность. К таким учебным дисциплинам относятся «Информатика и информационные технологии в профессиональной деятельности», «Делопроизводство и режим секретности в органах внутренних дел», «Правовая статистика». Кроме того, для всех обучающихся по указанным специальностям с 2021 года набора вводится новая учебная дисциплина «Основы кибербезопасности». Данная учебная дисциплина должна объединить в себе наработанный опыт кафедры по преподаванию учебной дисциплины «Основы информационной безопасности» и новые подходы именно по кибербезопасности.

Также для всех обучающихся преподается учебная дисциплина «Информационные системы и технологии органов внутренних дел», которая для вновь вводимой специализации трансформируется в учебную дисциплину «Информационные системы и технологии органов внутренних дел в сфере контроля за оборотом наркотиков». На указанной дисциплине будет изучаться использование информационных технологий в деятельности органов внутренних дел, унифицированное прикладное обеспечение обработки информации, системы телекоммуникаций, сервисы и ресурсы в деятельности органов внутренних дел в целом и подразделений по контролю за оборотом наркотиков, в частности.

Семь учебных дисциплин будут преподаваться только на вновь вводимой узкой специализации. Три из них являются обязательными дисциплинами вариативной части учебного плана, одна – дисциплиной по выбору (элективной), а еще три будут преподаваться в качестве факультативов.

На учебной дисциплине «Естественно-научные основы противодействия незаконному обороту наркотиков» (факультатив) будут изучаться медико-биологические аспекты влияния на организм человека наркотических средств, физико-химические свойства наркотических средств и методы их детектирования, основы обработки результатов естественнонаучных наблюдений (математическая статистика и теория вероятностей).

Таблица 1

Учебные дисциплины информационного блока подготовки специалистов НОН ИТТ

№ п/п	Семестр	Название учебной дисциплины	Часы					Вид промежуточной аттестации
			Всего	Ауд.	Лекц.	ПЗ	Сем.	
1.	1,2	Информатика и информационные технологии в профессиональной деятельности	216 (108+ 108)	130 (60+ 70)	14+ 18	38+ 48	8+ 4	зачет, экзамен
2.	2	Делопроизводство и режим секретности в органах внутренних дел	72	40	14 (6)	12 (8)	14 (6)	зачет
3.	2	Естественно-научные основы противодействия незаконному обороту наркотиков (факультатив)	72	40	10	26	4	зачет
4.	4	Основы кибербезопасности	72	40	10	20	10	зачет
5.	6	Правовая защита информации	72	50	20	10	20	зачет
6.	6	Основы операционных систем (факультатив)	72	40	6	28	6	зачет
7.	6-7	Выявление и фиксация цифровых следов при раскрытии преступлений сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий	144 (72+ 72)	80 (40+ 40)	16 (6+ 10)	48 (28 + 20)	16 (6+ 10)	зачет (6 сем.) зачет, практикум (7 сем.)
8.	7	Основы компьютерных сетевых технологий (факультатив)	72	40	6	28	6	зачет
9.	8	Использование информационных	72	40	10	22	8	зачет

		технологий в противодействии незаконному обороту наркотиков						
10.	8	Правовая статистика	72	30	8	22		зачет практикум
11.	10	Информационные системы и технологии органов внутренних дел в сфере контроля за оборотом наркотиков	72	50	10	30	10	зачет
12.	10	Применение компьютерных методов и средств для противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий	144	84	10	64	10	экзамен, практикум

На учебной дисциплине «Основы операционных систем» (факультатив) будут изучаться существующие операционные системы, их принципиальные различия. Также будут рассмотрены возможности редактора реестра и показаны возможные уязвимости операционных систем. Кроме того, будут изучаться способы ограничения доступа к работе компьютера и способы ограничения доступа к файлам и папкам.

На учебной дисциплине «Основы компьютерных сетевых технологий» (факультатив) будут изучаться основные понятия компьютерных сетей, а также архитектура вычислительной сети и сетевое взаимодействие. Также будут рассмотрены принципы организации Интернет, порядок функционирования социальных сетей, Интернет-магазинов, мессенджеров и т.д. Кроме того, будут изучаться особенности функционирования системы Интернет платежей, майнинг, криптовалюты и другие виды электронных финансовых активов.

На учебной дисциплине «Правовая защита информации» будет изучаться правовое регулирование информации, информационных отношений, информационной сферы. Также будут рассмотрены основы оборота документированной информации и особенности правового регулирования Интернет. Кроме того, будут изучаться виды конфиденциальной информации и правовые основы их защиты. Отдельным направлением в учебной дисциплине будет изучение дисциплинарной, административной и уголовной ответственности за нарушения законодательства в информационной сфере.

На учебной дисциплине «Выявление и фиксация цифровых следов при раскрытии преступлений сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий» будут изучаться основные мероприятия по предупреждению, пресечению и реагированию на компьютерные инциденты. Также будет изучаться порядок исследования компьютерной техники и элементов инфраструктуры в целях снятия цифровой информации, извлечение данных из мобильных устройств. Отдельно будут рассматриваться методы и средства исследования компьютерных систем, выявление сетевых аномалий при сетевых взаимодействиях.

На учебной дисциплине «Использование информационных технологий в противодействии незаконному обороту наркотиков» будут изучаться поиск информации с использованием поисковых систем сети «Интернет», методика получения значимой информации, получение данных из открытых источников информации, программно-технические средства сбора данных.

Учебная дисциплина «Применение компьютерных методов и средств для противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий» аккумулирует знания и умения, полученные при изучении предыдущих дисциплин. Учебный процесс будет организован путем выполнения сквозных интегрированных заданий по сбору информации из различных источников, определения следообразования, собранной информации; обработка полученной информации для деаннонимизации объектов исследования. При наличии программно-технических средств криминалистических исследований (UFED, «Мобильный криминалист»), будут проведены занятия по извлечению и анализу информации из мобильных устройств.

Представляется, что подход, предложенный в Белгородском юридическом институте МВД России имени И.Д. Путилина будет интересен коллегам, которые будут осуществлять подготовку сотрудников аналогичных категорий. Причем речь идет не только о специализации НОН ИТТ, но и о подготовке всех категорий сотрудников, деятельность которых направлена на раскрытие преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Литература

1. В России за три года в три раза выросла IT-преступность, заявили в МВД. Сайт «РИА НОВОСТИ». [Электронный ресурс]. Режим доступа: https://ria.ru/20191210/1562205715.html (дата обращения – 10.05.2021).

2. Волженин В.В. К вопросу о квалификации, раскрытии и расследовании преступлений, предусмотренных статьей 273 УК РФ // Вестник науки и образования. 2019. № 24-2. С. 52-55.

3. Выступление Президента России Владимира Путина на коллегии МВД России 26.02.2020. Сайт «Президент России». [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/events/president/transcripts/62860 (дата обращения – 10.05.2021).

Сведения об авторах

Прокопенко Алексей Николаевич, кандидат технических наук, доцент, начальник кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

Жукова Полина Николаевна, доктор физико-математических наук, доцент, профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

Гусев Юрий Михайлович, заместитель начальника кафедры огневой подготовки Белгородского юридического института МВД России имени И.Д. Путилина.

Путилов Артур Олегович

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ КИБЕРАТАК

Одним из важнейших ресурсов современной организации, который находится под угрозой утечки, является информация. Информация постоянно подвергается угрозе неконтролируемого распространения (утечки). Применение комплексной системы защиты информации (КСЗИ) позволяет защитить её от разглашения и несанкционированного доступа. КСЗИ представляет собой комплекс инженерно-правовых и организационных мероприятий.

Главными целями применения средств информационной защиты является обеспечение стабильного функционирования учреждений и организаций, а также принятие превентивных мер по отношению к потенциальным угрозам безопасности информации.

К основным задачам комплексной системе защиты информации можно отнести следующие задачи:

- своевременное выявление и ликвидация угроз элементам критической инфраструктуры информационной безопасности;
- пресечение возможных попыток получения доступа к конфиденциальной информации, передаваемой по каналам связи;
- резервное копирование банков информации, утрата которых существенно влияет на устойчивое функционирование учреждений;
- анализ актуального состояние информационной инфраструктуры и формирование перечня рекомендаций по изменению ее внешней и внутренней среды;
- регенерация поврежденных информационных систем.

Все угрозы информационной безопасности можно разделить на внешние и внутренние угрозы.

Внешние угрозы (или кибератаки) затрагивают физическую и интеллектуальную собственность и представляют собой реальную опасность.

В большинстве случаев киберпреступления совершаются с применением специализированного программного обеспечения. Функционал подобных программ содержит разнообразные возможности нарушения целостности документов ограниченного доступа.

Вредоносное программное обеспечение провоцирует широкий перечень угроз. К таковым относятся:

- внедрение вирусов, дестабилизирующих работу программных компонентов;
- распространение системных утилит, исследующих сетевой трафик;
- программная блокировка действий пользователей системы;
- преодоление программной защиты с целью получения несанкционированных прав, нарушения целостности или удаление информации.

Практика показывает, что существенная часть инцидентов спровоцирована так называемыми внутренними угрозами.

Действия сотрудников могут привести к утечке коммерческой тайны, хищению интеллектуальной собственности и в целом нанести ущерб информационной системе. Подобные действия могут иметь место, как по корыстным мотивам, так и в связи с неосторожностью сотрудников из-за их недостаточной некомпетентности.

Информационную безопасность можно обеспечить с помощью:

- предотвращения сетевых вторжений IDS/IPS;
- межсетевого экранирования Firewall;
- двухфакторной аутентификацией пользователей;
- защиты передачи данных VPN;
- криптографической защиты.

К защите сетевого периметра относится большой класс программно-аппаратных решений для организации, предоставляющих возможности защиты доступа к корпоративной сети извне. Наряду с межсетевыми экранами к нему можно отнести системы обнаружения и предотвращения вторжений (IDS/IPS), а также шлюзы безопасности. Кроме того, с целью защиты внешних коммуникаций используется технология организации виртуальных частных сетей (VPN), которая помогает обеспечить зашифрованную передачу информации, исключая возможность доступа к ней лиц, не имеющих на это право.

В заключение следует отметить, что достижение эффективного уровня защиты информации возможно только при условии тщательной настройки соответствующих программных и аппаратных решений, их своевременного обслуживанию и должного использования в комплексе с другими мерами обеспечения информационной безопасности.

Литература

1. Кибератака как современная форма совершения акта агрессии. Латынина К.Р. В сборнике: Студенческая наука: взгляд молодых. Материалы студенческой научно-практической конференции. Министерство науки и высшего образования Российской Федерации, Майкопский государственный технологический университет. 2019. С. 106-109.

2. Интеллектуальные системы предотвращения кибератак. Бирюков Д.Н., Ломако А.Г., Петренко С.А. В сборнике: The 2019 Symposium on Cybersecurity of the Digital Economy - CDE'19. Третья международная научно-техническая конференция. 2019. С. 184-195.

3. Мировой опыт противодействия кибератакам. Левшук О.И.В книге: Борьба с преступностью: теория и практика. Тезисы докладов VIII Международной научно-практической конференции. Могилев, 2020. С. 104-107.

4. Кибератаки в инфотелекоммуникационных сетях. Левин Ю.В., Худайназаров Ю.К., Митрофанов М.В., Алмаев Т.Ю. В книге: Нейрокомпьютеры и их применение. XVII Всероссийская научная конференция. Тезисы докладов. 2019. С. 80-81.

Сведения об авторе

Путилов Артур Олегович, старший преподаватель кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий, Московский университет МВД России имени В.Я. Кикотя.

Разбегаев Павел Витальевич

ЭЛЕКТРОННОЕ ОБУЧЕНИЕ КАК ФАКТОР ПОВЫШЕНИЯ КАЧЕСТВА ОБРАЗОВАНИЯ

В настоящее время активно протекает процесс информатизации общества, в связи с чем, система образования подвержена реформированию. Наиболее развивающимся ее направлением становится реализация образовательных программ с применением методов электронного обучения, использованием компьютерной техники и информационных технологий [2].

Электронное обучение – это 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.

Электронное обучение в настоящее время становится наиболее удобным и быстрым видом обучения. Это связано, например, с тем, что руководители различных организаций могут осуществлять обучение работников, в кратчайшие сроки и, не отходя от рабочего места, тем самым экономя время. К тому же, результаты исследований подтверждают, что электронное обучение способствует лучшему усвоению материала, а также в два раза повышается скорость обучения. С финансовой точки зрения электронное обучение также является более выгодным, так как не требует особых затрат, в связи с чем, заметна экономия бюджета примерно на 80%. Положительным моментом явля-

ется то, что для всех учащихся предоставляется единый стандартизированный учебный материал, а также имеется возможность проверки знаний обучающихся в электронном виде.

Исходя из вышеизложенных положительных аспектов электронного обучения, представляется возможным сформулировать цели электронного обучения. Во-первых, это обеспечение доступности образования, эффективности и его качества, во-вторых, предоставление необходимых условий для обучения с учетом возможных особенностей психофизического развития и здоровья обучающихся, в том числе обучения по индивидуальному учебному плану.

Широкое использование электронного обучения, компьютерной техники и информационных технологий, связанных с ней, привело к тому, что практически любая сфера деятельности человека совершенствуется в области информатизации различных процессов. Логично, что компьютеры заняли свою нишу и в области образования. Информационные средства и технологии осваиваются и успешно применяются во всех образовательных организациях, начиная с дошкольных и заканчивая высшими учебными заведениями. Педагога получили возможности применять информационные технологии как непосредственно в процессе объяснения учебного материала обучающимся, так и при решении различных задач, касающихся организации обучения. В конечном итоге, основной целью разработки и использования электронных технологий в образовательной деятельности является повышение эффективности учебного процесса.

Рассмотрим электронные средства обучения, как основной элемент электронных (информационных) технологий.

Электронные средства обучения долгое время воспринимались как некое дополнительное вспомогательное средство, облегчающее педагогическую деятельность. Постепенное устойчивое внедрение в этот процесс новых информационных технологий, связанное с распространением компьютерной техники, породило новые направления информатизации педагогической деятельности. Целый ряд процессов стал информатизированным. Средства же, преобразовавшие таким образом образовательные процессы, получили название «программированные педагогические средства», «компьютерные учебные средства», «учебные компьютерные программы».

Приведем классификацию электронных средств обучения.

1. Электронное издание [1] – это электронный информационный источник. По сути - аналог традиционного «бумажного».

Разница заключается только в том, что «бумажное» издание не содержит в себе ничего, кроме текста (графических изображений), электронное издание же может включать в себя различные анимационные фрагменты, звук, видео или музыку. Различна также технология предъявления материала. Если в книгах – это бумажный лист, то электронное издание иллюстрирует материал на экране компьютера. При желании, его можно легко перенести на бумагу, например, распечатав на принтере. Текст может быть произвольно разбит на фрагменты, а ознакомление с содержанием производиться в удобном для пользователя порядке. Навигация по тексту электронного издания нелинейная.

2. Электронный учебник – это информационная система комплексного назначения [3]. Данная система обеспечивает реализацию возможностей средств информационно-коммуникационных технологий на всех этапах процесса обучения. Это процесс становится возможным без применения бумажных носителей информации и обеспечивается посредством единой компьютерной программы.

Электронный учебник в обязательном порядке осуществляет подачу учебного материала, постановку познавательной задачи, организует выполнение заданий, формирующих научные знания. Применяя данный вид электронного средства обучения, педа-

гог поддерживает обратную связь с обучающимися и контролирует их деятельность. И хотя предназначение электронного учебника полностью совпадает с обычным, их содержание разнится. Так, электронный учебник включает в себя кроме сугубо теоретического материала, еще и наглядный материал (что особенно повышает его методическую ценность в сравнении с обычным учебником), практические примеры, задачи, методические рекомендации для обучающихся.

С учетом того, что эффективность электронного учебника превосходит обычный (ввиду применяемых технологий), такой вид учебного издания разработан и широко используется при освоении образовательных программ среднего, высшего и дополнительного профессионального образования.

Изложенное обусловлено возможностью использования современных компьютерных технологий, таких как мультимедиа и гипермедиа.

3. Программные средства.

Их применение способствует эффективному усвоению учебного материала, так как обращения через гиперссылки к видеоматериалу, изображениям, звуковому сопровождению позволяют обучающемуся продуктивно пользоваться содержащимся в учебнике материалом. В конечном итоге, это способствует выбору индивидуального подхода к обучению, учитывая все перечисленные факторы.

Одна из основных функций любых видов программных средств - подача учебного материала в разнообразных формах, стимулирующих и инициирующих процессы усвоения знаний, приобретения умений и (или) навыков учебной или практической деятельности. Это является основой формирования и развития определенного вида мышления обучающихся, активизируется их познавательная деятельность. При этом педагог имеет возможность эффективно осуществлять контроль как за самим процессом. так и за результатом обучения. Если возникает такая необходимость, то педагог организует повторение теоретической части пройденного учебного материала и его практической составляющей. Данные программные средства реализуются с помощью мультимедийных технологий.

В учебных целях программные средства используются для решения фундаментальных задач. Во-первых, они оказывают помощь в развитии навыков и умений, которые могли бы пригодиться для принятия наиболее оптимальных решений в реальных ситуациях, связанных с какими-либо сложностями или рисками. Во-вторых, использование программных средств способствует грамотному и планомерному формированию навыков самостоятельной работы обучающихся, например, работы с информацией и вычленение наиболее полезных ее сегментов. И, наконец, применение учебных программ в учебном процессе позволяет осуществлять контроль обучающегося за своими действиями с возможностью корректировки полученных результатов (самокоррекции).

Характерной особенностью программных средств является то, что в них широко используются возможности компьютерной графики. Это позволяет повысить степень наглядности материала; усилить контроль и самоконтроль овладения учебным материалом, используя контролирующие программные средства; сформировать необходимые умения и навыки для выбора «нужной» информации из общего массива и ее систематизации, ориентируясь на поставленные задачи, применяя информационно-поисковые (справочные) программные системы.

Исходя из указанного, можно сделать вывод, что электронная среда обучения, на основе которой происходит взаимодействие обучаемого и педагога, а также разнообразие технических и программных средств обучения позволяют повысить качество организации, а также эффективность учебного процесса

Литература

1. Карпенко Е.Р., Лузянина Т.В. Использование электронных обучающих материалов для развития языковых навыков и умений //Материалы XVIII-й Всероссийской научно-практической конференции «Актуальные проблемы филологии и методики преподавания иностранных языков. Ставрополь, 2020.

2. Разбегаев П.В. Основные дискуссионные проблемы электронного обучения. // Математические методы и информационно-технические средства: материалы XV Всерос. науч._практ. конф., 21 июня 2019 г. / ред. кол. И.Н. Старостенко (отв. ред.), Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2019.

3. URL: https://moluch.ru/archive/117/32109/ (дата обращения 11.06.2021).

Сведения об авторе

Разбегаев Павел Витальевич, кандидат педагогических наук**,** доцент, начальник кафедры информатики и математики Волгоградской академии МВД России**;** email: pavel173@mail.ru.

Серезевский Алексей Вадимович

РАЗРАБОТКА И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ФОРМУЛЬНЫХ ПОДСТАНОВОК ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА СОСТАВЛЕНИЯ УЧЕБНЫХ ЗАДАЧ ПО ДИСЦИПЛИНЕ «ФИЗИКА»

Автоматизация процесса составления учебных задач по дисциплине «Физика» в настоящее время имеет высокий уровень значимости для преподавателей, поскольку мы живём в эпоху стремительного распространения информации и любая однажды решённая задача практически сразу становится достоянием общественности через всемирную систему объединенных компьютерных сетей для хранения и передачи информации Интернет.

Теоретически составить задач по дисциплине «Физика» можно сколь угодно много, очень сложно оценить пределы возможных генераций. При этом процесс составления задач достаточно трудоёмкий. Задавшись вопросом получения всевозможных комбинаций исходных переменных, автором статьи всесторонне была рассмотрена идея автоматизировать процесс получения всевозможных формул из некоторого начального заданного списка формул, попутно вычисляя их количество, поскольку на каждой такой формуле можно построить уникальное текстовое условие задачи и предложить её ученику для решения.

Рассмотрим следующий пример. Пусть нам необходимо получить всевозможные формулы для составления задач на кинематику броска тела вертикально вверх в поле силы тяжести, при этом тело достигает наивысшей точки подъёма и падает в ту же самую точку, откуда было брошено.

Перечислим сопутствующие физические величины:

v_0 - начальная скорость тела;

g - ускорение свободного падения;

h - максимальная высота подъема тела;

$t_{\text{под}}$ - время движения тела от момента броска до достижения им наивысшей точки подъёма;

S - путь, пройденный телом от момента броска до момента падения;

v - скорость тела в момент времени, предшествующий соприкосновению его с поверхностью;

$t_{пад}$ - время движения тела от наивысшей точки подъёма до момента падения.

Рассмотрим минимальный состав связывающих данные величины формул:

$$h = \frac{v_0^2}{2g},\ \ t_{под} = \frac{v_0}{g},\ \ S = 2h,\ \ v = \sqrt{2gh},\ \ t_{пад} = \sqrt{\frac{2h}{g}}.$$

Выполняя попарное сравнение этих формул можно находить в них одинаковые переменные и, выражая их, приравнивать между собой, упрощая выражение и получая таким образом новую, более сложную формулу. Добавляя полученную формулу в этот же список можно продолжать аналогичные действия получая всё новые и новые формулы. И так, на первый взгляд, до бесконечности. Однако есть некоторые ограничения, которые приводят к конечности результата. Во-первых, необходимо проверять каждую вновь полученную формулу на то, чтобы множество входящих в неё переменных не являлось ни подмножеством, ни надмножеством любого множества переменных из одной из уже имеющихся формул в текущий момент перебора. Во-вторых, необходимо понимать, что количество переменных в формуле не может превышать определённого значения, которое определяется как количество так называемых задающих переменных, увеличенное на единицу.

Понимание задающих и вычисляемых переменных рассмотрим на примере. Количество задающих переменных должно быть изначально минимизировано таким образом, чтобы все остальные (вычисляемые) можно было определить через задающие. В нашем примере это v_0 - начальная скорость тела и g - ускорение свободного падения. Остальные переменные вычисляются по формулам, приведённым выше. Процесс разделения переменных на задающие и вычисляемые, а также составление формул целиком и полностью «ложится на плечи» методиста, который составляет задачи. Здесь пока не удалось получить чётких правил, поэтому этот процесс на данном этапе автоматизировать не представляется возможным, чего нельзя сказать о процессе получения новых формул, о котором было написано выше: автором статьи успешно была осуществлена программная реализация данного алгоритма на языке Python и апробирована на более чем 75 различных формульных комбинациях для различных физических ситуаций. Например, для рассматриваемого выше примера броска тела алгоритмом было получено за несколько секунд ещё 61 формула к 5 имеющимся. Ручная проверка, на которую ушло несколько часов, показала аналогичный результат. В некоторых случаях алгоритм получает несколько тысяч формул, в зависимости от количества переменных, на что уходит порой до нескольких десятков минут. Вручную и без ошибок получить такое количество формул не представляется возможным.

На основе полученных формул, которым автоматически присваивается некоторый уровень сложности в виде числового значения, происходит дальнейшее составление текстовых условий задач с вариацией числовых значений. В настоящее время реализован и пока тестируется алгоритм получения сложности каждой вновь получаемой формулы на основе ручного присваивания исходным формулам уровня сложности в виде целого чисел от 0 до 10 и в процессе слияния формул эти числа суммируются. Также реализован алгоритм автоматического получения текстового условия задачи из формул на основе текстового описания всех переменных в именительном и винительном падежах, о чём будет подробно описано в последующих статьях, касающихся данного исследования.

Сведения об авторе

Серезевский Алексей Вадимович, кандидат технических наук, начальник кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя; email: serezev@yandex.ru.

Старостенко Игорь Николаевич,
Епифанцева Виктория Александровна

ОТ ЦИФРОВИЗАЦИИ К ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ: ДРАЙВЕРЫ РАЗВИТИЯ

Характерной чертой современного мира является исключительно высокая скорость происходящих изменений в окружающей среде. Во многом эти изменения связаны с распространением цифровых технологий в организациях основных отраслей экономики и социальной сферы.

В Указе президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» определены пять основополагающих целей, определяющих стратегию развития страны на ближайшие десять лет. Одна из них – это цифровая трансформация (ЦТ). В качестве целевых показателей ЦТ указаны достижение цифровой зрелости ключевых отраслей экономики и социальной сферы, в том числе образования; увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95%; рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к интернету, до 97%; увеличение в четыре раза вложений в отечественные решения в сфере информационных технологий по сравнению с показателем 2019 года [1].

Необходимым условием для понимания сущности ЦТ является анализ предпосылок возникновения этого процесса. К первой предпосылки относится смена технологического уклада и переход к Индустрии 4.0. Четвертая промышленная революция предполагает масштабную перестройку процессов производства и управления, заключающуюся в переходе на полностью автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени, в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия/организации, с перспективой объединения в единую сеть вещей и услуг. В условиях Индустрии 4.0 обмен обратной связью между поставщиком и потребителем мгновенен и динамично влияет на изменение услуги, ее параметры и опции. Обратная связь может стать одним из ключевых драйверов развития системы в целом. Переход к новой модели происходит тогда, когда не менее 40% операций по отрасли осуществляются в цифровом виде. Второй предпосылкой ЦТ является развитие существующих и появление новых цифровых технологий. Примерами таких технологий являются робототехника, микроэлектроника, Интернет вещей, системы распределенного реестра, быстрая беспроводная связь и другие доступные цифровые технологии. Третья предпосылка – развитие инфраструктуры, без которой невозможна ЦТ и переход к инновационной деятельности. Важными составляющими этой предпосылки являются увеличение распространенности мобильных устройств, рост скорости передачи данных, увеличение процента подключенных к сети Интернет. Четвертая предпосылка – рост объема данных. Объем данных в мире ежегодно возрастает на 30%. По прогнозам к 2025 году объем всей совокупности созданных, собранных и воспроизведенных данных во всем мире может вырасти до 160-170 зеттабайт. Если в прошлом основной рост объемов данных происходил за счет неструктурированных данных, создаваемых пользователями всевозможных социальных сред с помощью различных электронных устройств, то в ближайшем будущем основным источником данных будет являться Интернет вещей. Основной объем данных будут производить компании: на промышленность и другие сферы экономики придется до 60% всех данных мира. К росту объема данных приводит увеличение вычислительных мощностей, разработка технологий анализа, хранения и обработки данных, интеллектуализация систем, развитие нейросетей и искусственного интеллекта.

Предпосылки ЦТ сами по себе не являются цифровой трансформацией, но являются составными частями этого процесса и делают этот процесс возможным. Первым этапом на пути к цифровой трансформации является автоматизация – перевод существующих процессов в digital-формат. Проекты автоматизации направлены на создание внутренней информационной системы для автоматизации и повышения эффективности внутренних процессов, целей и ресурсов. Внедрение информационных систем не приводит к кардинальным изменениям, но создаёт предпосылки для частичного или полного перехода на онлайн-взаимодействие. На следующем этапе (этап цифровизации) происходит улучшение существующих процессов путем внедрения информационных технологий, оптимизации и реинжиниринга, а также анализа данных для принятия решений. Переведенные в digital-формат данные и процессы уже можно использовать для упрощения и оптимизации операций. Проекты цифровизации ориентированы на создание или функциональное расширение имеющейся информационной системы, использование цифровых технологий на платформенных решениях. При реализации цифровых проектов кардинальных изменений не происходит. Перевод на онлайн-взаимодействие только части клиентов не позволяет значительно перестроить существующие процессы, поменять цели и схемы использования ресурсов. Результаты автоматизации и цифровизации служат основой для ЦТ. На этапе ЦТ происходит глубокое и комплексное преобразование существующих процессов с широким применением цифровых решений и технологий. Такая реорганизация приводит к существенному улучшению характеристик процессов (сокращение времени выполнения, затрачиваемых ресурсов, исчезновение посреднических подпроцессов) и/или появлению их принципиально новых качеств и свойств, открывает возможность для создания и реализации принципиально новых стратегий. Реализация цифровой трансформации во многих случаях происходит как выполнение ряда связанных между собой проектов. Это могут быть проекты автоматизации, цифровые проекты и проекты цифровой трансформации. Некоторые проекты могут проходить все стадии эволюции: начинаясь как проект автоматизации, постепенно переходит в стадию цифрового и на определенном этапе становится трансформационным. Проекты ЦТ направлены на создание или расширение платформенных решений, которые предназначены для кардинального изменения системы отношений между участниками взаимодействия. Примером проекта ЦТ является портал и мобильное приложение «Наш город», разработанные для выстраивания конструктивного диалога между жителями Москвы и органами исполнительной власти города. Данное решение позволило оптимизировать работу служб приема жалоб от населения сразу нескольких ведомств, синхронизировать их работу между собой и организовать взаимодействие с помощью цифрового решения.

Образование традиционно считается крайне консервативной сферой, но и оно под влиянием внешних факторов, связанных в первую очередь с информационными и коммуникационными технологиями, претерпевает значительные изменения [2]. Ландшафт инноваций в образовании становится всё более разнообразным и сложно структурированным. К ключевым направлениям цифровой трансформации образовательной системы относятся развитие цифровых сервисов, модернизация инфраструктуры, управление данными и кадровым потенциалом.

Деятельность в направлении развития цифровых сервисов связана с персонализацией обучения и преодолением цифрового разрыва. Персонализация обучения предполагает не только накапливание знаний, но и развитие способности учиться, ориентироваться в большом информационном потоке, оценивать актуальность знаний и навыков в текущий момент и адаптироваться к изменениям, которые могут произойти за время обучения. Основным трендом персонализации образовательной траектории обучающихся должно стать использование технологии искусственного интеллекта (ИИ).

Эффективное использование ИИ, данных и аналитики, а также машинного обучения должны позволить преподавателям повысить эффективность своей деятельности и создать идеальные условия для обучения и развития учащихся. ИИ будет играть важную роль и в осуществлении персонализированной оценки знаний. Способность ИИ не только осваивать и проверять огромные объемы данных, но и устанавливать связи между разрозненными источниками данных поможет обучающимся выявить те сферы, в которых им потребуется взаимодействие в режиме реального времени или дополнительная помощь. В результате ИИ позволяет разработать индивидуальную образовательную траекторию для каждого обучающегося с учетом его сильных и слабых сторон, способностей и поставленных задач.

Еще один характерный тренд нынешнего времени – использование технологий виртуальной и дополненной реальности и геймификация образовательного процесса.

Виртуальная реальность (VR) полностью погружает пользователя в виртуальную среду, созданную компьютером. Технологии виртуальной реальности способны обеспечить свободу передвижения: пользователи могут перемещаться в цифровой среде, слышать звуки и использовать специальные ручные контроллеры для ориентации в пространстве и воспроизведения тактильных ощущений.

В дополненной реальности (AR) пользователи по-прежнему могут видеть реальный мир и взаимодействовать с ним, одновременно просматривая цифровой контент, доступ к которому обеспечивают специальные очки или гарнитуры, накладывающие цифровой контент на реальную среду.

Смешанная реальность объединяет виртуальные объекты с реальным миром. Пользователь может не только просматривать цифровой контент, но и взаимодействовать с виртуальными объектами, которые могут находиться в реальной среде.

Основное направление для развития VR и AR в образовании заключается в возможности этих технологий погружать человека в виртуальный мир. Все то, что крайне затруднительно или невозможно создать в реальном мире, может быть воспроизведено в мире виртуальном: визуализация алгебраических поверхностей второго и более высоких порядков, электрических и магнитных полей, проведение лабораторных работ в современных лабораториях, моделирование наиболее известных исследовательских проектов, знакомство с трехмерными экспонатами музеев мира, воссоздание древних городов, битв или других исторических событий и др. Такой вид обучения позволяет лучше воспринимать и понимать окружающую действительность, способствует повышению вовлеченности, коммуникаций между обучаемыми и интереса к образовательному процессу.

Согласно исследованиям немецкого психолога Германа Эббингауза в процессе обучения среднестатистический обучающийся через час забывает около 40% изученного материала, через день – 60%, в течение месяца – 90%. Эффективным средством снижения скорости забывания изученного материала является микрообучение. Это еще один ключевой тренд современного образования, заключающийся в представлении образовательного контента малыми блоками. Каждый блок посвящен конкретной, очень узкой тематике, программа обучения делится на модули и реализуется в формате «1 модуль – 1 мысль – 1 навык». Модули микрообучения значительно короче, тем традиционные электронные курсы, обучение требует меньше времени, мотивация к обучению выше. Возможность многократного повторения информация позволяет обучающимся лучше запоминать важную информацию. Кроме того, разработка микрокурсов не требует значительных временных и финансовых ресурсов.

Существующие программные продукты для создания микрокурсов (например, онлайн-конструктор iSpring Page или сервис для микрообучения TalentCards), позволяют любой тип электронного контента (обучающие видео, подкасты, скринкасты, лон-

гриды, презентации, сценарии и задания) представить в формате микрообучения и создавать не только отдельные микромодули, но и полноценные микрокурсы.

Среди самых сильных трендов современного образования – популяризация мобильного обучения. Мобильное обучение (M-learning) позволяет получать доступ к знаниям в любой момент времени через мобильные технологии, например, смартфоны или планшеты. По оценкам экспертов в 2020 году объём мирового m-learning составил $38 млрд. К 2024 году, при прогнозном среднегодовом темп роста в пределах 15-20%, величина рынка может достигнуть $70 млрд. Микрообучение является популярной разновидностью мобильного обучения. Учебный контент разбивается на небольшие сегменты и инкапсулируется в различные форматы. Каждая единица контента самодостаточна, является частью всей системы обучения. В каждом блоке обучающийся осваивает отдельный микронавык, отрабатывает его с помощью практических упражнений или тренажеров. Обучение гармонично интегрировано в учебный процесс и доступно с любых устройств. Мобильные устройства для реализации этого алгоритма подходят идеально. Обучающиеся скачивают мобильное приложение, изучают теоретический материал, выполняют практические задания и тесты, могут общаться между собой, с преподавателями, вести совместную работу над проектами. Возможности микрообучения и мобильного обучения могут быть ограничены только функционалом приложения.

Таким образом, реализация проектов в рамках цифровой трансформации образования подразумевает изменение подходов к организации работы и повышение эффективности процессов функционирования образовательных организаций, изменение характера взаимодействия между всеми участниками данных отношений. Развитие и внедрение проектов позволит предоставить равный доступ к качественному образовательному контенту и цифровым образовательным сервисам для всех категорий обучающихся. По мере развития информационных систем и цифровых сервисов будет решаться задача создания модели цифрового университета, позволяющая сформировать единую экосистему сервисов и услуг с разнообразным персонализированным верифицированным цифровым контентом и построением индивидуальных образовательных траекторий обучающихся на основе обработки данных с помощью интеллектуальных алгоритмов.

Литература

1. Указ президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

2. Старостенко И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257-262.

3. Старостенко И.Н. Цифровая трансформация образовательного процесса в период пандемии COVID-19 / И.Н. Старостенко // Математические методы и информационно-технические средства: Материалы XVI Всероссийской научно-практической конференции, Краснодар, 19 июня 2020 года. – Краснодар: Краснодарский университет МВД России, 2020. – С. 100-105.

4. Караваев Н.Л. Совершенствование методологии геймификации учебного процесса в цифровой образовательной среде / Н.Л. Караваев, Е.В. Соболева. – Киров: Вятский государственный университет, 2019. – 105 с.

5. Шрайберг Я.Л. Формирование единого пространства знаний на базе сетевой информационной инфраструктуры в условиях становления и развития современной цифровой экономики Ежегодный доклад Четвёртого международного профессионального форума «Крым-2018» / Я.Л. Шрайберг // Научные и технические библиотеки. – 2018. – № 9. – С. 3-75.

6. Старостенко И.Н. О некоторых аспектах оптимизации образовательного процесса с использованием информационных технологий / И.Н. Старостенко // Математические методы и информационно-технические средства: Труды VI Всероссийской научно-практической конференции, Краснодар, 25 июня 2010 года – Краснодар: Краснодарский университет МВД России, 2010. – С. 183-189.

Сведения об авторах

Старостенко Игорь Николаевич, кандидат физико-математических наук, доцент, начальник кафедры информатики и математики Краснодарского университета МВД Росси; e-mail: staros80@mail.ru.

Епифанцева Виктория Александровна; преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: torohova_viktori@mail.ru.

Телков Александр Юрьевич

ЗАЩИТА HTTP ТРАФИКА СВЯЗИ ОПЕРАТОРА С УЗЛОМ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ОТКРЫТОГО РЕШЕНИЯ ELK STACK

В период пандемии аналитиками отмечается рост количества кибератак от прогосударственных хакерских групп и киберкриминала, эксплуатирующих тему COVID-19, с использованием шпионского программного обеспечения, шифровальщиков, бэкдоров. Отмечаются факты поиска злоумышленниками способов проникновения в сети предприятий с использованием адресных атак сотрудников, работающих удаленно, путем заражения их компьютеров вредоносными программами, через которые затем был получен доступ к сервисам корпоративных сетей. Кроме традиционного пути заражения компьютеров с помощью электронных писем, в ряде случаев имело место проникновение в информационные системы через корпоративные сервисы удаленного доступа путем подбора паролей учетных записей VPN, удаленных рабочих столов, служб ssh и др. [1].

В [2] описаны основные этапы совершения киберпреступления, которые, в общем случае, подразумевают: разведку и сбор данных; выбор способа атаки; доставку; эксплуатацию; закрепление; исполнение команд; достижение цели. Практически на каждом из этапов совершения кибератаки она потенциально с высокой вероятностью может быть обнаружена правильно настроенными подсистемами защиты компонент атакуемой информационной системы или соответствующими сетевыми средствами мониторинга безопасности провайдера услуг связи – системами обнаружения вторжений, антивирусами, анализа содержимого и т.п.

С учетом разнородного характера информации, на основе анализа которой могут быть сделаны выводы о наличии вредоносного кода или вредоносной активности, в сетях средних и крупных масштабов применяют системы управления событиями информационной безопасности, так называемые SIEM [3]. Положительные примеры мировой практики применения подобных систем позволяют говорить о внушительном списке проверенных решений: IBM QRadar Security Intelligence, Splunk Enterprise Security, McAfee Enterprise Security Manager, AlienVault Unified Security Platform, Micro Focus ArcSight Enterprise Security Manager, RSA NetWitness Platform, FireEye Helix Security Platform, Rapid7 insightIDR, Fortinet FortiSIEM, MaxPatrol SIEM, RuSIEM, SIEM KUMA и единая модульная платформа лаборатории Касперского и др. По состоянию на июнь 2021 г. на сайте ФСТЭК России в Государственном реестре сертифицированных

средств защиты информации имеется порядка 10 продуктов, в составе названий которых фигурирует аббревиатура SIEM.

Одним из направлений, стабильно набирающих популярность в практике обеспечения кибербезопасности информационных систем, выступает использование стеков программных решений с открытым исходным кодом для операционных систем семейства Линукс. Примером такого решения является ELK Stack, для которого необходима длительная и тонкая настройка механизмов получения информации со всевозможных источников событий безопасности, но при этом имеется обширный гибкий функционал для основных задач, возложенных на SIEM. ELK Stack содержит отдельные подсистемы, наличие которых характерно для любой SIEM: подсистема нормализации логов Logstash, подсистема хранения логов Elasticsearch и подсистема отображения данных Kibana. В общем случае работа системы в нужном функционале достигается настройкой всех трех подсистем и дополнительной настройкой агентов сбора информации с источников событий.

Однако, в известных вариантах ELK Stack, распространяющихся с открытым исходным кодом, отсутствуют средства безопасного сетевого доступа к компоненту отображения данных Kibana. Сервис работает на порту 5601 TCP и доступен по открытому протоколу http. Данный факт ставит под сомнение возможность применения системы ELK Stack в таком виде в сетях малого и среднего масштаба даже для целей обучения.

Для исключения возможности компрометации информации, передаваемой по протоколу http между оператором и узлом мониторинга событий информационной безопасности, предлагается на том же узле, на котором выполняется компонент Kibana из набора ELK Stack, настроить web-сервер nginx в роли обратного прокси-сервера с одновременным запретом прямых соединений к компоненту отображения данных Kibana по сети по протоколу http. Фактически, это приведет к необходимости разрешения взаимодействия службы 5601 TCP между службами локального хоста с установленными SIEM и nginx по протоколу http и необходимости запрета обращений к порту 5601 TCP по сети по протоколу http. Взамен этого по сети к узлу SIEM оператору потребуется обращаться по защищенному протоколу https.

Таким образом, предлагаемая методика защиты сеанса связи между оператором и системой отображения данных Kibana в стеке программных решений ELK Stack, настроенного в роли SIEM, заключается:

во-первых, в переходе от незащищенного протокола http к защищенному протоколу https при распределенном сетевом взаимодействии за счет обратного проксирования сетевого соединения с помощью web-сервера nginx;

во-вторых, в добавлении процесса аутентификации пользователя при обращении к странице отображения данных средствами утилит базовой аутентификации web-сервера nginx;

в-третьих, в настройке правил межсетевого экрана на узле с SIEM, принуждающих оператора пользоваться протоколом https при сетевом взаимодействии.

Данная методика может быть реализована поэтапно на узле с установленным компонентом Kibana после применения следующих шагов:

1. Установка web-сервера nginx и настройка обращений к нему по сети по протоколу https и порту 443 TCP;

2. Настройка web-сервера nginx в режиме обратного прокси-сервера, который подразумевает сетевое взаимодействие с оператором по протоколу https на серверном порту 443 TCP и локальное взаимодействие с компонентом Kibana по протоколу http на серверном порту 5601 TCP;

3. Настройка базовой аутентификации на web-сервере nginx с помощью web-утилиты htpasswd;

4. Установка на узел с web-сервером nginx и компонентом Kibana службы межсетевого экрана iptables и последовательное добавление в начало цепочки input нескольких правил: разрешение сетевых подключений на порт 443 TCP с допустимых IP адресов, разрешение подключений к порту 5601 TCP службам локального узла, запрет подключений к порту 5601 TCP с любых адресов, запрет подключений к порту 443 TCP с любых адресов.

Поскольку просмотр и интерпретация правил межсетевого экрана начинается сверху вниз, указанная цель принуждения использования протокола https при сетевом взаимодействии вместо http будет достигнута за счет п. 4 приведенного списка шагов. Необходимость аутентификации пользователя обеспечивается п. 3.

На рис.1 для примера показан вид окна аутентификации при доступе к компоненту Kibana по сети по протоколу https.

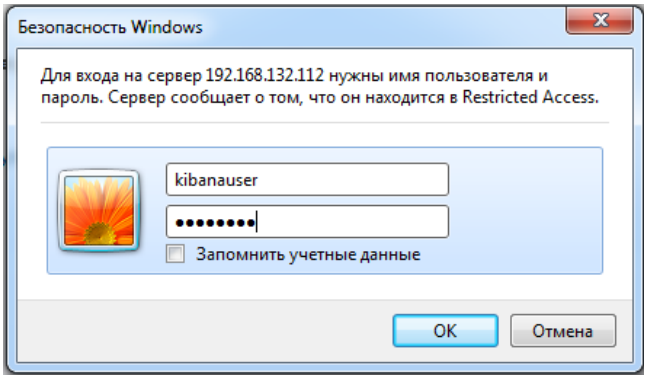


Рис.1. Аутентификация пользователя при доступе к компоненту отображения данных через web-обозреватель по сети.

На рис. 2 показан фрагмент данных «информационной доски», связанных с отображением факта сетевой атаки на протокол удаленных рабочих столов Windows Server.

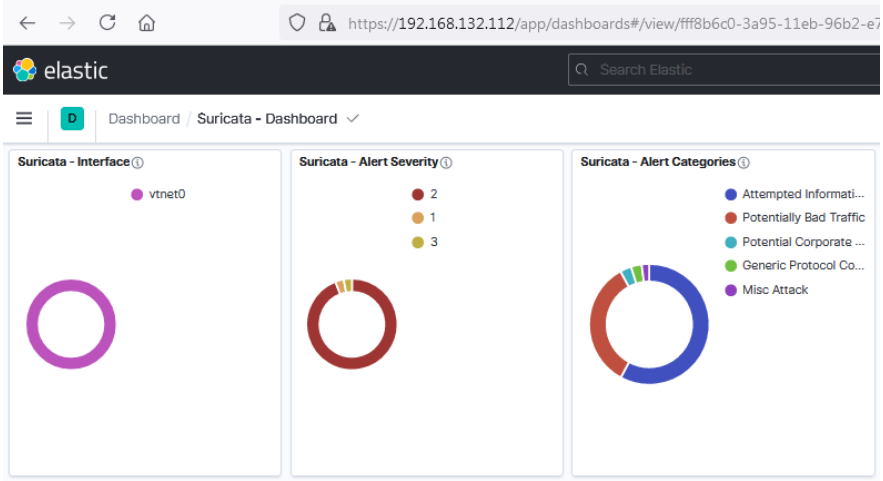


Рис.2. Фрагмент «информационной доски» с отображением результатов детектирования сетевой атаки crowbar из инструментария Kali.

Данная атака формировалась с помощью программы crowbar из инструментария операционной системы Kali Linux и детектировалась с помощью системы обнаружения вторжений suricata, установленной в транзитном программном маршрутизаторе pfsense. Отправка данных в ELK Stack обеспечивалась с помощью программного пакета syslog-ng и происходила в формате JSON. Как видно из рис. 2, просмотр данных обеспечивается по безопасному протоколу https.

Таким образом, предложена и проиллюстрирована методика перехода от незащищенного протокола http при сетевом доступе к странице отображения данных SIEM компонента Kibana стека программ ELK Stack к протоколу https с предварительной аутентификацией пользователя, настроенной с помощью утилит web-сервера nginx, работающего в режиме обратного прокси сервера.

Литература

1. HI-TECH CRIME TRENDS 2020/2021. Отчет компании Group-IB об изменении вектора кибератак в 2020/2021 гг. Доступен на официальном сайте компании по запросу. – URL:https://www.group-ib.ru/resources/threat-research/2020-report.html

2. Руководство по реагированию на инциденты информационной безопасности. - URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2017/08/12170645/Incident_Response_Guide_rus_2021.pdf

3. Обзор мирового и российского рынка SIEM-систем. - URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem

Сведения об авторе

Телков Александр Юрьевич, кандидат физико-математических наук, доцент, доцент кафедры компьютерной безопасности и технической экспертизы Воронежского института МВД России; e-mail: telkov@phys.vsu.ru.

Хромых Анна Алексеевна
Старостенко Игорь Николаевич

ОБ ОПЫТЕ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНОГО КЛАССА CLASSROOM ДЛЯ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Для организации дистанционного обучения курсантов и слушателей, обучающихся по специальностям 10.05.05 Безопасность информационных технологий в правоохранительной сфере и 38.05.01 Экономическая безопасность, в Краснодарском университете МВД России на кафедре информатики и математики используется виртуальный учебный класс – Google Classroom [4, 5].

Класс – это бесплатный сервис для учебных заведений и некоммерческих организаций. Также он доступен всем, у кого есть личный аккаунт Google. Благодаря Классу общение учащихся и преподавателей выходит на новый уровень и не ограничивается пределами аудитории. В нем можно создавать курсы, раздавать задания, общаться и систематизировать работу [1, 2].

Для перехода в Класс используется соответствующая иконка (рис. 1).

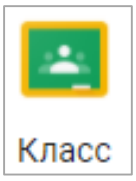


Рис. 1. Иконка Google Classroom.

В классе преподаватели могут создавать учебное курсы, куда могут выкладывать задания и публиковать объявления как для групп, так и для каждого курсанта в отдельности (рис. 2).

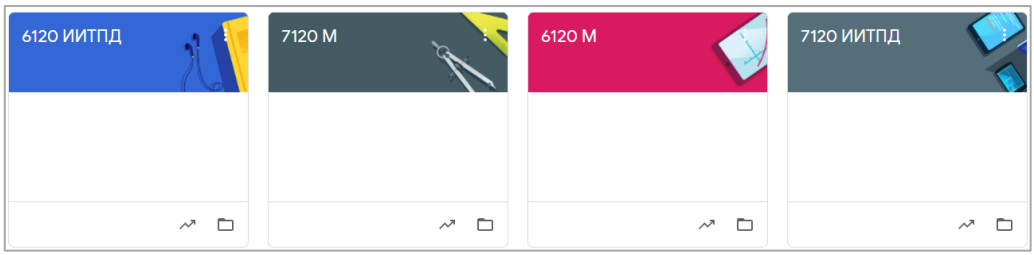


Рис. 2. Учебные курсы.

Присоединиться к учебному курсу курсанты и слушатели могут через приглашение от преподавателей по электронной почте, по ссылке или с помощью кода (рис. 3).

Рис. 3. Код доступа к курсу.

Каждый курс содержит ленту, задания, пользователей, оценки (рис. 4).

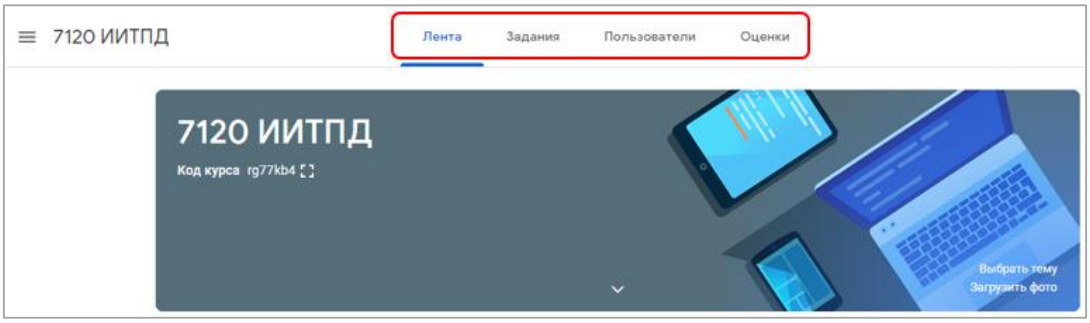


Рис. 4. Элементы курса.

Вкладка Лента выступает как соцсеть (рис. 5). Здесь преподаватель может делиться информацией как со всем курсом, так и с каждым курсантом в отдельности.

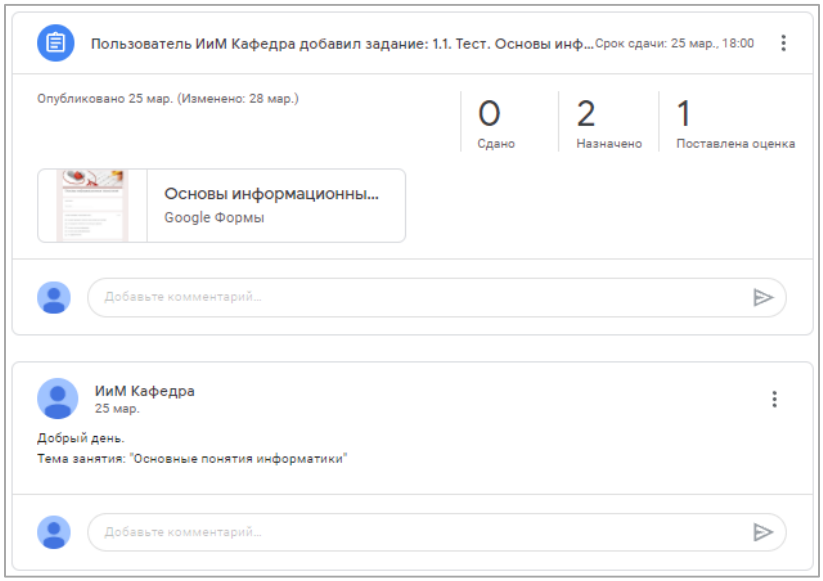


Рис. 5. Элемент Класса Лента.

Во вкладке Задания преподаватель может выкладывать задания по каждой теме изучаемой дисциплины (рис. 6).

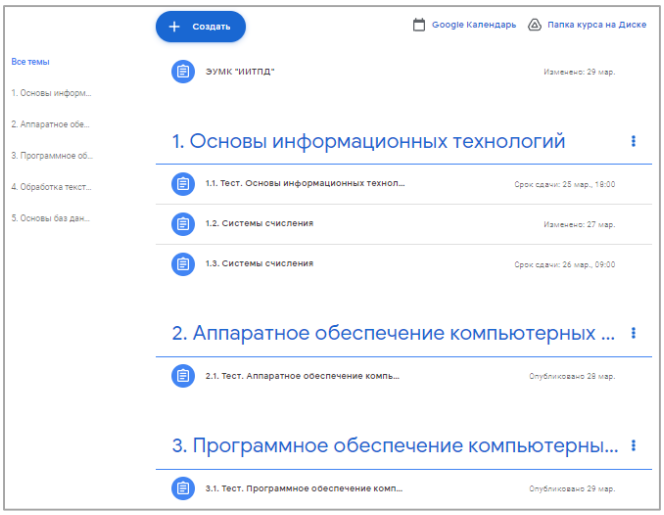


Рис. 6. Элемент Класса Задания.

Задания могут быть в виде различных прилепленных материалов, файлов, в виде теста или вопроса (рис. 7).

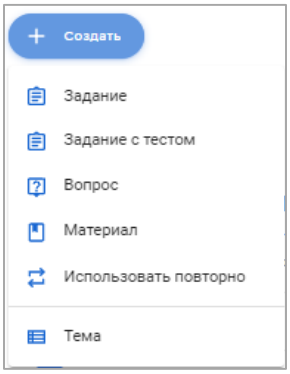


Рис. 7. Виды заданий

При добавлении задания указывается срок опубликования, т.е. когда откроется доступ к соответствующему материала; срок сдачи задания; критерий оценивания. Если курсанты и слушатели отправят выполненное задание по истечению срока сдачи, то преподаватель увидит сообщение «Пропущен срок сдачи». Работы, выполненные курсантами и слушателями, могут проверяться автоматически, если указан критерий, а также вручную преподавателем (рис. 8).

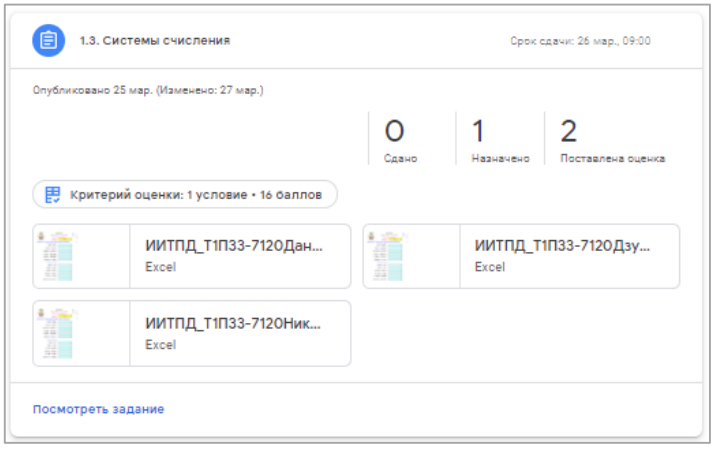


Рис. 8. Окно результатов.

Во вкладке Пользователи располагается список всех курсантов (рис. 9).

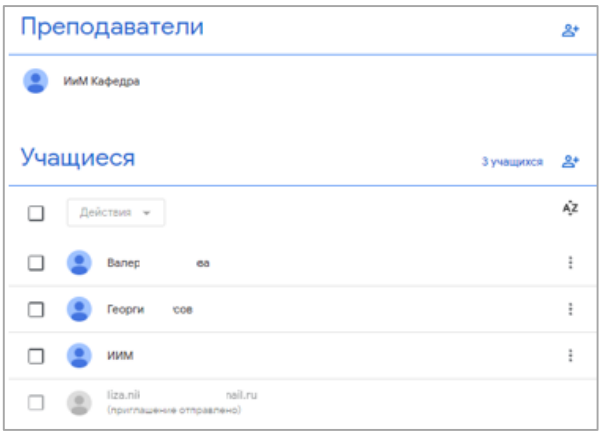


Рис. 9. Элемент Класса Пользователи.

Выбрав определенного курсанта, можно получить детальную информацию о выполненных им заданиях (рис. 10).

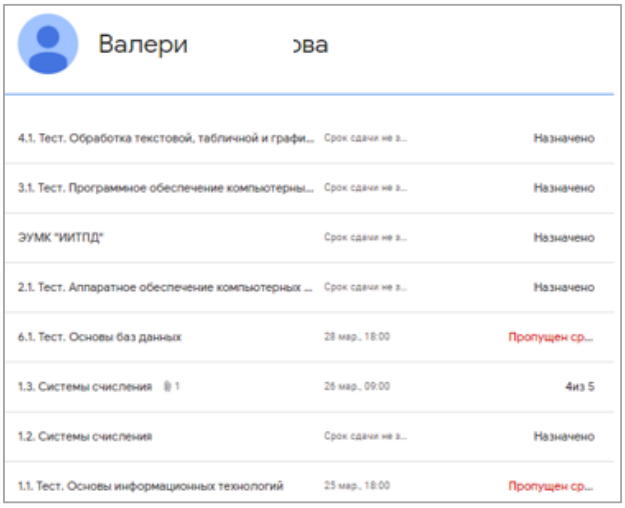


Рис. 10. Информация о работах курсанта.

Во вкладке Оценка фиксируется детальная информация о выполненных курсантами работах. Информацию можно получить как вертикально по каждому заданию, так и горизонтально каждому курсанту (рис. 11).

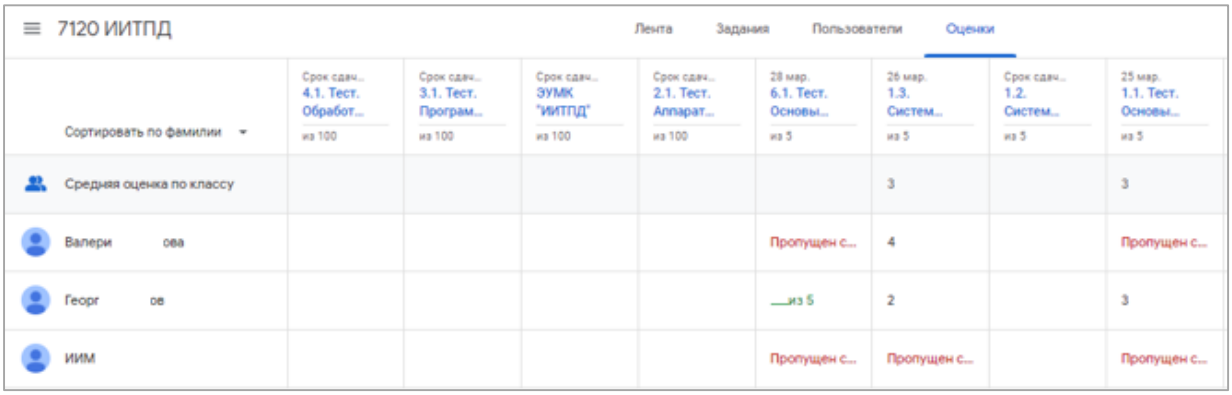


Рис. 11. Элемент Класса Оценки

Удобство представленного класса заключается в том, что все материалы, выкладываемые преподавателем, хранятся в одном месте на виртуальном диске недоступном курсантам и слушателям.

Благодаря используемой платформе Google, в которой был создан Classroom, особых требований к компьютерной системе не предъявляется и имеется возможность использования электронных учебно-методических материалов для дистанционного обучения в любом аппаратном и программном окружении, имеющем браузер [3].

Литература

1. Епифанцева В.А. Использование цифровых образовательных ресурсов в учебном процессе в условиях реализации ФГОС нового поколения: опыт, проблемы // В.А. Епифанцева // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина, – 2019. С. 210 – 214.

2. Епифанцева В.А. Технология создания электронного портфолио Краснодарского университета МВД РФ / В.А. Епифанцева, А.А. Хромых // Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 7 Всерос. науч.-практ. конф., 21 мая 2021 г. /ред. кол.: И.Ф. Амельчаков, И.Н. Озеров, В.Л. Акапьев, А.Н. Прокопенко, В. А. Насонова. – Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2021.

3. Епифанцева В.А. Онлайн обучение – необходимость или эволюция образования в целом / В.А. Епифанцева, А.А. Хромых // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Международной научно-практической конференции (22 мая 2020 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2020. С. 104 – 106.

4. Старостенко И.Н. Актуальные вопросы информатизации образования // Общество и право. 2017. № 4 (62). С. 274-277.

5. Хромых А.А. Технология разработки электронного образовательного ресурса по дисциплине «Математика» / А.А. Хромых, И.Н. Старостенко // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 7-й Всероссийской научно-практической конференции. – Белгород. Белгородский юридический институт МВД России им. И.Д. Путилина: Белгородский юридический институт МВД России имени И.Д. Путилина, 2021.

Сведения об авторах

Хромых Анна Алексеевна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: AnnXA@mail.ru.

Старостенко Игорь Николаевич, кандидат физико-математических наук, доцент, начальник кафедры информатики и математики Краснодарского университета МВД Росси; e-mail: staros80@mail.ru.

Содержание

Акапьев В.Л., Прокопенко А.Н., Савотченко С.Е. Математические аспекты реализации систем компьютерного тестирования..... 3

Аршинов Г.А. Совершенствование акустических методов определения дефектов в элементах конструкций..... 10

Аршинов Г.А. Уточнение акустических методов диагностики микродефектов материала в вязкоупругих стержнях..... 16

Атласов И.В., Орехов П.В. Вариант оптимизации направления автотранспортного дорожного потока (полосы движения) с помощью предвидения дорожного затора на регулируемом перекрестке, оснащенном видеонаблюдением..... 23

Астафьев Е.Р., Варфоломеева С.В. Влияние и учет семиотических особенностей языка математики на формирование познавательных и коммуникативных компетенций..... 26

Баранов В.В., Журбин Г.Е. Некоторые вопросы управления информационной безопасностью беспилотного летательного аппарата..... 30

Бессонов А.А. О некоторых вопросах использования математических методов в криминалистике и расследовании преступлений..... 33

Болтачев Э.Ф. О некоторых негативных тенденциях развития технологии анонимных сетевых соединений..... 36

Васин О.И., Щербаков В.А., Кулаков А.А. Технология блокчейн в автоматизированых системах специального назначения..... 40

Дрога А.А., Ковалева Е.Г., Савотченко С.Е. Проблемы обеспечения информационной безопасности мобильных устройств в правоохранительных органах..... 44

Епифанцева В.А., Хромых А.А. Об опыте разработки электронного учебно-методического комплекса для организации дистанционного обучения..... 51

Еськин Д.Л. Возможности применения технологии дополненной реальности правоохранительными органами..... 54

Ефремов С.К. Анализ ошибок прогнозирования успеваемости курсантов с использованием искусственной нейронной сети..... 57

Жилин Р.А. О результатах кластеризации однородных альтернатив..... 60

Жмурко Д.Ю. Корреляция временных рядов показателей деятельности АПК с циклами астронимических объектов..... 62

Иванов В.Ю., Волков А.Г. Автоматизированная система для фиксации аутентичных фотоснимком на базе смартфона с ОС ANDROID..... 68

Иванов И.П. Возможности математических методов и современных цифровых разработок в прогнозировании и предотвращении преступлений..... 71

Коимшиди Г.Ф., Саркисян А.Ж. АИС «Анализ и прогноз преступности» на платформе Excel как элемент рабочего места криминолога..... 73

Кропачев С.Ю., Крыгин С.В. Использование Windows 10 Timeline при расследовании компьютерных инцидентов..... 78

Лаптев В.Н. Место и роль информации в обеспечении успешного функционирования и развития открытых систем..... 83

Лаптев В.Н. Основные положения диалектики природы и их место в функционировании и развитии ОВД..... 88

Медведев В.А., Аристов Р.В. Искусственный интеллект, как перспективный метод борьбы с преступностью..... 99

Михайленко Е.В. Технологии подготовки компьютерных программ для генерации и проверки практических заданий по теме «Сравнения»..... 101

Нестеренко И.С. Особенности дистанционного обучения в условиях пандемии в образовательных системах Министерства внутренних дел Российской Федерации..... 111

Прокопенко А.Н., Жукова П.Н., Гусев Ю.М. К вопросу о подготовке сотрудников полиции, раскрывающих преступления, совершенные с использованием информационно-телекоммуникационных технологий..... 115

Путилов А.О. Основные направления защиты информации от Кибератак..... 119

Разбегаев П.В. Электронное обучение как фактор повышения качества образования..... 121

Серезевский А.В. Разработка и программная реализация алгоритма формульных подстановок для автоматизации процесса составления учебных задач по дисциплине «Физика» 124

Старостенко И.Н., Епифанцева В.А. От цифровизации к цифровой трансформации образования: драйверы развития..... 126

Телков А.Ю. Защита HTTP трафика связи оператора с узлом мониторинга событий информационной безопасности на базе открытого решения ELK STACK..... 130

Хромых А.А., Старостенко И.Н. Об опыте использования виртуального класса classroom для организации дистанционного обучения..... 133

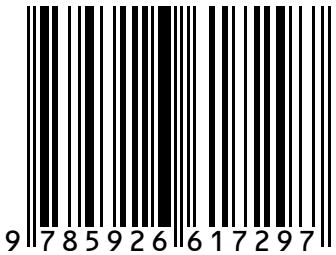
Научное издание

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ
И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ
СРЕДСТВА**

Материалы
XVII Всероссийской научно-практической конференции
(18 июня 2021 г.)

В авторской редакции
Компьютерная верстка *Н. А. Никитиной*

ISBN 978-5-9266-1729-7



Подписано в печать 11.11.2021. Формат 60х84 1/8.
Усл. печ. л. 15,0. Тираж 60 экз. Заказ 179.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.