

Краснодарский университет МВД России

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ
И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ
СРЕДСТВА**

Материалы
XX Международной научно-практической конференции
(6 июня 2024 г.)

Краснодар
2024

УДК 512.54.0
ББК 87.256.631
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);

М. В. Шарпан, кандидат физико-математических наук
(секретарь);

А. С. Победа;

А. А. Хромых, кандидат физико-математических наук;

С. К. Ефремов, кандидат технических наук, доцент;

К. И. Руденко, кандидат социологических наук

Математические методы и информационно-технические средства
М340 [Электронный ресурс] : материалы XX Междунар. науч.-практ. конф.,
6 июня 2024 г. / редкол.: И. Н. Старостенко, Е. В. Михайленко,
М. В. Шарпан, А. С. Победа, А. А. Хромых, С. К. Ефремов, К. И. Руденко. –
Электрон. дан. – Краснодар : Краснодарский университет МВД России,
2024. – 1 электрон. опт. диск.

ISBN 978-5-9266-2032-7

В сборнике содержатся материалы XX Международной научно-практической конференции, состоявшейся в Краснодарском университете МВД России 6 июня 2024 г., по направлениям «Математические методы и моделирование», «Программное обеспечение и информационно-технические средства», «Информационные технологии в борьбе с экстремизмом, терроризмом и организованной преступностью», «Информационные технологии в образовании», «Проблемы информатизации и информационной безопасности деятельности ОВД».

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

УДК 512.54.0
ББК 87.256.631

ISBN 978-5-9266-2032-7

© Краснодарский университет
МВД России, 2024

СОДЕРЖАНИЕ

Аликина С.В. Основные принципы машинного обучения.....	7
Антропова Г.Р., Гилмуллин Р.Р. Решение двойных интегралов в системе компьютерной алгебры и их приложения в геометрии.....	11
Аршинов Г.А., Аршинов А.Г. Оценка времени оборота средств, вложенных в производство продукции предприятия, в зависимости от цены ее реализации	16
Астафьев Е.Р. Проведение в военных вузах инструкторско-методических занятий по математическим и информационным дисциплинам.....	20
Бакулин В.М. Вопросы импортозамещения программного обеспечения в образовании.....	25
Богачева М.В. Возможности и перспективы использования технологий искусственного интеллекта в административной и оперативной деятельности органов внутренних дел	31
Бокадаров С.А., Даниленко В.А. Анализ способов противодействия современным угрозам информационной безопасности.....	38
Будиловская Д.Е., Степанов С.А. Применение искусственного интеллекта при обработке результатов анкетных данных.....	43
Воронцов Г.О., Коваленко А.В. Классические методы оптимизации для автоматизированной компоновки генерального плана промышленного предприятия.....	49
Добровольская Н.Ю. Технология единой точки входа как основа авторизации пользователей различных приложений.....	53
Дрога А.А., Чижов И.А. Использование информационных технологий и систем в мероприятиях по обнаружению наркотических веществ.....	57
Дырма С.В. Противодействие кражам, совершаемым с использованием информационно-коммуникационных технологий.....	62
Епифанцева В.А., Иванов И.П. Использование робототехники в органах внутренних дел Российской Федерации.....	67
Еськин Д.Л. Проблема использования искусственного интеллекта в противоправной деятельности.....	70
Ефремов С.К. Сокращение размерности задачи прогнозирования успеваемости курсантов с использованием искусственной нейронной сети.....	75
Жмурко Д.Ю., Лаптев С.В. Эволюция интернета: от Web 3.0 к Web 4.0 – перспективы развития глобальной сети.....	79

Иночкина Е.В., Тютюник Н.П. Диффузионная нейронная сеть генерации неоднородных облаков точек.....	88
Камышов Ю.Н., Печатнова Е.В., Егорова Н.С. Сравнение результатов опроса населения на различных электронных ресурсах по вопросу обеспечения безопасности дорожного движения.....	94
Карпика А.Г. Анализ моделей оценки поведения пользователей компьютерных систем.....	99
Кенжалиева С.З., Алексеев А.Д., Белов А.В. Направления криптоанализа и их математическая основа.....	103
Киришин И.И., Печатнова Е.В., Шадых А.О. Актуальные вопросы практического применения БВС самолетного типа VTOL в МВД России.....	110
Копыткова Л.Б., Фурсов А.А. Модели модулярного кодирования целых чисел разных знаков.....	115
Коренева О.В., Алланов А.Е. Применение операционного исчисления в исследовании передаточной функции.....	121
Коренева О.В., Огарев А.А. Метод операторов и преобразование Лапласа, их применение в электротехнике и теории автоматического управления.....	127
Корчагина Е.В., Ярцева А.А. Оптимизация системы информационной безопасности в учреждениях УИС с помощью моделирования информационных потоков.....	133
Кошелев Д.А., Ромашов А.А., Корза Е.А. Сравнительный анализ методов модуляции с использованием стохастических сигналов для обеспечения безопасности информации, передаваемой в КРУ РТК ВН.....	137
Кубасов И.А. Перспективы развития математических методов в информационно-аналитическом обеспечении деятельности органов внутренних дел.....	144
Кулиш О.А., Джураев Э.С. Методика криптоанализа текста, зашифрованного шифром простой перестановки.....	150
Лаптев С.В., Лаптев В.Н. О главном критерии оценки творческой деятельности профессионалов.....	156
Левачева Ю.В. Обеспечение безопасности данных в образовательных организациях.....	168
Лемайкина С.В. Проблемы деанонимизации использования криптовалют в преступной сфере.....	173

Лихобабина А.В. Математические методы организации распределения по группам специалистов, проходящих подготовку в образовательных организациях.....	180
Матвеев С.Н., Нуждина О.Е. Сравнительный анализ информационных средств «живая математика», «математический конструктор» и «Geogebra»	186
Мельник В.А., Фомичева М.Ю. Математические методы в кибербезопасности.....	194
Меньших Т.В., Ворончихин М.М. Применение теории графов в оптимизации сетей связи.....	200
Меняйло Д.В., Барсова Е.Р. Программное обеспечение и его применение в сфере противодействия незаконному обороту наркотиков.....	204
Михайленко Е.В. Методы и технологии разработки программных продуктов для использования в учебном процессе по математическим и информационно-техническим дисциплинам.....	209
Назаров А.К. Анализ современных угроз встраиваемых систем.....	221
Наумова Н.А., Иващенко Н.В., Орлов Р.В. Приложения разложения многочленов на множители в теории кодирования.....	224
Нестеренко И.С., Арипов А.Л., Бровченко С.Ю. Telegram-платформа как инструмент профилактики киберпреступлений в рамках правового просвещения населения в условиях цифровой трансформации современного российского общества.....	229
Никифорова Л.В. Моделирование периодической системы управления структурно неопределенным объектом с запаздываниями.....	235
Прокопенко А.Н., Жукова П.Н., Страхов А.А. Некоторые вопросы лицензирования в сфере защиты информации в России на современном этапе.....	242
Разбегаев П.В. Полицейская робототехника: история и перспективы применения.....	253
Рыбальченко А.Ю., Дрога А.А. Особенности противодействия преступлениям, связанным с незаконным оборотом наркотических средств и психотропных веществ, в условиях цифровизации.....	259
Савин В.Н., Гончарова М.С. Анализ устойчивости хэш-функции к взлому радужными таблицами.....	264
Савотченко С.Е., Акапьев В.Л., Чеканов А.Н. Математическая модель поиска потенциального подозреваемого по признакам совершенного преступления.....	270

Самойлова Ю.М., Некрасова А.А. Системы искусственного интеллекта в правоохранительной деятельности.....	275
Селеменова Т.А., Ермакова С.А. К приложению теории статистических решений.....	281
Старостенко И.Н. Угрозы и уязвимости, связанные с сетевым протоколом IP.....	286
Толстых М.Ю., Баханов М.В. Приложение-детектор деструктивного контента в музыкальных произведениях ARFA.....	292
Толстых М.Ю., Быков Д.Р. Цифровые средства противодействия незаконному обороту наркотиков.....	297
Халафян А.А., Авраменко А.А., Патрушев Р.С. Построение прогностических моделей методами Data Mining для принятия обоснованных клинических решений в стоматологии.....	301
Хромых А.А. Построение аддитивной модели временного ряда, характеризующего количество дорожно-транспортных происшествий с пострадавшими на территории Краснодарского края	305
Чижев И.А., Дрога А.А. Виды мошенничества с использованием электронных средств платежа.....	311
Чубырь Н.О. Асимптотический метод решения краевой задачи для стационарной системы уравнений.....	317
Шарпан М.В., Сиякаев Д.Д. Особенности реализации ролевой модели разграничения доступа в современных операционных системах на примере ОС LINUX.....	321
Яхонтов И.С., Крепышев Д.А. CDN: принципы работы и практическое применение.....	330
Яхонтова И.М., Ковыляев Р.А. Визуализация данных в VBA: принципы, применение и преимущества.....	335
Яценко В.М. Выбор метода аппроксимации экспериментальных данных для описания роста покрытия в процессе микродугового оксидирования.....	340

Аликина Светлана Викторовна

ОСНОВНЫЕ ПРИНЦИПЫ МАШИННОГО ОБУЧЕНИЯ

Использование искусственного интеллекта становится все более популярным и востребованным в современном мире. Искусственный интеллект определяется как комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека [1].

Создание искусственного интеллекта чаще всего базируется на следующих технологиях: машинное обучения, глубокое обучения, обработка и генерация естественного языка.

Под машинным обучением понимают раздел теории искусственного интеллекта, в основе которого лежит поиск методов решения задач путем обучения в процессе решения похожих задач через использование средств математической статистики, дискретной математики, численных методов и других разделов математики [2].

Машинное обучение является одним из самых актуальных и перспективных направлений в современном мире. Его применение охватывает множество сфер: от разработки автономных автомобилей до улучшения рекомендательных систем в социальных сетях. В основе эффективности машинного обучения лежат определенные принципы, которые помогают алгоритмам извлекать полезные знания из данных. Рассмотрим основные методы машинного обучения.

Контролируемое обучение (обучение с «учителем»). В этом случае алгоритму предоставляются примеры входных данных и соответствующие им выходные данные. Алгоритм обучается на основе этих пар, стремясь предсказать правильный выход для новых входных данных. Следовательно, при контролируемом обучении «учитель» обучает машину, используя данные, некоторые из которых уже содержат правильные ответы. Такой метод используется, например, для решения задач классификации и регрессии.

Неконтролируемое обучение (обучение без учителя) используется в случаях, когда у нас нет размеченных данных. Алгоритмы машинного обучения должны самостоятельно находить структуры и закономерности в данных. Это означает, что пользователь не предоставляет маркированные (отмеченные) данные. Здесь широко применяются методы кластеризации, снижения размерности и ассоциативного анализа.

Обучение с подкреплением. В этом случае алгоритму машинного обучения предоставляется среда, в которой он самостоятельно принимает решения и получает обратную связь в виде награды или штрафа. Алгоритм учится оптимизировать свое поведение для достижения заранее заданных целей. Под штрафом или наградой следует понимать некоторую скалярную величину, которой оценивается каждый шаг взаимодействия со средой, показывающую насколько эффективно алгоритм справляется с поставленными задачами [3].

Машинное обучение имеет огромный потенциал и обширные перспективы использования в различных областях.

В медицине машинное обучение помогает в диагностике заболеваний, прогнозировании эффективности лечения, разработке персонализированных подходов к пациентам, анализе медицинских изображений и многое другое. Это позволяет улучшить качество медицинской помощи и снизить риски ошибок.

В сфере финансов машинное обучение применяется для анализа рынков, прогнозирования трендов, управления рисками, выявления мошенничества, автоматизации торговли и принятия инвестиционных решений.

В автомобильной промышленности машинное обучение используется для разработки автономных транспортных средств, оптимизации маршрутов, управления транспортными потоками и улучшения безопасности дорожного движения.

В области сетевых технологий машинное обучение применяется для улучшения рекомендательных систем, персонализации контента, анализа данных о поведении пользователей, обнаружения спама и прочих задач.

В производственной сфере машинное обучение помогает в оптимизации производственных процессов, контроле качества продукции, предсказании отказов оборудования и планировании производства.

В научных исследованиях машинное обучение используется для анализа и интерпретации сложных данных, моделирования физических процессов, прогнозирования климатических изменений и многих других задач.

Это лишь небольшая часть областей, где машинное обучение может найти применение. Несмотря на все положительные моменты использования машинного обучения, существуют и некоторые затруднения в работе алгоритма. К этим проблемам можно отнести: недостаточное количество обучающих данных, низкое качество этих данных, неоднозначные связи между входными и выходными переменными.

Для эффективного обучения алгоритма может не хватать достаточного количества данных. Никогда не бывает излишка обучающих данных, но при этом они должны быть разнообразными, чтобы предотвратить переобучение. Разговор о переобучении в машинном обучении возникает, когда модель учится на искаженных или слишком больших объемах обучающих данных, что в конечном итоге негативно сказывается на ее производительности после развертывания. Например, использование алгоритма машинного обучения для решения таких задач, для которых более рациональным было бы решение посредством линейной регрессии. Недообучение представляет собой модель, которая обучается на данных, заставляющих ее устанавливать неоднозначные связи между входными и выходными переменными. Также недообучение может возникнуть, когда алгоритм является слишком простым для обучающего датасета [4].

Также существует проблема интерпретируемости. Так, например, нейросеть многие ученые называют «черным ящиком», который получает данные на входе и, перерабатывая их, выдает ответ. При этом если входные данные содержат ошибки, предрассудки, то они со временем накапливаются в

обучаемой модели и приводят к дисбалансу. Для исключения ошибок интерпретации необходимо прибегнуть к специальным мерам [5].

Таким образом, с постоянным развитием технологий и увеличением объема данных мы можем ожидать дальнейшего расширения спектра задач, которые можно решить с помощью методов машинного обучения. Но необходимо понимать, что используя машинное обучение существует возможность негативных последствий.

Литература

1. Национальная стратегия развития искусственного интеллекта на период до 2030 года (Утверждена указом Президента РФ от 10.10.2019 г. № 490). https://www.consultant.ru/document/cons_doc_LAW_335184/1f32224a00901db9cf44793e9a5e35567a4212c7/
2. Миронов А. М. Машинное обучение. Ч. 1 / А.М. Миронов; Московский государственный университет имени М. В. Ломоносова, Механико-математический факультет, Кафедра математической теории интеллектуальных систем. – Москва: Макс-Пресс, 2018. – 85 с.
3. Черкасов Д.Ю., Иванов В. В. Машинное обучение // Наука, техника и образование. – 2018. – № 5 (46). - С. 85-87.
4. Вичугова А. ТОП-5 проблем с данными в ML-системах и MLOps для их устранения // Школа больших данных, 2024. – <https://bigdataschool.ru/blog/mlops-ml-issues-and-challenges.html>.
5. Оселедец И.В. Успехи и проблемы машинного обучения // Проектирование будущего. Проблемы цифровой реальности: труды 5-й Международной конференции (3-4 февраля 2022 г., Москва). – М.: ИПМ им. М.В. Келдыша, 2022. – С. 102-108. – <https://keldysh.ru/future/2022/9.pdf>
<https://doi.org/10.20948/future-2022-9>

Сведения об авторе

Аликина Светлана Викторовна, преподаватель кафедры информатики и математики Волгоградской академии МВД России.

**Антропова Гюзель Равильевна,
Гилмуллин Рушан Ралифович**

РЕШЕНИЕ ДВОЙНЫХ ИНТЕГРАЛОВ В СИСТЕМЕ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И ИХ ПРИЛОЖЕНИЯ В ГЕОМЕТРИИ

В современном образовании необходима и широко используется на практике компьютерная поддержка в решении научно-технических и различных математических задач. Программное обеспечение позволяет проводить решение более сложных исследовательских задач, благодаря тому, что исключаются громоздкие вычисления [1, 2]. Такой подход, позволяет реализовать на практике различные обучающие тренажеры, как составленные педагогом самостоятельно, так и разработанные специалистами [3, 4]. Рассмотрим использование системы компьютерной алгебры Maple при решении кратных интегралов в дифференциальной геометрии и на плоскости Лобачевского.

Во многих задачах прикладного характера требуется вычисление кратных интегралов. Основным приёмом вычисления кратных интегралов является приведение его к повторным интегралам. Этот подход для двойных интегралов реализуется без больших затруднений. Однако уже для тройных интегралов приведение к повторному интегрированию требует сложных вычислений. С этой точки зрения мы предлагаем в решении интегралов использовать систему компьютерной алгебры [6]. Заметим, что компьютерное вычисление можно сопровождать и аналитическим решением.

Такой подход в решение многих задач позволяет исследователю проверить правильность выполненных вычислений. А с точки зрения обучения такой приём выступает в качестве тренажёра.

Отметим, что приложение кратных интегралов обширно. В качестве демонстрации здесь приведем их применение в элементарной и высшей геометрии [5].

Рассмотрим пример вычисления двойного интеграла на области

$$G: \begin{cases} y = x^3; \\ y = -\sqrt{x}; \text{ от функции } f(x, y) = xy - 4x^3y^3. \\ x = 1. \end{cases}$$

Получим:
$$\int_0^1 dx \int_{-\sqrt{x}}^{x^3} (xy - 4x^3y^3) dy = \int_0^1 dx \left(\frac{xy^2}{2} - x^3y^4 \right) \Big|_{-\sqrt{x}}^{x^3} =$$

$$\int_0^1 \left(\frac{x^7}{2} - x^{15} - -\frac{x^2}{2} + x^5 \right) dx = \left(\frac{x^8}{16} - \frac{x^{16}}{16} - \frac{x^3}{6} + \frac{x^6}{6} \right) \Big|_0^1 = \frac{1}{16} - \frac{1}{16} - \frac{1}{6} = 0.$$

Двойной интеграл в системе компьютерной алгебры Maple вычисляется командой `int()`. Команда интегрирования принимает в себя 3 аргумента, `int(<уравнение плоскости>, <промежуток первого аргумента>, <промежуток второго аргумента>)`.

В итоге получим результат:

$$\text{int}(xy - 4x^3y^3, y = -\text{sqrt}(x)..x^3, x = 0..1); \text{ ответ: } 0.$$

Рассмотрим пример на модели Пуанкаре плоскости Лобачевского.

$$G: \begin{cases} \gamma_1: (x-1)^2 + y^2 = 1; \\ \gamma_2: (x-3)^2 + y^2 = 9; \\ \gamma_3: (x-4)^2 + y^2 = 4; \\ \gamma_4: x = 1; \\ \gamma_5: x = 4. \end{cases}$$

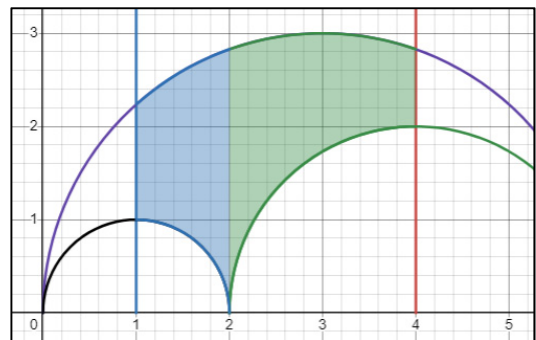


Рис. 1. Пятиугольник на плоскости Лобачевского

Разделим площадь на две части. Тогда площадь искомой фигуры будет равна сумме площадей составляющих:

$$S = S_1 + S_2$$

$$\begin{aligned} S_1 &= \int_1^2 dx \int_{\sqrt{1-(x-1)^2}}^{\sqrt{9-(x-3)^2}} \frac{1}{y^2} dy = \int_1^2 dx \left(-\frac{1}{y} \right) \Big|_{\sqrt{1-(x-1)^2}}^{\sqrt{9-(x-3)^2}} = \\ &= \int_1^2 \left(\frac{1}{\sqrt{1-(x-1)^2}} - \frac{1}{\sqrt{9-(x-3)^2}} \right) dx = \left(\arcsin \left(\frac{x-1}{1} \right) - \arcsin \left(\frac{x-3}{3} \right) \right) \Big|_1^2 = \end{aligned}$$

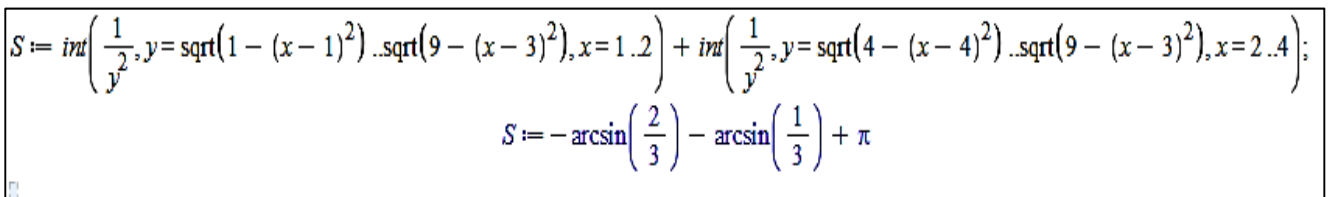
$$= \arcsin(1) - \arcsin\left(-\frac{1}{3}\right) - \arcsin(0) + \arcsin\left(-\frac{2}{3}\right) =$$

$$= \frac{\pi}{2} + \arcsin\left(\frac{1}{3}\right) - \arcsin\left(\frac{2}{3}\right).$$

$$S_2 = \int_2^4 dx \int_{\sqrt{4-(x-4)^2}}^{\sqrt{9-(x-3)^2}} \frac{1}{y^2} dy = \frac{\pi}{2} - 2\arcsin\left(\frac{1}{3}\right). \text{ Тогда:}$$

$$S = S_1 + S_2 = \frac{\pi}{2} + \arcsin\left(\frac{1}{3}\right) - \arcsin\left(\frac{2}{3}\right) + \frac{\pi}{2} - 2\arcsin\left(\frac{1}{3}\right) =$$

$$\pi - \arcsin\left(\frac{1}{3}\right) - \arcsin\left(\frac{2}{3}\right).$$



$$S := \int_{\frac{1}{y}}^{\sqrt{1-(x-1)^2} \dots \sqrt{9-(x-3)^2}}, x=1..2 \Big) + \int_{\frac{1}{y}}^{\sqrt{4-(x-4)^2} \dots \sqrt{9-(x-3)^2}}, x=2..4 \Big);$$

$$S := -\arcsin\left(\frac{2}{3}\right) - \arcsin\left(\frac{1}{3}\right) + \pi$$

Рис. 2. Вычисление площади фигуры в системе компьютерной алгебры Maple

Рассмотрим пример из курса дифференциальной геометрии. Найти площадь части боковой поверхности конуса $z^2 = x^2 + y^2, z \geq 0$, вырезаемой из нее цилиндром $x^2 - ax + y^2 = 0$.

Перейдём к цилиндрическим координатам $x = v \cos u, y = v \sin u, z = v$, $(u, v) \in G, G = \{(u, v): v \leq a \cos u, -\frac{\pi}{2} \leq u \leq \frac{\pi}{2}\}$.

Найдем коэффициенты первой квадратичной формы этой поверхности:

$$\vec{r}(u, v) = (v \cos u, v \sin u, v), \vec{r}_u = (-v \sin u, v \cos u, 0), \vec{r}_v = (\cos u, \sin u, 1).$$

$$\gamma_{11} = v^2, \gamma_{12} = 0, \gamma_{22} = 2.$$

Тогда площадь поверхности будет равен

$$\iint_G \sqrt{\gamma_{11}\gamma_{22} - \gamma_{12}^2} du dv = \iint_G \sqrt{2}v du dv = \sqrt{2} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} du \int_0^{a \cos u} v dv =$$

$$= \sqrt{2} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{a^2 \cos^2 u}{2} du = \frac{\sqrt{2}a^2}{2} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^2 u du = \left| \cos^2 u = \frac{\cos 2u + 1}{2} \right|$$

$$\begin{aligned}
&= \frac{\sqrt{2}a^2}{2} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\cos 2u + 1}{2} du = \\
&= \frac{\sqrt{2}a^2}{4} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} (\cos 2u + 1) du = \frac{\sqrt{2}a^2}{4} \left(-\frac{1}{2} \sin 2u + u \right) \Bigg|_{-\frac{\pi}{2}}^{\frac{\pi}{2}} = \frac{\sqrt{2}a^2}{4} \left(\frac{\pi}{2} + \frac{\pi}{2} \right) = \\
&= \frac{\sqrt{2}a^2\pi}{4}.
\end{aligned}$$

В итоге получим результат:

$$\text{int}\left(\sqrt{2}y, y = 0..a \cos(x), x = -\frac{\pi}{2}.. \frac{\pi}{2}\right); \text{ответ: } \frac{\sqrt{2}a^2\pi}{4}.$$

Мы рассмотрели, как можно на практике использовать программное обеспечение и как проявляется одно из главных достоинств использования информационно-коммуникационных технологий – возможность исследования более сложных математических моделей, благодаря сокращению громоздких вычислений и рутинных операций.

Литература

1. Антропова Г.Р., Матвеев С.Н. Организация спецкурса по геометрии средствами информационных технологий (в подготовке бакалавров)// Мир науки. 2017.Т.5. №2.- URL: <http://mir-nauki.com/PDF/33PDMN217.pdf>.
2. Антропова Г.Р., Матвеев С.Н., Шакиров Р.Г. Повышение эффективности обучения геометрии Лобачевского с помощью системы Wingeom // Проблемы современного педагогического образования. – 2024. – № 82-1. – С. 19-23. – EDN BSCXNS.
3. Антропова Г.Р., Матвеев С.Н., Шакиров Р.Г. Реализация некоторых задач дифференциальной геометрии в программе Geo Gebra // Высшее образование сегодня. 2020. №6. С.59-63. URL: [download/elibrary_42840120_88091866.pdf](download/elibrary_42840120_88091866.pdf). EDN: YXYADF.

4. Антропова, Г. Р., Матвеев С.Н. Приложение Wingeom в реализации преобразований плоскости Лобачевского // Научно-технический вестник Поволжья. – 2023. – № 11. – С. 411-413. – EDN HRAUCQ.

5. Бугров Я.С. Высшая математика в 3 т. Том 3. В 2 кн. Книга 1. Дифференциальные уравнения. Кратные интегралы: учебник для вузов. – Москва: Издательство Юрайт, 2024. – 288 с.

6. Сиразов, Ф. С. Применение системы компьютерной алгебры Maxima при решении некоторых примеров теории чисел // Актуальные вопросы математического образования: состояние, проблемы и перспективы развития: Материалы Всероссийской научно-практической конференции Сургут, 26 февраля – 03 2018 года / Ответственный редактор Н.В. Суханова. – Сургут: Сургутский государственный педагогический университет, 2018. – С. 157-161. – EDN YAQDNB.

Сведения об авторах

Антропова Гюзель Равильевна, кандидат педагогических наук, доцент кафедры математики Набережночелнинского института (филиала) Казанского (Приволжского) федерального университета.

Гилмуллин Рушан Ралифович, магистрант Набережночелнинского государственного педагогического университета.

Аршинов Георгий Александрович

Аршинов Александр Георгиевич

ОЦЕНКА ВРЕМЕНИ ОБОРОТА СРЕДСТВ, ВЛОЖЕННЫХ В ПРОИЗВОДСТВО ПРОДУКЦИИ ПРЕДПРИЯТИЯ, В ЗАВИСИМОСТИ ОТ ЦЕНЫ ЕЕ РЕАЛИЗАЦИИ

На основе линейной зависимости $V(P_3)$ рыночного спроса на готовую продукцию предприятия, где P_3 – установленная стоимость единицы товара, P_r – ее сложившаяся средняя рыночная стоимость, исследуем влияние оборота вложенного в производство капитала на оптимальную цену реализации единицы произведенной продукции путем математического моделирования [1].

Зададим функцию спроса линейной (рис. 1):

$$V(P_3) = -k_1 P_3 + k_2$$

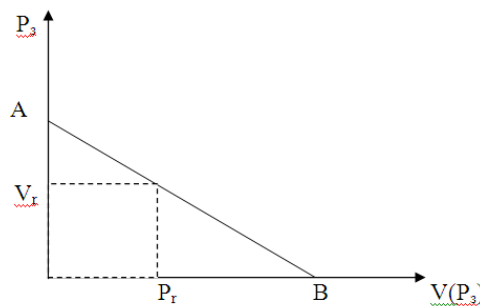


Рис. 1 Функция спроса

По точкам $A(P_r, V_r)$ и $B(nP_r, 0)$ ($n > 1$) графика функции $V(P_3)$ при величине V_r , являющейся средним значением объема продукции, реализованного на рынке найдем k_1, k_2 , решая систему уравнений:

$$\begin{cases} -k_1 P_r + k_2 = V_r \\ -k_1 n P_r + k_2 = 0 \end{cases}$$

В итоге

$$k_1 = \frac{V_r}{P_r(n-1)}, \quad k_2 = \frac{nV_r}{n-1}. \quad (1)$$

С учетом формул (1)

$$V(P_3) = -k_1 P_3 + n P_r k_1.$$

Найдем доход, получаемый предприятием от реализации его продукции в единицу времени.

$$D(P_3) = (-k_1 P_3 + n P_r k_1) P_3.$$

Определим производную функции $D(P_3)$ и приравняем ее к нулю, получим уравнение, из которого найдем оптимальную цену P_3 :

$$-2P_3 + nP_r = 0,$$

откуда $P_3 = \frac{nP_r}{2}.$

Прибыль будет получена при

$$D(P_3) > 0$$

или

$$(-k_1 P_3 + n P_r k_1) P_3 > 0, \quad (2)$$

Имеют место соотношения $k_1 > 0$, $P_3 > 0$, тогда:

$$-P_3 + nP_r > 0$$

На графике показаны области выполнения неравенства (2) (рис. 2).

Доход и прибыль будут максимальными, если при цене реализации единицы произведенной продукции

$$P_3 = \frac{nP_r}{2}.$$

Прибыль, полученная за время t , вычисляется по формуле:

$$\Pi_3 = (-P_3^2 + nP_r P_3) k_1 t - C_3,$$

где C_3 – затраты на производство и продажу готовой продукции за время t .

По формуле

$$D(P_3) = C_3$$

найдем время $T_{об}$, за которое произойдет оборот капитала, вложенного на производство продукции, получим:

$$(-P_3^2 + nP_r P_3) k_1 t - C_3 = 0,$$

тогда

$$T_{об} = \frac{C_3}{(-P_3^2 + nP_r P_3)k_1}.$$

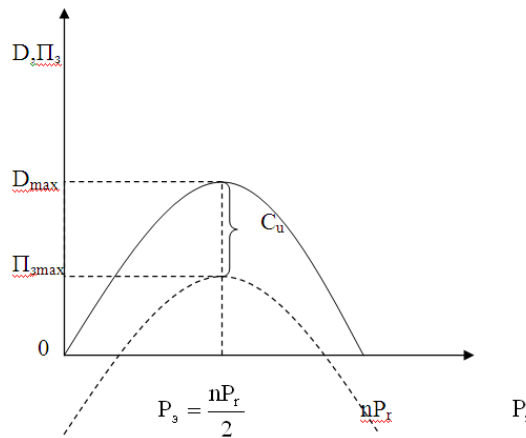


Рис. 2. Условие рентабельной работы

Минимальное время $T_{об}$, которому соответствует оборот капитала получим при оптимальной цене реализации

$$P_3 = \frac{nP_r}{2}.$$

При $n=2$ $P_3=P_r$, и

$$T_{об} = \frac{C_3}{(-P_3^2 + 2P_r^2)k_1}.$$

Учитывая значения

$$k_1 = \frac{V_r}{P_r(n-1)}, n=2,$$

имеем:

$$T_{об}(P_r) = \frac{C_3}{P_r V_r}$$

Если $n=1,6$, то $P_3 = P_3 = \frac{nP_r}{2} = 0,8P_r$.

Цена P_3 , приводящая к максимальной прибыли предприятия, на 20% меньше средней P_r , и оборот капитала произойдет за время

$$T_{об} = \frac{C_3}{(-0,8^2 P_r^2 + 1,6P_r 0,8P_r) \frac{V_r}{P_r(1,6-1)}}.$$

Литература

1. Анализ условий образования эффективных объединений предприятий молочного подкомплекса АПК / Г.А. Аршинов, В.Г. Аршинов, В.Н. Лаптев, С.В. Лаптев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2017. – №08(132). С. 128 – 155. – IDA [article ID]: 1321708012. – Режим доступа: <http://ej.kubagro.ru/2017/08/pdf/12.pdf>.

Сведения об авторах

Аршинов Георгий Александрович, доктор технических наук, доцент, профессор кафедры компьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина.

Аршинов Александр Георгиевич, студент Кубанского государственного аграрного университета имени И.Т. Трубилина.

Астафьев Евгений Рудольфович

ПРОВЕДЕНИЕ В ВОЕННЫХ ВУЗАХ ИНСТРУКТОРСКО-МЕТОДИЧЕСКИХ ЗАНЯТИЙ ПО МАТЕМАТИЧЕСКИМ И ИНФОРМАЦИОННЫМ ДИСЦИПЛИНАМ

На современном этапе обучения система образования предполагает непрерывный рост квалификации преподавателя в его профессиональной деятельности. В связи с этим возрастает роль методической работы, направленной на повышение эффективности и качества учебного процесса, на применение инновационных методов и приемов обучения; на повышение уровня профессиональной компетентности преподавателя; на воспитание обучающихся.

Основой повышения педагогического мастерства преподавательского состава (ПС) кафедры являются методические занятия. В соответствии с Приказом Министра обороны РФ от 30.05.2022 № 308 «Об организации образовательной деятельности в федеральных государственных организациях, осуществляющих образовательную деятельность и находящихся в ведении Министерства обороны РФ» инструкторско-методические занятия (ИМЗ) являются одной из основных форм методической подготовки ПС кафедры в военных вузах.

ИМЗ организуются по наиболее важным и сложным темам учебной программы в целях отработки единой организации и методики проведения занятий, освоения новых, более эффективных методических приемов. Они проводятся руководящим составом образовательной организации (филиала, института, факультета), преподавательским составом и командирами подразделений слушателей (курсантов) (ст. 69 Приказа МО РФ №308) [1].

Особое внимание на подготовку по математике и информатике обратил Президент РФ В.В. Путин на проведенной видеоконференции с лучшими студентами ведущих вузов России 25 января 2022 года. Он сделал особый акцент на то, что «математика – [это] не какая-то абстрактная, отвлеченная область знаний», а «наука будущего, инструмент для развития новых технологий и самых передовых».

Для выполнения квалификационных требований к военно-профессиональной подготовке выпускников на кафедре математики (и информатики) систематически организуются и проводятся инструкторско-методические занятия по изучаемым темам учебных дисциплин «Математика», «Информатика» и «Вычислительная техника» в целях отработки единой организации и методики проведения занятий, а также освоения новых, более эффективных методических приемов проверки знаний и умений обучающихся, методики проведения занятия с использованием мультимедийного комплекса.

Мультимедийный комплекс способствует развитию коммуникативных способностей, а также развитию информационной грамотности [3].

Предлагаемые подходы использования математико-статистического аппарата при проведении педагогических исследований предполагают грамотный и правильный выбор статистических критериев и умелое использование применяемых методов анализа [2].

Рассматриваемые темы реализуется в рамках базовой части основной профессиональной образовательной программы.

Актуальность изучения рассматриваемых тем обусловлена необходимостью:

- развития интеллекта и способностей обучающихся к логическому и алгоритмическому мышлению;
- создания фундамента математического образования;
- воспитания математической культуры;
- понимания роли теоретических основ математического анализа и в частности использования основных понятий: множества, основные понятия математической логики, функция, предел функции для решения практических задач в различных профессиональных сферах;
- формирования у обучаемых умений и навыков работы с современной компьютерной техникой;

- выработки самостоятельного получения знаний по использованию вычислительной техники и применению современных информационных технологий.

Процесс изучения рассматриваемых тем направлен на формирование у обучающихся способности к поиску, переработке и передаче актуальной информации из различных источников, готовности квалифицированно использовать современные информационные компьютерные технологии.

Основной целью освоения изучаемых тем является:

- формирование у обучающихся математических знаний, необходимых для изучения дисциплин естественнонаучного и профессионального циклов;
- привитие практических навыков решения военно-прикладных задач основными математическими методами, необходимыми для моделирования реальных процессов и явлений;
- расширение знаний и умений по применению вычислительной техники;
- целесообразность их использования при решении прикладных задач;
- формирование и развитие профессиональных навыков обучающихся.

В качестве примера можно рассмотреть проведенное на кафедре ИМЗ «Организация и методика проведения учебных занятий по дисциплине «Информатика» по теме № 1 «Архитектура и программное обеспечение компьютеров» для курсантов, обучающихся по специальности 25.05.04».

В соответствии с рабочей программой учебной дисциплины «Информатика» данная тема состоит из следующих дидактических элементов: Понятие информации. Общая характеристика процессов сбора, обработки, передачи и накопления информации. Современные компьютеры. Архитектура и устройство современных компьютеров. Понятие и классификация программного обеспечения. Операционные системы. Системы обработки текстов. Табличные процессоры. Базы данных. Системы управления базами данных. Компьютерная графика. Системы подготовки презентаций.

Основной целью освоения данной темы является формирование у обучающихся знаний, необходимых для понимания информационных процессов, изучения прикладных и офисных программных средств, стимулирования активной познавательной деятельности, формирования творческого мышления.

Актуальность изучения темы обусловлена необходимостью:

- выработки первичных навыков решения задач, в том числе с помощью ЭВМ, позволяющих в дальнейшем изучать и эффективно использовать цифровые прицельно-навигационные и радиотехнические комплексы;
- привития практических навыков решения военно-прикладных задач на ЭВМ с использованием языков программирования высокого уровня.

В соответствии с требованиями ФГОС для реализации компетентностного подхода при изучении данной темы предусматривается широкое использование активных и интерактивных форм проведения занятий в сочетании с самостоятельной работой обучающихся.

При изложении нового материала необходимо, чтобы обучающиеся усвоили как физическую сущность рассматриваемых явлений, так и метод подхода к их изучению. Внедрение проблемного обучения, как основы развития творческого мышления обучающихся, должно быть предметом особой заботы преподавателей.

Для проверки хода и качества усвоения учебного материала, стимулирования учебной деятельности обучающихся, совершенствования методики проведения занятий запланирована контрольная работа.

При изучении данной темы следует обратить внимание на использование обучающимися электронного учебного пособия, разработанного преподавательским составом кафедры.

Таким образом, проводимые на кафедре методические занятия с преподавательским составом и, в частности, инструкторско-методические

занятия, способствуют повышению педагогического мастерства, а также эффективности организации и качеству учебного процесса.

Литература

1. Об организации образовательной деятельности в федеральных государственных организациях, осуществляющих образовательную деятельность и находящихся в ведении Министерства обороны РФ: приказ Министра обороны РФ от 30.05.2022 № 308.

2. Астафьев, Е.Р. Общие подходы к оценке эффективности методики обучения курсантов с использованием математико-статистических методов / Е.Р. Астафьев, С.В. Варфоломеева, Р.Р. Черный // Научные чтения имени профессора Н.Е. Жуковского: материалы XI Международной научно-практической конференции. – Краснодар: Краснодарское ВВАУЛ, 2021. – С. 439-441.

3. Третьякова, Н.В. Об использовании элементов электронной образовательной среды в учебном процессе / Н.В. Третьякова, Е.Р. Астафьев // Математические методы и информационно-технические средства: материалы XVIII Всероссийской научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2022. – С. 163-165.

Сведения об авторе

Астафьев Евгений Рудольфович, кандидат физико-математических наук, доцент кафедры математики (и информатики), Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А.К. Серова.

Бакулин Василий Михайлович

ВОПРОСЫ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОБРАЗОВАНИИ

Процесс цифровой трансформации общества оказал большое влияние на все сферы деятельности в нашей стране. Эта трансформация основана на использовании различных информационных технологий, которые в свою очередь опираются на соответствующие технические и программные решения. Сфера образования, включая среднее и высшее, также претерпела изменения под воздействием цифровизации. Качество программно-технических решений напрямую влияет на успешность цифровизации [1]. Традиционно, зарубежные разработчики были лидерами в создании программного обеспечения, что привело к тому, что большинство ИТ-решений в образовательной системе были основаны на импортных продуктах. Однако, в последнее время, из-за ухода многих иностранных компаний с российского рынка и прекращения ими поддержки своих продуктов, возникла необходимость в поиске альтернативных решений, будь то свободное программное обеспечение или программные продукты отечественных разработчиков [2, 3].

Программное обеспечение, используемое для организации образовательного процесса, по своему функциональному назначению можно разделить на три условные группы:

- Программное обеспечение общего назначения, включая системное и классическое офисное программное обеспечение;
- Программное обеспечение для поддержки образовательного процесса;
- Специализированное программное обеспечение, предназначенное для изучения определённых дисциплин и специальностей.

В рамках данной статьи ограничимся рассмотрением только первой группы программного обеспечения, которая включает в себя операционные системы и программы, которые необходимы для ежедневной работы, учёбы или

других видов деятельности пользователей ПК (так называемые офисные приложения).

Общеизвестно, что большинство домашних и офисных компьютеров в России используют операционную систему Microsoft Windows различных версий. В марте 2022 года Microsoft и ряд других зарубежных производителей программного обеспечения объявили о своём уходе с российского рынка, что выразилось в прекращении продаж новых лицензий и продлении подписок на облачные сервисы по модели SaaS (Software as a service – программное обеспечение как услуга). Это, в свою очередь, создаёт трудности при покупке новой компьютерной техники, так как возникает вопрос установки лицензионных версий операционных систем от Microsoft и другого программного обеспечения от зарубежных разработчиков. На данный момент проблема не столь остра, потому что в образовательных учреждениях уже имеется достаточное количество техники с необходимыми лицензиями, которая будет функционировать до момента физического или морального износа, а также существует запас приобретённых лицензий, которые, согласно заявлениям иностранных производителей, продолжат действовать. Тем не менее, со временем, когда текущие лицензии будут исчерпаны и старая техника выведена из эксплуатации, проблема с установкой необходимого программного обеспечения станет всё более актуальной.

Одним из путей решения проблемы с программным обеспечением является переход на отечественные операционные системы. В едином реестре российских программ представлены такие операционные системы, как «Альт», «Астра Линукс», «РедОС», «AlterOS» и другие [4], большинство из которых основаны на различных дистрибутивах Linux.

Данный шаг в сторону самостоятельности и независимости в сфере информационных технологий является важным. Однако, эти системы не совместимы с Microsoft Windows, что влечёт за собой проблемы совместимости

существующего программного обеспечения и необходимость адаптации пользователей к новым принципам работы.

Проблема совместимости и замены программного обеспечения лежит в зоне ответственности разработчиков, но задача подготовки и обучения пользователей работе с новыми операционными системами требует уже комплексного подхода со стороны системы образования (как школьного, так и вузовского).

Переход на отечественные операционные системы может быть сложным процессом, но он также открывает возможности для развития местной индустрии программного обеспечения и подготовки специалистов, способных работать с новыми технологиями.

Личный опыт преподавания основ использования информационных технологий в вузе выявил ряд препятствий, которые могут затруднить процесс обучения работе с отечественным программным обеспечением. Рассмотрим каждое из них:

1. Привычки пользователей: Многие пользователи привыкли к продуктам Microsoft, особенно к операционной системе Windows, что является результатом длительного доминирования этой системы на рынке благодаря её интуитивно понятному интерфейсу, активному продвижению в сфере образования, а также широкому использованию в сферах домашнего развлечения и досуга.

2. Квалификация педагогических работников: педагогические работники, как и обучающиеся, зачастую привыкли к определённым программным продуктам и могут испытывать трудности при переходе на новые системы. Централизованное обучение в рамках курсов повышения квалификации педагогических работников может помочь в данном вопросе, но даже оно может столкнуться с рядом проблем:

Во-первых, многие педагогические работники люди достаточно возрастные, и за годы своей работы выработали устойчивые навыки использования конкретного набора программ, причем зачастую даже каких-то

конкретных версий. Как следствие, данные люди имеют сложности с освоением новых и не привычных принципов и приемов работы с вычислительной техникой и программным обеспечением.

Во-вторых, пандемия COVID-19 привела к увеличению доли дистанционного обучения в сфере повышения квалификации, что имеет как свои преимущества, так и недостатки. Отсутствие непосредственного контакта с преподавателем и необходимость самостоятельной работы могут снижать эффективность обучения, особенно когда речь идет о практических навыках [5]. К тому же, для успешного освоения новых программ необходимо выделять достаточное количество времени (от 4 до 6 часов в день, согласно типовым рабочим программам повышения квалификации), что практически невыполнимо при проведении занятий без отрыва от работы. Очные курсы повышения квалификации могут предложить более эффективный подход к практическому обучению, так как они, с одной стороны – позволяют преподавателям непосредственно контролировать процесс практического обучения, а с другой – гарантируют достаточное выделение времени на освоение учебного курса.

3. Общая ИТ-инфраструктура: Десятилетиями инфраструктура образовательных учреждений была настроена на использование определённой информационной экосистемы [6], основанной на продуктах Microsoft. Изменение этой экосистемы требует значительных временных и финансовых затрат на поиск аналогов и перенастройку всей ИТ-инфраструктуры.

Для преодоления этих препятствий потребуются комплексный подход, включающий обновление учебных программ, методическую поддержку и возможно, государственную поддержку в переходе на отечественные операционные системы. Это также может включать разработку более интуитивно понятных интерфейсов для отечественного программного обеспечения, чтобы облегчить процесс адаптации пользователей.

Значительно лучше обстоят дела в области поиска отечественных аналогов для офисных пакетов программного обеспечения. Такие отечественные

продукты как «МойОфис», «Р7-Офис» и др., предлагают альтернативы зарубежным решениям, и хотя они могут уступать по некоторым параметрам, разработчики активно работают над их улучшением.

Обучение работе с отечественными офисными пакетами осуществляется значительно проще, чем с операционными системами благодаря схожести графических интерфейсов и стандартным элементам управления.

Обобщая результаты анализа возможностей перехода на отечественные программные решения нужно сказать, что чисто технически замена возможна и имеется достаточное количество российских программных продуктов для внедрения их в образовательный процесс. Самая большая сложность импортозамещения данного вида программного обеспечения кроется в преодолении повседневных привычек работы обучающихся и освоении новых программных продуктов непосредственно педагогическими работниками.

Планомерное и централизованное изменение учебных программ, разработка новых учебных и методических материалов, а также своевременное обучение педагогических работников – ключевые шаги для успешного перехода на отечественные решения. Это поможет не только в импортозамещении, но и в подготовке специалистов, способных работать с широким спектром цифровых технологий.

Литература

1. Руденко М.Н., Чернявский С.В., Чернявский В.С., Субботина Ю.Д. Импортозамещение информационно-коммуникационных технологий в России // Вестник Томского государственного университета. Экономика. 2022. №58. С.77-87.

2. Приказ Минкомсвязи России от 29.06.2017 N 334 «Об утверждении методических рекомендаций по переходу федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения» [Электронный ресурс]. URL: <https://digital.gov.ru/ru/documents/5635/>.

3. Указ Президента РФ от 30 марта 2022 г. N 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001202203300001>

4. Единый реестр российских программ для электронных вычислительных машин и баз данных. [Электронный ресурс]. URL: <https://reestr.digital.gov.ru/reestr> (Дата обращения 20.05.2024).

5. Бакулин В.М. Анализ проблем перехода к дистанционным формам обучения в вузе // Современные проблемы науки и образования. – 2021. – № 1.; URL: <https://science-education.ru/ru/article/view?id=30476> (дата обращения: 20.05.2024).

6. Григорьев В.К., Бирюкова А.А., Овчинников М.А. Инфраструктурная поддержка импортозамещения программного обеспечения // Открытое образование. 2018. Т.22 №3. С.52-60; DOI: <https://doi.org/10.21686/1818-4243-2018-3-52-60>.

Сведения об авторе

Бакулин Василий Михайлович, кандидат физико-математических наук, доцент кафедры информатики и математики Волгоградской академии МВД России.

Богачева Мария Валерьевна

**ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ
ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В
АДМИНИСТРАТИВНОЙ И ОПЕРАТИВНОЙ ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

Активная цифровизация деятельности российской полиции в XXI веке принципиально меняет многие подходы и особенности функционирования органов внутренних дел. МВД России вместе со всей страной и другими правоохранительными органами активно внедряет различные новые информационные технологии, в том числе технологии искусственного интеллекта.

С одной стороны, появление новых информационных технологий приводит к активизации преступного сообщества, использованию данных технологий для совершения преступлений. Преступность мигрирует в Интернет, количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий ежегодно растет и по состоянию на 2023 год уже более трети преступлений совершается с использованием ИТТ.

Однако, с другой стороны внедрение новых технологий позволяет интенсифицировать деятельность органов внутренних дел, сделать ее более эффективной. Уход от ручной обработки большого количества информации, использование технологий больших данных, робототехнических устройств, беспилотников и других информационных технологий позволяет принципиально изменить деятельность полицейских и сделать ее удобной и современной.

Цифровизация направлена как на информатизацию управленческой деятельности, так и на предупреждение, раскрытие и расследование преступлений. Кроме того, внедрение информационных технологий затронуло все направления деятельности органов внутренних дел, но наиболее активно используется в сфере оказания государственных услуг населению и в контроле дорожного движения.

Одним из основных направлений цифровизации правоохранительных органов в целом и МВД России, в частности, является внедрение технологий искусственного интеллекта, в том числе нейронных сетей. Данная деятельность осуществляется на основании:

- Указа Президента РФ от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом»;
- Распоряжения Правительства РФ от 20.05.2023 № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года»;
- Распоряжения Правительства РФ от 16.03.2024 № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления»;
- Распоряжения МВД России от 25.01.2024 № 1/724 «Об утверждении Ведомственной программы цифровой трансформации Министерства внутренних дел Российской Федерации на 2024 год и плановый период 2025 - 2026 годов» и других нормативных правовых актов.

В соответствии с указанными документами к основным направлениям применения технологий искусственного интеллекта (ИИ) и больших данных (БД) относятся:

1. Обеспечение оперативного сбора, обработки и качественного анализа больших объемов структурированных и неструктурированных данных из множества различных источников (ведомственных баз данных, баз данных других государственных органов власти, социальных сетей и т.д.).
2. Применение в целях повышения эффективности раскрытия и расследования преступлений (в том числе, киберпреступлений).
3. Технология распознавания лиц, основанная на алгоритмах машинного обучения анализа черт лица и сравнения их с базой данных известных лиц.

Заместителем Министра внутренних дел Российской Федерации генерал-полковником полиции В.Д. Шуликой утвержден Комплекс мероприятий внедрения технологий искусственного интеллекта в деятельность органов внутренних дел Российской Федерации (на 2023-2025 годы). Указанный Комплекс мероприятий предполагает, в том числе:

- выработку предложений по внедрению ИИ-технологий в информационные системы и сервисы МВД России;
- формирование наборов данных (датасетов) для обучения и тестирования нейросетевых моделей;
- упорядочивание информационных систем и сервисов МВД России с учетом входящих в их состав ИИ-решений и др.

На наш взгляд и в соответствии с Комплексом мероприятий, требуется несколько уточнить первое направление использования искусственного интеллекта и технологий больших данных в деятельности российской полиции, которым является анализ информации, накопленной в базах и банках данных органов внутренних дел в оперативных целях.

Необходимо отметить, что общий объем информационных ресурсов министерства составляет триллионы записей. В этой связи обычный поиск по запросам становится неэффективным. Кроме того, множество информационных ресурсов не связано между собой и содержится в разных базах данных. В деятельность МВД России внедрены и используются сервисы ИСОД МВД России, автоматизированные информационные банки данных «Регион» и «Федеральная часть», программно-технический комплекс «Розыск-Магистраль», автоматизированные системы криминалистической регистрации («Папилон», «Арсенал») и другие информационные ресурсы [1].

Созданы и используются различные специализированные информационные поисковые системы, направленные на сопровождение экономических преступлений («Блок»), позволяющая установить связи в преступном сообществе («Спрут»), объединяющая информацию о хищениях

денежных средств из хранилищ («Сейф»), помогающая в расследовании серийных убийств («Маньяк») и другие [2].

Однако, несмотря на имеющиеся гигантские объемы информации, качество поиска не растет. Это обусловлено спецификой накопленной информации, которую требуется анализировать не только по формальным признакам, но и по явным и неявным связям. Как справедливо отмечает В.В. Конюшев «большие данные в контексте правоохранительной деятельности преимущественно характеризуются не только большим объемом, но прежде всего многосвязной сложностью, определяемой, в том числе, необходимостью учета причинно-следственных связей на предшествующих этапах формирования информации» [3]. То, что с блеском проделывает человеческий мозг опытного оперативного сотрудника пока не может сделать искусственный интеллект.

В перспективе первое направление использование ИИ в деятельности полиции должно реализоваться в едином механизме поиска лица, его связей, родственников и друзей, имущества и финансов, используемого транспорта. Необходимо создание такой системы поиска, которая использовала бы информацию не только накопленную в МВД России, в том числе межгосударственный банк данных, но и информацию из налоговых органов, Росреестра, ФСИН России, ФССП России и иных источников. Искусственный интеллект должен заменить человека-оператора и обеспечить выстраивание полной системы жизни и деятельности лица, которое подозревается в совершении преступления, в том числе его социальных сетей, мессенджеров и иных информационных контактов. Для получения существенной части вышеуказанной информации требуется получение судебной санкции на проведение оперативно-розыскных мероприятий. В этой связи указанная система должна иметь закрытый характер, а работа в ней находиться под контролем руководителя оперативного подразделения в органе внутренних дел.

Специалисты отмечают, что в ближайшие годы также возможно внедрение технологий ИИ и БД для:

- контентного и семантического анализа текстов, в том числе для оценки психологического состояния их авторов и скрытых смыслов, заложенных в сообщениях;
- аутентификации субъектов доступа к компьютерной информации по клавиатурному почерку;
- установления криминалистически значимых фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений;
- выявление признаков серийности преступлений;
- интеллектуальной поддержки планирования и принятия управленческих решений по проведению оперативно-профилактических и оперативно-розыскных мероприятий;
- распознавания транзакций и сделок, имеющих признаки отмывания денежных средств, полученных преступным путем, финансирования терроризма, а также операций на нелегальных рынках;
- построения виртуальных моделей мест преступления и их физического моделирования на основе 3D печати;
- анализа действующих и разрабатываемых нормативных правовых актов на предмет наличия коллизий и выработки предложений по совершенствованию;
- создания киберфизических систем, основанных на интеграции вычислительных и физических синергетически увязанных ресурсов и др. [4]

Кроме того, на наш взгляд, имеется реальная перспектива внедрения в деятельность органов внутренних дел технологий искусственного интеллекта в помощь в деятельности конкретных подразделений и служб.

Например, деятельности участковых уполномоченных полиции при составлении паспорта участка. Для составления указанного документа и ведения его в электронном виде, как базы данных, участковый уполномоченный должен

потратить сотни или тысячи человеко-часов для получения информации. Однако, большая часть требуемой информации содержится или в информационных ресурсах МВД России, или доступна по запросу в других министерствах и ведомствах.

Работу по получению и структурированию указанной информации вполне может выполнить ИИ. Для этого требуется разработка модели паспорта участка и обучение нейросети на нескольких примерах. Потребуется несколько вариантов паспорта участка: в крупном городе, малом городе и в сельской местности. Сбор информации о проживающих лицах, торговых и промышленных предприятиях, государственных организациях на территории участка может быть выполнен в автоматическом режиме. Для этого нейросети достаточно указать адреса домов и требуемые сведения. Причем собираемая информации, в отличие от первого направления использования ИИ, является полностью открытой или содержится в информационных ресурсах министерства.

Резюмируя вышесказанное, можно констатировать, что массовое внедрение технологий искусственного интеллекта в деятельность органов внутренних дел в ближайшие годы неизбежно. При этом в настоящее время основными направлениями для внедрения являются частные отдельные задачи, которые позволяют улучшить работу сотен или тысяч сотрудников, однако не затрагивают деятельность большинства сотрудников. Представляется, что разработка единой системы анализа и поиска информации о лицах, подозреваемых в совершении преступлений, позволит принципиально улучшить раскрываемость преступлений. Кроме того, разработка частных решений по применению технологий ИИ в деятельности отдельных подразделений может существенно облегчить им выполнение служебных обязанностей. Например, автоматизированное создание паспорта участка способно кардинально изменить деятельность участкового уполномоченного полиции. На наш взгляд технологии

ИИ и БД должны внедряться там, где они способны улучшить и облегчить работу десятков и сотен тысяч сотрудников МВД России.

Литература

1. Транспортная безопасность: информационное и техническое обеспечение: учебное пособие / А.Н. Александров, П.Н. Жукова, А.Н. Прокопенко [и др.]. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2022. – 176 с.

2. Гордеев А.Ю. Перспективы развития и использования искусственного интеллекта и нейросетей для противодействия преступности в России (на основе зарубежного опыта) // Научный портал МВД России. 2021. № 1. С. 123-135.

3. Конюшев В.В. Основные направления и специфика применения технологий искусственного интеллекта в информационно-коммуникационной системе цифровой полиции // Охрана, безопасность, связь. 2020. № 5-3. С. 75-80.

4. Проект Концепции использования искусственного интеллекта в деятельности подразделений МВД России // Искусственный интеллект на службе полиции: сборник статей Международной научно-практической конференции, Москва, 27 мая 2021 года / Академия управления МВД России. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2021. – С. 94-116. – EDN HZKXYC.

Сведения об авторе

Богачева Мария Валерьевна, старший преподаватель кафедры административно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина.

**Бокадаров Станислав Александрович,
Даниленко Владислав Алексеевич**

АНАЛИЗ СПОСОБОВ ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННЫМ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Актуальность противодействия современным угрозам информационной безопасности связана с повышенной активностью злоумышленников и учащением случаев утечки конфиденциальной информации из организаций, личных данных пользователей. При этом способы атак злоумышленников становятся всё более сложными и профессиональными. В связи с этим возникает необходимость своевременного изучения существующих и потенциальных угроз информационной безопасности, а также разработки эффективных мер противодействия им (рис. 1).

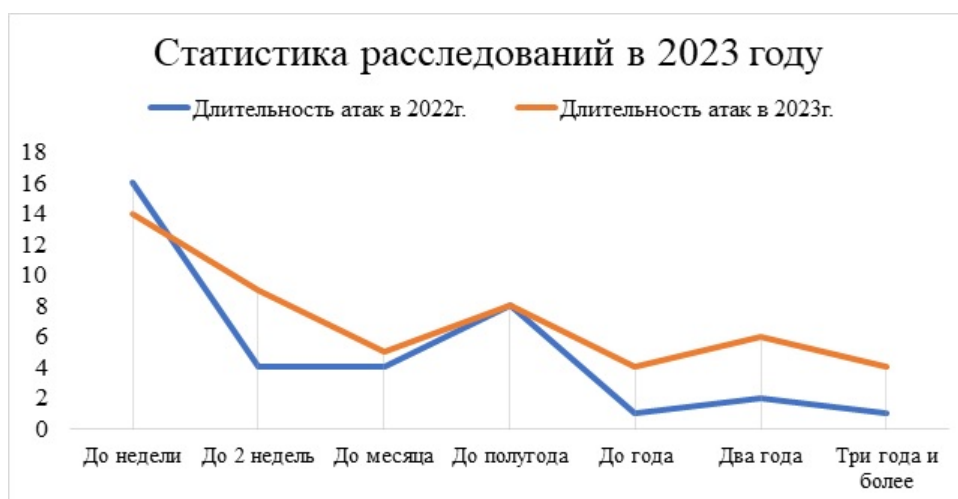


Рис. 1. Статистика длительности атак

Из статистики за 2022 и 2023 год видно, что длительность атак злоумышленников увеличилась. Они больше не стремятся к быстрым и массовым атакам, как это было раньше. Злоумышленники переходят к точечным ударам по системам безопасности. Их незаконные действия направлены на конкретные цели. Это связано с тем, что системы безопасности стали более совершенными, и массовые атаки часто оказываются неэффективными. Такая тактика требует от злоумышленников тщательной подготовки и планирования. Они должны провести разведку, чтобы определить слабые места своей цели и

затем провести атаку. Для полного анализа современных тенденций киберугроз приведём статистику способов атак за 2022-2023 год [1] (рис. 2).

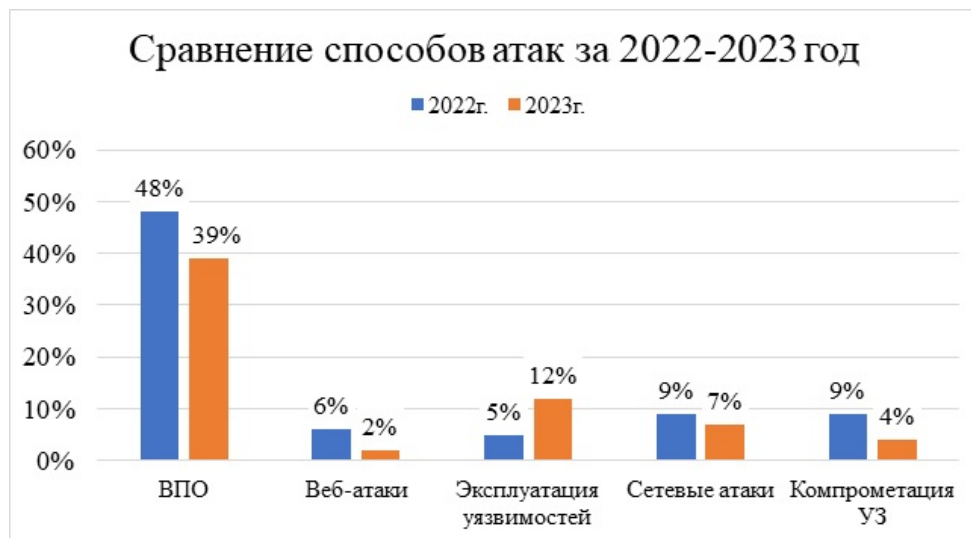


Рис. 2. Сравнение способов атак за 2022-2023 год

Самым заметным изменением в приоритетах злоумышленников стало сокращение использования вирусного программного обеспечения на 9% по сравнению с прошлым годом. При этом они стали гораздо чаще использовать уязвимости в системах безопасности и защитных программах. Данный показатель увеличился на 7%. Смена фокуса злоумышленников связана с несколькими факторами. Так, например, они научились использовать уязвимости в отечественном программном обеспечении, которых не меньше, а иногда и больше, чем в западных аналогах. Другой причиной можно назвать развитие технологий и систем безопасности, которые не позволяют им продолжать действовать как раньше.

К самым распространённым способам противодействия угрозам информационной безопасности относят:

- 1) шифрование и хеширование информации, использование криптографических методов её защиты;
- 2) использование программ-антивирусов;
- 3) обучение сотрудников с правилами обращения с конфиденциальной информацией;

4) организация контроля доступа к серверным помещениям и физической защиты сетевой инфраструктуры.

Шифрование информации – метод защиты информации, который используется для сокрытия данных с использованием алгоритмов. Это фундаментальный раздел криптографии. Он считается наиболее популярным среди других способов защиты информации и при этом наиболее эффективным. Обычно его используют для защиты частной информации, конфиденциальности данных и повышения безопасности обмена данными между клиентскими приложениями и серверами. Стоит различать между собой шифрование и хеширование. Хеширование – это преобразование входных данных в уникальную последовательность символов, из которой невозможно получить исходное сообщение. Примером его использования является проверка целостности данных. Если изменить в исходном файле или тексте хоть один бит, то в результате получается новая уникальная последовательность. Таким образом, при передаче сообщения через интернет шифрование используется, чтобы передаваемую вами информацию не смогли прочесть посторонние пользователи, а хеширование используется, чтобы никто не смог изменить ваше сообщение.

Антивирусные программы работают в фоновом режиме, сканируя файлы на наличие угроз. Это позволяет им быстро реагировать на новые угрозы и обеспечивать высокий уровень защиты. Важно помнить, что антивирусные программы не только обнаруживают и удаляют вредоносные программы, но и предупреждают о возможной угрозе в режиме реального времени. Они могут блокировать доступ к потенциально опасным веб-сайтам, проверять входящую почту на наличие вирусов, а также защищать от атак со стороны злоумышленников.

Российский информационно-аналитический центр Anti-Malware.ru проводил проверку 20 самых популярных комплексных персональных антивирусных программ. По итогам теста, самыми надёжными антивирусными

продуктами оказались Kaspersky Internet Security 2011 и Dr. Web Security Space 6.0. В этом исследовании эксперты проверяли множество различных аспектов защиты и в итоге получили результаты в 100% и 99% защиты соответственно [2].

Организация контроля доступа к серверным помещениям и физическая защита сетевой инфраструктуры являются критически важными аспектами обеспечения безопасности информационных систем. Контроль доступа включает в себя ограничение доступа к серверным помещениям и сетевому оборудованию только авторизованному персоналу. Это достигается путем использования систем контроля и управления доступом, которые могут включать в себя электронные замки, считыватели карт доступа, биометрические системы аутентификации и другие технологии. К другим способам защиты сетевой инфраструктуры относят установку охранных систем, видеонаблюдения и систем оповещения о вторжении [3].

Из анализа способов противодействия угрозам информационной безопасности можем сделать вывод, что ни один из представленных методов защиты не может обеспечить максимальную защищённость отдельно от других. Используя самые передовые криптографические методы шифрования, мы не можем обеспечить безопасность данных в организации при плохой организации контроля доступа к серверам. Злоумышленники могут завладеть данными, скопировав их на внешний носитель информации. Поэтому очень важно уделять внимание обучению сотрудников правилам обращения с конфиденциальной информацией. Оно включает в себя не только изучение правовой основы конфиденциального делопроизводства, но и ознакомление с возможными угрозами, методами работы злоумышленников, структурой системы защиты и порядком работы с конфиденциальными сведениями. Обучение также направлено на формирование у сотрудников понимания необходимости выполнения требований по защите любой конфиденциальной информации и приобретение навыков работы с ней. Регулярное повышение квалификации

сотрудников и совершенствование методик обучения позволяют поддерживать высокий уровень защиты информации в организации.

Литература

1. Атаки на российские компании во II квартале 2023 года // Solar URL: <https://rt-solar.ru/analytics/reports/3610/> (дата обращения: 02.06.2024).
2. Тесты антивирусов // Anti-Malware URL: https://www.anti-malware.ru/antivirus_tests (дата обращения: 05.06.2024).
3. Бокадаров С.А. Передовые технологии как угроза информационной безопасности / С.А. Бокадаров, М. А. Гудков, А.Н. Перегудов, А.А. Симонова // Актуальные проблемы деятельности подразделений УИС. – 2020. – С. 330-332.

Сведения об авторах

Бокадаров Станислав Александрович, кандидат технических наук, доцент кафедры безопасности информации и защиты сведений, составляющих государственную тайну Воронежского института Федеральной службы исполнения наказаний.

Даниленко Владислав Алексеевич, курсант Воронежского института Федеральной службы исполнения наказаний.

**Будиловская Дарья Евгеньевна,
Степанов Сергей Анатольевич**

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОБРАБОТКЕ РЕЗУЛЬТАТОВ АНКЕТНЫХ ДАННЫХ

Профессиональный психологический отбор – это один из видов профессионального отбора и представляет собой систему мероприятий, где широко используется анкетирование, и как следствие обработка анкетных данных.

Автоматизация обработки анкетных данных при помощи искусственного интеллекта представляет собой эффективный способ сокращения времени и минимизации ошибок, которые могут возникнуть в процессе ручной обработки. Различные этапы обработки данных, начиная с ввода информации в систему и заканчивая анализом и выводами, могут быть значительно ускорены благодаря использованию алгоритмов искусственного интеллекта.

Кроме того, автоматизированный подход к обработке анкет позволяет снизить вероятность возникновения ошибок на различных этапах, что способствует повышению качества и достоверности результатов исследования. В этом случае на помощь приходят технологии искусственного интеллекта. С их помощью можно автоматизировать процесс обработки данных, ускорить его и уменьшить вероятность возникающих ошибок.

Искусственный интеллект – это область науки, которая быстро развивается и постоянно усовершенствуется. Сам по себе искусственный интеллект является областью компьютерных наук, то есть создание алгоритмов и систем, в основе которых находятся базовые математические принципы [3].

На основе искусственного интеллекта разработаны технологии распознавания документов, такие как OCR и машинное обучение. Именно эти технологии могут автоматизировать процесс ввода и анализа анкет, сокращая затраты времени и ресурсов.

Инструментарий исследователя должен обязательно включать в себя современные методы и технологии обработки больших массивов, как структурированных, так и неструктурированных данных. К одному из таких методов относятся искусственные нейронные сети, которые обладают широкими функциональными возможностями. Применения искусственных нейронных сетей для обработки информации актуально в наше время. Их основное преимущество перед классическими методами многомерной статистики заключается в том, что не накладываются ограничения на исходные данные, т.е. не требуется наличия нормального распределения или линейной зависимости между переменными.

Кроме того, нейронные сети способны обрабатывать данные, представленные в разных шкалах, что является важным при работе с анкетными данными. Задача настоящей статьи – продемонстрировать возможности искусственных нейронных сетей для обработки результатов анкетирования.

В качестве метода исследования был использован аппарат самоорганизующихся карт признаков Кохонена, который позволил сформировать и описать группы респондентов, давших сходные ответы по вопросам.

Самоорганизующиеся карты признаков Кохонена (СКП Кохонена) – это одна из разновидностей нейронных алгоритмов с обучением без учителя. Они используются для решения задач векторной классификации. В качестве первоначальных данных метода выступает набор объектов, каждому из которых сопоставлен вектор значений признаков. Необходимо разбить исходное множество на кластеры, т.е. для каждого объекта найти свой кластер, к которому он будет принадлежать.

Данный метод позволит решить задачу классификации новых объектов, но не позволяет строить основные правила классификации. Поэтому в совокупности с СКП Кохонена могут быть использованы деревья классификации.

Метод деревьев классификации (ДК) позволяет изучить статистическую связь между одной зависимой и группой независимых переменных, а также определять принадлежность объектов тому или иному классу в зависимости от значений переменных, характеризующих объекты.

На сегодняшний день разработано большое число алгоритмов, позволяющих реализовывать деревья классификаций. Самые популярные из них это алгоритмы CART, C4.5, QUEST, CHAID.

Методика комбинация СКП Кохонена и ДК позволит выработать эффективный алгоритм структурирования и анализа информации, который включает в себя два этапа: разбиение множества объектов на кластеры и применение ДК для построения наглядного решающего правила распределения объектов.

К примеру, база данных с результатами анкетирования включает в себя более 140 переменных (вопросов) различного типа (категориальные, логические, интервальные, порядковые и другие) и более 5000 записей. В качестве инструментария исследования использовался пакет STATISTICA. [1]

На первом этапе из базы данных необходимо отобрать переменные, включающие в себя вопросы, касающиеся сформулированной выше задачи исследования, и социально-демографические характеристики респондентов. Далее проводится процедура предобработки данных, состоящая из удаления записей, содержащих ошибки, записей, содержащих пропуски по вопросам, относящимся к задаче исследования. В результате можно сформировать выборку из 2300 записей.

Анализ карт Кохонена позволяет описать каждый кластер и выявить его особенности.

Модуль кластеризации с использованием самоорганизующихся карт признаков Кохонена в программе STATISTICA позволяет наряду с задачей разбиения объектов на группы решать задачу классификации новых объектов.

В контексте искусственного интеллекта в современном мире можно выделить выдающийся пример - Chat GPT, разработанный компанией OpenAI. Эта модель подразумевает генерацию текста и построена на основе технологии Transformer. Она обучена на обширном корпусе данных и является одним из самых передовых достижений в области обработки естественного языка.

Сама аббревиатура GPT расшифровывается как Generative Pretrained Transformer, что означает «генеративный предварительно обученный трансформер». Другими словами модели GPT генерируют новый текст, к тому же они не просто анализируют данные, а создают оригинальные тексты. Эта способность лежит в основе инструментов вроде ChatGPT, Claude и Gemini, которые способны порождать связные тексты на основе небольших промптов.

Как это работает? Пользователь вводит вопрос, а модель формулирует ответ, учитывая заданный контекст. Формируя ответ, модель предсказывает следующее слово или фразу на основе вероятности, вычисленной с помощью ее обучения.

Уже сейчас множество научных исследований с применением методов искусственного интеллекта активно участвуют в процессе сбора информации путем заполнения анкет. Тем не менее, специалисты не могут прийти к общему мнению относительно их эффективности. За последние годы роботы, использующие такие алгоритмы, претерпели значительные изменения. В компании Vox populi были проведены эксперименты, связанные с проведением интервью при помощи простого чат-бота в Telegram, который был разработан на языке программирования Python. Основная идея работы такого бота заключается в том, что ChatGPT задавал задания по проведению опросов на определенную тему с возможностью задавать уточняющие вопросы, а Telegram использовался в качестве платформы для взаимодействия с пользователем, отображения вопросов и получения ответов. Все заданные вопросы и полученные ответы были сохранены в базе данных. Такой подход позволил проводить несколько простых

интервью быстро, так как одновременно приглашалось и опрашивалось большое количество участников.

После завершения сбора информации необходимо приступить к анализу данных. Если возникают задачи по анализу данных в программе SPSS или необходимо выполнить определенные вычисления, можно запросить у ChatGPT написание соответствующего синтаксиса. То же самое можно сделать, если требуется программный код для анализа данных на языках Python или R. Это может значительно ускорить процесс обработки результатов анкетирования.

Возможности применения искусственного интеллекта в прикладных исследованиях на сегодняшний день очень широки. Такие технологии создают новые перспективы, но вносят и новые вызовы, которые необходимо будет преодолеть в будущем:

1. Обеспечение конфиденциальности данных, справедливости и избежание предвзятости при работе с алгоритмами.

2. Качество данных: искусственный интеллект требует большого объема данных для обучения алгоритмов и достижения высокой точности и надежности результатов.

3. Применение искусственного интеллекта может усложнить интерпретацию полученных результатов и выводов.

4. Предвзятость результатов: неправильное использование искусственного интеллекта может привести к непредсказуемым или нежелательным последствиям.

5. Понимание контекста: важно помнить, что искусственный интеллект может иметь ограниченное понимание социокультурного контекста, что может повлиять на результаты исследования.

Технологии искусственного интеллекта позволяют эффективно обрабатывать большие объемы информации, выявлять скрытые закономерности, проводить сложные статистические анализы и делать предсказания на основе полученных результатов.

Таким образом, результаты данного исследования позволяют утверждать, что применение искусственного интеллекта при обработке результатов анкетных данных является перспективным направлением развития научных исследований и практических приложений для обработки данных военнослужащих различных воинских частей, соединений, а также Высших военных учреждений.

Литература

1. Синицын Е.В. Магистерская диссертация «Применение искусственного интеллекта при обработке анкетных данных», ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина» г.Екатеринбург, 2018 – 101 с.
2. Фомина Е.Е. научная статья «Применение аппарата нейронных сетей для анализа результатов анкетирования», ФГБОУ ВО «Тверской государственный университет» г.Тверь, 2020 – 12 с.
3. Шилина М.Г., Левченко В.Ю. BIG DATA, OPEN DATA, LINKED DATA, метаданные в PR: актуальные модели трансформации теории и практики // Медиаскоп. – 2014. – № 1. – С. 16.

Сведения об авторах

Будиловская Дарья Евгеньевна, преподаватель кафедры математики (и математических основ криптографической защиты информации) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Степанов Сергей Анатольевич, курсант Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

**Воронцов Глеб Олегович,
Коваленко Анна Владимировна**

КЛАССИЧЕСКИЕ МЕТОДЫ ОПТИМИЗАЦИИ ДЛЯ АВТОМАТИЗИРОВАННОЙ КОМПОНОВКИ ГЕНЕРАЛЬНОГО ПЛАНА ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Предлагается подход к автоматизации генерального плана с помощью классических методов оптимизации: метода полного перебора, метода ветвей и границ, методов теории графов и метода градиентного спуска. Автоматизация генплана позволит существенно повысить эффективность процесса проектирования: увеличение скорости принятия решений, ускорение выполнения задач размещения объектов на территории предприятия, улучшение качества проектной документации.

Автоматизация является неотъемлемой частью современного проектирования. Она ускоряет процесс создания проектной документации, сокращает расходы на ручной труд, освобождая специалистов от выполнения рутинных задач и позволяя им сосредоточиться на решении более значимых вопросов. Классические методы оптимизации позволяют точно определить наилучшее расположение объектов (зданий, сооружений и др.) на генеральном плане, учитывая различные ограничения и цели [1, 2]. Исследования [3, 4] подробно освещают проблемы планировок производственных объектов.

Метод полного перебора.

Метод полного перебора предполагает изучение каждого возможного варианта размещения объектов с целью достижения оптимального результата. Метод проверяет все возможные комбинации и гарантирует нахождение абсолютно точного решения. Тем не менее, алгоритм обладает высокой вычислительной сложностью, что делает его неэффективным для задач с большим количеством объектов. Метод может быть полезен для тестирования других алгоритмов на небольших наборах данных, чтобы убедиться в корректности их работы. Однако для практического применения в условиях

большого количества информации, обычно рассматриваются более продвинутые методы.

Метод ветвей и границ.

Метод ветвей и границ позволяет эффективно решать оптимизационные задачи, где прямой перебор всех возможных вариантов является слишком затратным по времени. Этот метод существенно сокращает количество перебираемых вариантов за счет исключения целых групп неоптимальных решений.

Для выполнения алгоритма необходимо определить начальное расположение объектов на генеральном плане, например, с помощью эвристического метода. Начальное расположение будет являться ориентиром для дальнейшего улучшения, способствуя более эффективному и целенаправленному поиску оптимального решения. Имея начальный генеральный план, можно быстрее исключать неперспективные ветви, так как уже есть представление о возможных решениях и их приблизительной стоимости. Затем выбирается местоположение первого объекта, и создаются ветви для каждого возможного местоположения следующего объекта. Для каждой ветви рассчитывается стоимость расположения объектов, учитывая все ограничения и требования [1, 2]. Исключаются ветви, стоимость которых превышает уже найденное решение. Алгоритм завершается, как только будет найден оптимальный результат или когда все потенциальные ветви будут исследованы и оценены, что позволит исключить необходимость дальнейшего поиска.

Методы теории графов.

Методы теории графов являются эффективным средством для определения оптимального распределения объектов на генеральном плане. В контексте генплана, вершины графа могут представлять различные объекты, тогда как ребра отражают их взаимное расположение.

Метод поиска кратчайшего пути возможно использовать для нахождения самого короткого пути между парой вершин в графе. Метод минимального

основного дерева полезен для определения оптимальной сети связей между объектами с минимальными затратами на их соединение. Метод разбиения графа на компоненты связности формирует подграфы, в каждом из которых любые две вершины соединены путем. При этом такие подграфы не связаны с остальной частью исходного графа. Алгоритм может быть использован для выявления групп объектов, которые образуют независимые кластеры. Также возможно использование и других методов теории графов.

Метод градиентного спуска.

Метод градиентного спуска используется для поиска минимальных значений функций. Данный алгоритм определяет оптимальное размещение объектов с учетом заданных ограничений и целей [1, 2]. Предварительно формируется начальное расположение объектов, например, случайным способом. Для каждого объекта вычисляется градиент функции потерь, указывающий направление наибольшего увеличения функции. Антиградиент определяет направление, в котором необходимо изменить положение объекта. С учетом скорости обучения объект перемещается в сторону антиградиента. Алгоритм завершается после достижения заданного количества итераций или при достаточно малом изменении функции потерь.

Для расположения объектов на генеральном плане были рассмотрены классические методы оптимизации. Считаем, что среди точных методов, представленные алгоритмы являются наиболее применимыми для автоматизации генплана. Для создания программного обеспечения для размещения объектов на территории промышленного предприятия, также необходимо рассмотреть эвристические методы, в том числе применение искусственного интеллекта [5].

Литература

1. Воронцов Г.О., Коваленко А.В., Овсянникова А.В. Математические модели для автоматизированного размещения объектов на территории промышленного предприятия // Энергетика – известия высших учебных заведений энергетических объединений СНГ. 2024. (в печати).

2. Воронцов Г.О., Коваленко А.В. Математические модели для автоматизации генерального плана промышленного предприятия // Прикладная математика: современные проблемы математики, информатики и моделирования: материалы VI Всероссийской научно-практической конференции молодых ученых. 2024. (в печати).

3. Drira, A., Pierreval, H., Hajri-Gabouj S., 2007. Facility layout problems: A survey. Annual Reviews in Control, 31: 255-267.

4. Hosseini-Nasab, H., Fereidouni, S., Fatemi Ghomi, S.M.T., Fakhrazad, M.B., 2018. Classification of facility layout problems: a review study. Int J Adv Manuf Technol, 94: 957-977. <https://doi.org/10.1007/s00170-017-0895-8>.

5. Коваленко А.В., Воронцов Г.О. Оптимизация компоновки завода с помощью алгоритма машинного обучения // Прикладная математика: современные проблемы математики, информатики и моделирования: материалы V Всероссийской научно-практической конференции молодых ученых. 2023. С. 380-383.

Сведения об авторах

Воронцов Глеб Олегович, аспирант Кубанского государственного университета.

Коваленко Анна Владимировна, доктор технических наук, доцент Кубанского государственного университета.

Добровольская Наталья Юрьевна

ТЕХНОЛОГИЯ ЕДИНОЙ ТОЧКИ ВХОДА КАК ОСНОВА АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ РАЗЛИЧНЫХ ПРИЛОЖЕНИЙ

Для современных программ одним из основных требований является обеспечение безопасности данных, качественная реализация приложений требует наличия аутентификации и авторизации. Однако разработка модуля организации безопасности порой требует больше ресурсов, чем конструирование собственно функционала приложения. Следовательно, целесообразно предоставить технологию реализации единой точки аутентификации и авторизации, такая технология называется Single Sign-On (SSO) [2].

Популярным решением обеспечения SSO является технология Keycloak позволяющая организовать процесс аутентификации пользователей различных приложений. Использование технологии с открытым кодом позволяет дополнить имеющийся код приложения функционалом единой точки входа без существенных усилий разработчика. А инженеры DevOps могут организовать интеграцию обращений пользователей к общей базе данных без дополнительных инструментов [1].

Сконструируем собственную технологию единой точки входа, обеспечивающей приложениям следующий функционал: авторизация и аутентификация пользователей; возможность регистрации новых пользователей в системе; возможность подключения к сервису внешних сервисов; объединение подключенных сервисов в одну систему, обеспечение технологии SSO (Single Sign-On); обеспечение безопасности авторизации и аутентификации; возможность администрирования пользователей, присоединенных внешних сервисов и ролей в этих сервисах; привязка email к пользователю и возможность его подтверждения.

Выделим основные компоненты программной реализации предложенной технологии.

1. `backend_service` – серверное приложение, инкапсулирует в себя основную бизнес логику взаимодействия пользователей с внешними сервисами, осуществляет контроль и раздачу JWT, осуществляет отправку сообщения о подтверждении на почту. Используемый стек технологий: TypeScript, Nest.js, TypeORM, GraphQL.

2. `database` – СУБД, хранящая информацию о пользователях, внешних сервисах и их ролях. Стек технологий представлен PostgreSQL.

3. `database_admin_panel` – административная панель доступная только администратору, позволяющая осуществлять взаимодействие с базой данных напрямую и обеспечивающая её мониторинг. Стек технологий представлен pgAdmin.

4. `service_admin_panel` – клиентское приложение, административная панель, реализующая `api backend_service`. Обеспечивает удобный интерфейс для администрирования пользователей, внешних сервисов и ролей. Стек технологий включает TypeScript, React, Apollo Client, MUI.

5. `service_entrpoint` – клиентское приложение, инкапсулирует в себе логику хранения JWT, пересылку JWT на внешние домены или административную панель `service_admin_panel`. Обеспечивает интерфейс для базовой регистрации и авторизации в системе. Стек технологий: TypeScript, React, Apollo Client, MUI.

6. `proxu` – серверное приложение, `api-gateway`, обеспечивает единую точку для взаимодействия с приложением извне. Стек технологий представлен Nginx.

На рисунке 1 представлена основная концепция взаимодействия компонентов системы. Каждый модуль системы интегрируется в отдельный контейнер, который собирается с помощью технологии Docker. Для управления полученным мульти контейнерным приложением используется технология Docker-Compose.

Основная проблема обеспечения безопасности состоит в том, что получение постоянного токена при авторизации приводит к серьезным проблемам с его похищением.

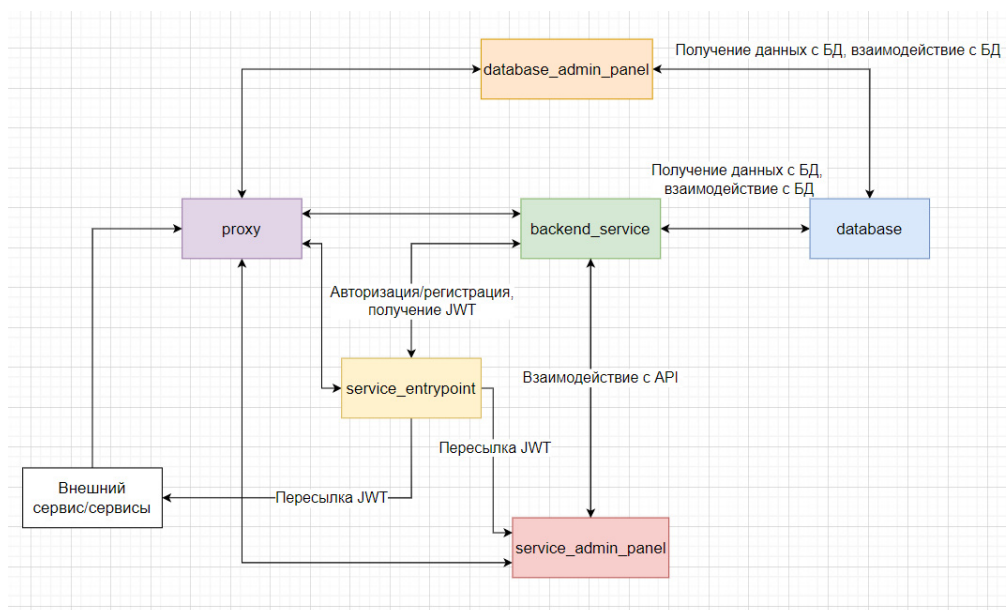


Рис. 1. Взаимодействие компонентов системы

Протокол OAuth2 представил решение, основанное на динамически меняющихся токенах, что позволяет сделать систему надежнее. В предлагаемом решении JWT возможно верифицировать на разных хостах, если они используют один и тот же секретный ключ (рис. 2). Это позволяет реализовать систему со слабой связностью.

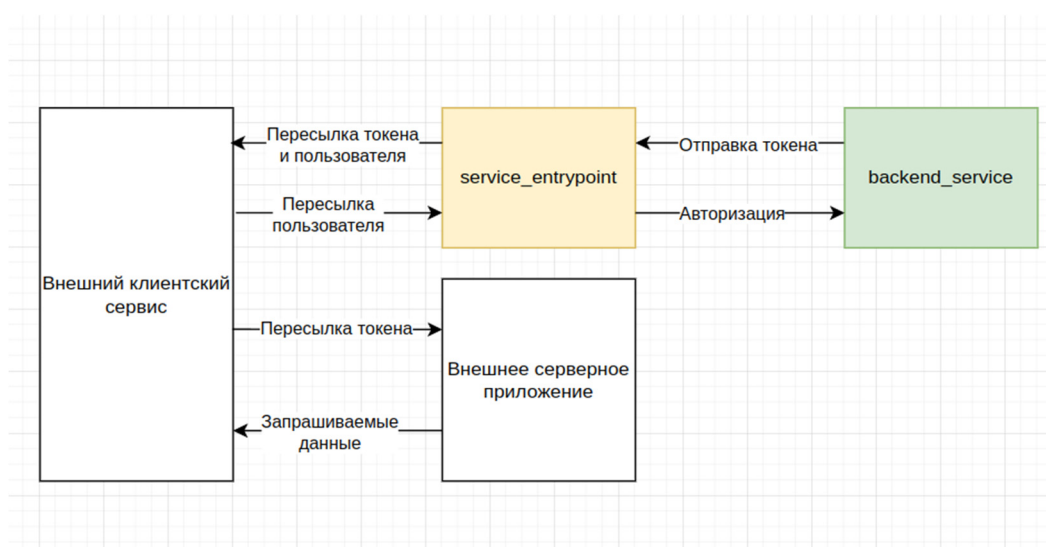


Рис. 2. Принцип использования токена во внешних сервисах

Для обеспечения доступа к одному токenu на разных доменах будем использовать отдельный домен для хранения токена и в случае отсутствия токена на внешнем клиенте перенаправлять пользователя на этот домен (рисунок 3). Этот функционал реализован в `service_entrpoint`.

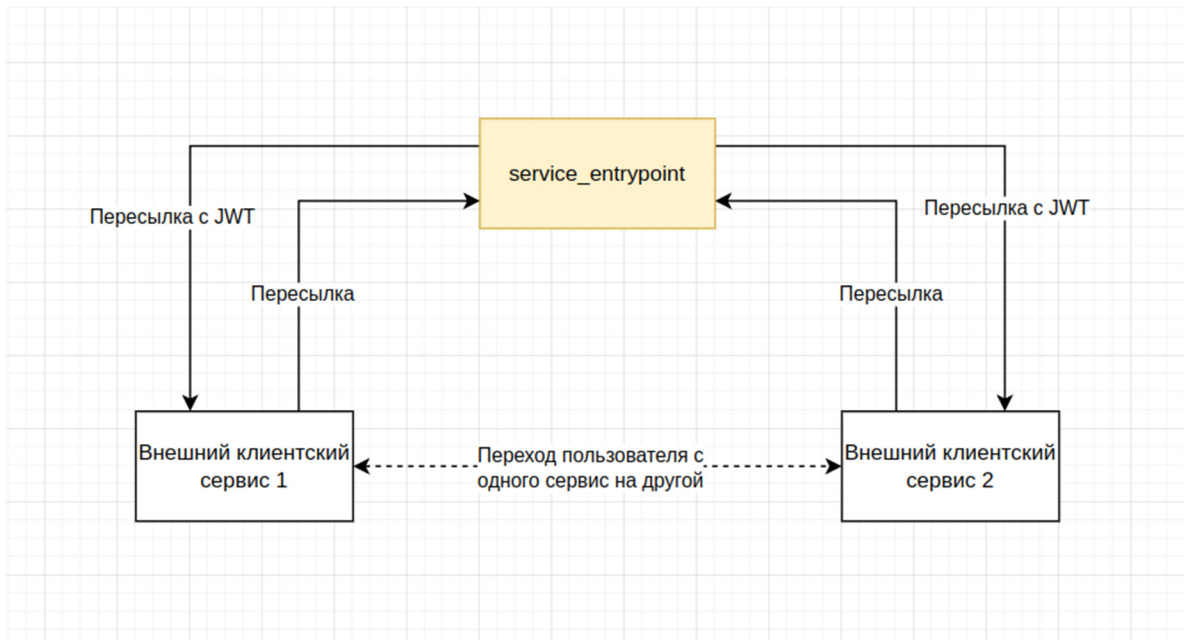


Рис. 3. Принцип обеспечения функционала единой точки входа

Предложенное решение позволяет реализовать единую точку входа, является ядром разработки клиент-серверного веб-приложения, отражающего технологию SSO и администрирование подключенных пользователей.

Литература

1. Билевич А.В. Единая точка входа в личный кабинет // Международный журнал гуманитарных и естественных наук. 2023. №5-1 (80). С. 50-53.
2. Юданов Ф.Н., Федотов А.М., Сейткасым Р.С. Технологии единой авторизации и организации единой точки доступа к информационным ресурсам сети // Вестник НГУ. Серия: Информационные технологии. 2012. №3. С. 117-126.

Сведения об авторе

Добровольская Наталья Юрьевна, кандидат педагогических наук, доцент кафедры информационных технологий Кубанского государственного университета.

**Дрога Андрей Анатольевич,
Чижев Илья Александрович**

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ В МЕРОПРИЯТИЯХ ПО ОБНАРУЖЕНИЮ НАРКОТИЧЕСКИХ ВЕЩЕСТВ

Спектр борьбы с наркопреступностью в настоящее время расширился в сторону информационных систем. Согласно статистике, все больше преступлений, связанных с незаконным оборотом наркотиков и наркотических средств, совершаются посредством использования сети интернет, а именно «теневых сайтов» и мессенджеров [1]. Проблема распространения наркопреступности в различных общественных сферах жизни затрагивает как Правительство Российской Федерации, так и правоохранительные органы. Так как их главной задачей является защита общества от преступных посягательств. Современное развитие информационных технологий расширило спектр возможностей преступников, поскольку теперь они реализуют преступный умысел минуя физические контакты и встречи, путем совершения действия через сеть интернет, что позволяет повысить уровень их анонимности. В связи с этим правоохранительные органы должны не только обладать техническими средствами для предупреждения и раскрытия данных преступления, но и специальными знаниями в области информационных технологий.

Высокий уровень распространения незаконного оборота наркотиков с использованием информационных технологий также связан с тем, что почти у каждого человека в современном мире есть гаджет с выходом в интернет, а также имеются аккаунты в различных социальных сетях (Telegram, WhatsApp, Viber).

В соответствии с законодательством Российской Федерации, пропаганда наркотических средств и их аналогов, уголовно наказуема, а также является одной из основных угроз национальной безопасности [2]. Поскольку она затрагивает не только полностью дееспособных граждан, но также и несовершеннолетних лиц – подростков. Опасность также заключается в том, что подростками гораздо проще манипулировать, в связи, с чем многие из них

вовлекаются в преступную сферу. Основным фактором является материальная выгода.

Так же для своей конфиденциальности в сети интернет, преступники используют специальные приложения, одним из таких является «Changingnumber» [3]. Оно позволяет сохранить анонимность благодаря вымышленным номерам, которые можно приобрести за определенную денежную сумму. Поэтому для борьбы с данными лицами правоохранительным органам нужно использовать информационные технологии и системы, оборудованные под это направление деятельности. Также стоит отметить использование программ, позволяющих сменить IP-адрес своего устройства, что делает вычисление лиц, совершающих преступления, практически невозможным. В связи с этим, современные способы совершения рассматриваемой категории преступлений напрямую связаны с использованием IT-технологий, поэтому способы и методика расследования таких преступлений должны быть модернизированы.

Одним из новых методов, который можно использовать для решения данной проблемы – является модернизация и современное техническое обеспечение оперативно-розыскных методов [4]. Рассмотрим применение данного метода на примере оперативно-розыскного мероприятия – опрос. Его можно использовать в качестве инструмента, для беседы с различными участниками чатов, бесед, групп в различных социальных сетях, тем самым получая информацию, представляющую оперативный интерес, непосредственно из сети интернет. Это является эффективным способом, так как информационное пространство – это «новый мир», к которому нужен свой особый подход. В этом пространстве есть множество сайтов и форумов, где люди пытаются сбыть или приобрести наркотические и психотропные вещества.

Также рассмотрим несколько иной подход к реализации наблюдения. Специально обученный оперативный сотрудник под вымышленным аккаунтом

будет участником данных сайтов или чатов, на которых предполагаемо, реализуется сбыт и приобретение наркотических и психотропных веществ.

Говоря о способах решения рассматриваемой проблемы, отметим, что вторым способом решения проблемы - это безопасное интернет-пространство, а если точнее реализовать легализации сайтов. Создать специальный отдел в правоохранительных органах, который будет заниматься легализацией и присмотром за сайтами, то есть данное подразделение будет заниматься прекращением деятельности тех сайтов, чья активность будет вызывать подозрения, если их деятельность будет оставаться без присмотра. Тем самым начнется очистка интернет пространства от тех участников, чьи мотивы были направлены на реализацию преступной деятельности.

Так же хочется отметить, что сам Интернет-провайдер адреса устройств, подключенных к сети. Например, если распространитель наркотических средств осуществляет свою преступную деятельность через сайт, можно попытаться установить владельца домена, которому он принадлежит.

Каждые страны имеют свои доменные имена:

- региональные (.ru, .su, .ua, .us, .de, .fr и т. д.);
- тематические (.com, .edu, .org, .net и др.);
- национальные (например, .рф).

За Российской Федерацией в настоящее время закреплены два имени:

1) .su – домен, оставшийся со времен Советского Союза и представляющий сегодня пространство ресурсов на русском языке.

2) .ru – домен, изначально закрепленный за Россией и указывающий на то, что сайт расположен в нашей стране.

Существуют домены общего пользования. Они необязательно регистрируются в том государстве, где проживает их создатель. Самые распространенные это:

- 1) .com – для коммерческих проектов;
- 2) .org – для некоммерческих сайтов различных организаций;

- 3) .net – для проектов, связанных с Интернетом;
- 4) .edu – для образовательных учреждений и проектов;
- 5) .biz –исключительно для коммерческих организаций;
- 6) .info – для всех информационных проектов;
- 7) .name – для личных сайтов;
- 8) .gov – для государственных структур.

Каждый из приведенных выше доменов регистрируется в официальных компаниях, которые имеют право на его коммерческое использование, и данные о владельцах в настоящее время получить не сложно.

Третьим способом решения является, который получил свою реализацию в настоящее время, это повышения информированности населения. Данный способ является достаточно эффективным, так как предполагает прямой контакт граждан и сотрудников правоохранительных органов. Квалифицированный сотрудник, который напрямую работает в данном направлении, будет с помощью официальных сайтов правоохранительных органов выкладывать информацию, направленную на обеспечения безопасности граждан в интернет пространстве, и ходить по различным учебным заведениям с лекциями для молодежи [5].

Анализируя современные информационные методы противодействия незаконного оборота наркотических средств, следует отметить, что необходимо усовершенствование законодательной базы, регулирующее данный вопрос, а также технических средств связи. Повысить уровень взаимодействия населения по вопросам распространения наркотических средств, ведь все эти методы будут иметь большое значение в борьбе с наркотическими и психотропными веществами.

Литература

1. Морозов А.В. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий // Научно-практический альманах МВД России «Профессионал». – 2018. – 4. – С.14 - 18.

2. Усманов И.М. Противодействие преступной деятельности организованных преступных групп, связанных с бесконтактным сбытом наркотических средств: учеб. пособ. / И.М. Усманов. – Казань: КЮИ МВД России, 2016. - 90 с.

3. Решняк, О.А. Противодействие новым потенциально опасным психоактивным веществам: проблемы правоприменения / А.А. Лихолетов, О.А. Решняк // Наркоконтроль. - 2015. - № 2 (39). - С. 26-30 (0,64/0,32 п. л.).

4. Решняк, О.А. О некоторых вопросах расследования незаконного сбыта синтетических наркотиков, совершенного бесконтактным способом / О.А. Решняк // Вестник Волгоградской академии МВД России. – 2019. – № 2 (49). – С. 45-50.

5. Билоус Е.Н. Некоторые вопросы деятельности подразделений по контролю за незаконным оборотом наркотиков органов внутренних дел по выявлению сбыта наркотических средств, совершенных бесконтактным способом / Е.Н. Билоус, М.Г. Кублова // Сборник научных статей по итогам Недели Российской науки Рязанском филиале Московского университета МВД России имени В.Я. Кикотя. Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя. – 2020. – С. 9-13.

Сведения об авторах

Дрога Андрей Анатольевич, заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института Министерства внутренних дел Российской Федерации имени И.Д. Путилина.

Чижов Илья Александрович, кандидат юридических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института Министерства внутренних дел Российской Федерации имени И.Д. Путилина.

Дырма Сергей Валерьевич

ПРОТИВОДЕЙСТВИЕ КРАЖАМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время, в условиях активного распространения и повсеместного использования информационных технологий, в том числе банковских счетов и бесконтактных форм оплаты услуг и товаров, достаточно актуальной для деятельности не только органов внутренних дел Российской Федерации, но и правоохранительных органов в целом составляет проблема противодействия кражам, совершаемым с использованием информационно-коммуникационных технологий.

В данной статье нами предлагается рассмотреть вопрос понятия преступления, совершённого с использованием информационно-коммуникационных технологий, особенностей совершения краж с использованием информационно-коммуникационных технологий, а также основные направления противодействия данной категории преступлений.

Развитие средств вычислительной техники, разработка и совершенствование программных продуктов, позволяющих быстро и эффективно обрабатывать огромные объемы данных позволило обеспечить практически каждому из нас оперативный доступ к самой разной информации, максимально упростить нашу жизнедеятельность, например, в области межличностной коммуникации, а также предоставить определенный уровень комфорта в распоряжении финансовыми ресурсами.

В настоящее время необходимость использования наличных денежных средств теряет свою актуальность. Более того, на примере развития онлайн-маркетинга мы можем наблюдать наглядную реализацию механизмов стимулирования к переходу на бесконтактные формы оплаты товаров и услуг. Даже в некоторых видах общественного транспорта выгоднее оплачивать банковской картой, нежели наличными.

Вместе с тем, повсеместное использование электронных средств платежа для оплаты товаров и услуг и в целом тенденция к переходу на бесконтактную форму товарно-денежных отношений определила необходимость не только совершенствование правовых механизмов, не только регулирующих данные отношения, но обеспечивающих более существенную защиту средств, хранящихся на банковских счетах граждан и организаций от преступных посягательств.

В этой связи в 2018 году был принят Федеральный закон № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», которым часть 3 статьи 158 УК РФ была дополнена пунктом «г» - «с банковского счета, а равно в отношении электронных денежных средств».

Если обратить внимание на совместное указание генеральной прокуратуры и МВД РФ «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых в формировании статистической отчетности», то преступления, предусмотренные п. «Г» ч.3 ст.158 УК РФ без дополнительных условий относятся категории совершённых с использованием информационно-коммуникационных технологий. Несомненно, реализовать объективную сторону преступления, выражающуюся в тайном изъятии средств с банковского счета, без использования информационно-коммуникационных технологий попросту невозможно. Оплата товаров в магазине похищенной или найденной банковской картой также не является исключением, поскольку денежные средства списываются с банковского счета по средствам глобальной сети «Интернет», к которой подключен платежный терминал.

По нашему мнению, преступлением совершённым с использованием информационно-коммуникационных технологий следует считать уголовно-наказуемое деяние, объективная сторона которого (либо ее часть) совершена при использовании программных и (или) аппаратных средств дистанционной передачи информации.

Согласно анализу статистических сведений в период с 2018 по 2023 года при общем снижении количества зарегистрированных в Российской Федерации всех видов преступлений на 0,2% (с 1991532 до 1947161), количество зарегистрированных преступлений, совершенных с использованием информационно-коммуникационных технологий увеличилось на 387,5% (с 174674 до 676951).

Если в 2018 году доля IT-преступлений в общей структуре преступности в Российской Федерации составляла всего 8,8%, то по итогам 2023 года указанная доля увеличилась до 34,8%. Таким образом, в настоящее время каждое третье преступление, совершаемое в стране, является IT-преступлением.

Доля краж, совершённых с использованием информационно-коммуникационных технологий в структуре всех видов IT-преступлений по итогам 2023 года составляет 17,6%.

Способы совершения краж рассматриваемой категории достаточно динамичны и многообразны, от использования вредоносного программного обеспечения с целью получения информации, необходимой для доступа к банковскому счету до использования методов социальной инженерии с целью получения конфиденциальной информации от самих граждан.

Социальная инженерия в самом общем своем понимании представляет собой совокупность методик получения конфиденциальной информации, либо доступа к таковой посредством психологического воздействия на человека. Социальная инженерия часто рассматривается как «манипулирование поведением человека с помощью использования социальных и психологических навыков» [4, С.135].

При этом социальная инженерия, по нашему мнению, является наиболее опасным методом с позиции противодействия преступлениям и наиболее эффективным с позиции злоумышленника методом завладения конфиденциальной информацией, необходимой для получения доступа к банковскому счету.

В научных трудах заслуженных ученых неоднократно отмечалось, что психологическая атака обычно очень успешна, потому что самым слабым звеном в компьютерной безопасности часто являются пользователи компьютерных систем [3, С.76].

Рассматривая противодействие кражам, совершаемым с использованием информационно-коммуникационных технологий, как некую систему, следует отметить, что деятельность уполномоченных органов сводится не только к целенаправленной работе по выявлению, раскрытию и расследованию подобных преступлений.

По нашему мнению, противодействие IT-кражам включает следующие направления:

1. Деятельность уполномоченных органов (субъектов) по совершенствованию нормативно-правового регулирования в данной сфере;
2. Профилактика совершения IT-преступлений, в том числе повышения общего уровня цифровой грамотности граждан;
3. Выработка, реализация и совершенствование механизмов, а также средств и методов противодействия IT-преступлениям;
4. Предупреждение совершения IT-преступлений (например, разработка и использования программных продуктов, в том числе на основе искусственного интеллекта, позволяющих в автоматическом режиме блокировать «подозрительные» операции по банковским счетам).
5. Подготовка специалистов в области защиты информации, а также специалистов по противодействию киберпреступности.

В заключении отметим, что в условиях интенсивной цифровизации всех сфер жизни общества вопросы защиты собственности, в том числе средств граждан и организации, хранящихся на банковских счетах являются особым приоритетом правоохранительных органов.

Литература

1. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVVS/student/risk_management/Состояние%20преступности%20в%20Росс1.pdf (дата обращения 10.04.2024).
2. Статистическая отчетность формы федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» // ЦСИ ФКУ «ГИАЦ МВД России» (10.5.0.16/csi).
3. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма; Инфра-М, 2018. – 352 с.
4. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. №1 (42). С.133-138.

Сведения об авторе

Дырма Сергей Валерьевич, старший преподаватель кафедры гуманитарных и социально-экономических наук, подполковник полиции Крымский филиал Краснодарского университета МВД России.

**Епифанцева Виктория Александровна,
Иванов Игорь Петрович**

ИСПОЛЬЗОВАНИЕ РОБОТОТЕХНИКИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В современном постиндустриальном обществе, когда уровень развития информационных технологий довольно высокий, большими темпами также развивается и робототехника.

Робототехника – это область науки и техники, которая занимается разработкой и применением роботов и различных робототехнических систем для облегчения трудовой деятельности человека и интенсификации производства.

Президентом Российской Федерации Владимиром Владимировичем Путиным при послании к Федеральному Собранию 29 февраля 2024 года была поставлена очень важная задача: повысить уровень роботизации в России на различных государственных предприятиях, в государственных организациях. Робототехнические комплексы должны осуществлять контроль оперативной обстановки, распознавать лица и автомобилей, также проводить идентификацию, осуществлять сбор и передачу разведывательной информации. Такой робот возможно использовать для улучшения мониторинга и наблюдения, патрулирования улиц, проведения допросов и обысков, участия в спасательных операциях, обезвреживания опасных предметов, поддержания порядка на массовых мероприятиях, что повысит эффективность.

Использовать такой робот возможно для повышения безопасности сотрудников ОВД. Его использование может значительно повысить безопасность самих сотрудников ОВД. Видеозаписи могут служить доказательством в суде, а также помогать в анализе и корректировке тактик и методов работы. Также можно использовать в местах с повышенной опасностью для осмотра местности, например, при обрушении зданий или катастрофах, также если основную управляющую схему обернуть в свинцовую фольгу (оболочку, капсулу, корпус) и обеспечить проводным соединением, то тогда есть

возможность использовать робота в зонах с повышенной радиационной опасностью и себестоимость меньше в отличие от зарубежных. Ещё одно достоинство роботов, это наличие портативной управляемой камеры. Благодаря ей происходит ускорение и упрощение сбора доказательств. В контексте следственных действий портативная управляемая камера может играть ключевую роль в сборе доказательств. Их можно использовать для документирования мест преступлений, аварий, ДТП и других инцидентов с высокой степенью детализации и точности. Это упрощает процесс сбора, анализа и предъявления доказательств, что, в свою очередь, способствует более быстрому и справедливому рассмотрению дел.

Портативные управляемые камеры также могут способствовать улучшению взаимодействия между ОВД и общественностью. Видеоматериалы могут использоваться для информирования граждан о текущей обстановке, мерах безопасности и итогах проведения различных операций. Это повышает прозрачность работы органов внутренних дел и способствует формированию доверия со стороны населения.

Использование портативных управляемых роботов-камер в деятельности органов внутренних дел (ОВД) представляет собой значительный шаг вперёд в области повышения эффективности и безопасности правоохранительной деятельности. Эти устройства обладают уникальной способностью к улучшению процессов мониторинга, наблюдения и сбора информации, что делает их незаменимым инструментом в ряде ситуаций. Портативные роботы-камеры способны оперативно передвигаться в зоны, недоступные или опасные для человека, обеспечивая при этом передачу видеоизображения в реальном времени. Это дает возможность оперативно реагировать на изменяющиеся обстоятельства, проводить разведывательную деятельность и документирование мест преступлений с минимальными рисками для сотрудников ОВД.

Тем не менее необходимо учитывать и потенциальные вызовы, связанные с использованием таких устройств, включая вопросы приватности, защиты

данных и этические аспекты применения робототехники в правоохранительной деятельности. Важно обеспечить, чтобы применение портативных роботов-камер строго соответствовало законодательству и нормам, регулирующим права и свободы граждан.

Интеграция портативных управляемых роботов-камер в практику работы ОВД открывает новые горизонты для повышения эффективности правоохранительных органов и укрепления общественной безопасности. С учетом быстрого развития технологий в области робототехники и искусственного интеллекта, можно ожидать дальнейшего расширения возможностей и улучшения функциональности таких устройств, что будет способствовать их ещё более широкому внедрению в деятельность ОВД в будущем.

Литература

1. Елифанцева В.А. Методы, способы и технологии защиты информации и баз данных в подразделениях МВД России с применением объектно-ориентированного программирования // В.А. Елифанцева // Математические методы и информационно-технические средства. Материалы XVI Всероссийской научно-практической конференции. Краснодар, 2020. С. 37-40.

2. Незнамов А.В., Наумов В.Б. Вопросы развития законодательства о робототехнике в России и в мире // Юридические исследования. 2017. № 8.

3. Постановление президента Российской Федерации Федеральному Собранию от 29.02.2024 «Постановление Президента Федеральному собранию». Электронный ресурс по состоянию на 04.06.2024: https://www.consultant.ru/document/cons_doc_LAW_471111/.

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

Сведения об авторах

Елифанцева Виктория Александровна, преподаватель кафедры информатики и математики Краснодарского университета МВД России.

Иванов Игорь Петрович, доцент кафедры информатики и математики, кандидат педагогических наук Краснодарского университета МВД России.

Еськин Дмитрий Леонтьевич

ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОПРАВНОЙ ДЕЯТЕЛЬНОСТИ

Информационные технологии в современном мире интенсивно развиваются, вызывая его необратимые изменения. Одним из важнейших достижений в области информационных технологий стало бурное развитие технологий искусственного интеллекта. Существует множество определений искусственного интеллекта. Суть большинства из них сводится к тому, что искусственный интеллект представляет собой совокупность технологий, позволяющих машинам имитировать когнитивные функции человека. К таким задачам можно отнести распознавание речи и образов, анализ данных и принятие решений, самообучение и т.д.

Изначально зародившись в середине XX века, технологии искусственного интеллекта сегодня находят широкое применение в самых разнообразных сферах жизни человека, открывая для него новые возможности. В повседневной жизни технологии искусственного интеллекта используются в быту в голосовых помощниках, для управления системами умного дома, в чат-ботах на основе больших языковых моделей, различных онлайн-сервисах, предлагающих тот либо иной контент в соответствии с предпочтениями пользователя. В промышленности технологии искусственного интеллекта позволяют автоматизировать различные рабочие процессы на производстве, например конвейерные операции, на основании анализа данных прогнозировать поломки оборудования и проводить его обслуживание заранее, минимизируя простои. В транспортной отрасли искусственный интеллект используется в автономных транспортных средствах, системах организации дорожного движения, позволяющих оптимизировать дорожное движение на основе анализа транспортных потоков, комплексах контроля безопасности дорожного движения. Медицинские системы на основе искусственного интеллекта способны анализировать медицинские данные пациентов, что позволяет

осуществлять раннюю диагностику различных заболеваний, определять предрасположенность пациента к развитию конкретных патологий, предлагать рекомендации по лечению заболеваний и т.д. В финансовом секторе искусственный интеллект используется для анализа рыночных данных, стратегий и составления прогнозов. В сфере образования персонализированные обучающие системы на основе искусственного интеллекта способны адаптироваться под нужды каждого обучающегося, подбирая подходящий его интересам и уровню подготовки учебный материал и т.д. Все это делает технологии искусственного интеллекта чрезвычайно перспективными. Однако, наряду с огромными преимуществами, искусственный интеллект несет в себе и ряд рисков. Один из этих рисков связан с использованием злоумышленниками искусственного интеллекта для достижения своих противоправных целей и представляет серьезную угрозу для безопасности и стабильности современного общества.

Способность систем искусственного интеллекта имитировать интеллектуальное поведение человека означает возможность для преступников выдавать себя за другую личность, что в юридической литературе стран англосаксонского права обозначается как кража личности [1]. В этих целях злоумышленниками стали прибегать к основанной на искусственном интеллекте технологии дипфейк, позволяющей синтезировать видеоизображение или голос жертвы, используя ее фотографию и образец аудиозаписи голоса. В сгенерированных с помощью данной технологии видео и аудиозаписях очень сложно распознать подделку. Синтезированные таким образом материалы могут быть использованы в различных противоправных целях. Например, созданные поддельные компрометирующие видеоматериалы с участием жертвы могут использоваться для ее дискредитации в целях нанесения ущерба репутации или карьере, либо для ее дальнейшего шантажа и вымогательства под угрозой их обнародования. Технология дипфейк представляет угрозу и для систем безопасности, использующих биометрическую аутентификацию. Например,

злоумышленники могут использовать созданные видеоизображения или аудиозаписи для обхода систем распознавания лиц или голоса в целях получения доступа к системам дистанционного банковского обслуживания или подтверждения операций, которые были заблокированы системой антифрода банка [2].

Следует отметить, что созданный с помощью технологии дипфейк аудиовизуальный контент также существенно расширяет возможности мошенников по воздействию на окружение жертвы с помощью методов социальной инженерии – совокупности методов и приемов психологического давления на человека, позволяющих получить доступ к конфиденциальной информации или защищенным ресурсам. Первый случай использования сгенерированного с помощью дипфейк голоса для мошенничества зафиксирован в начале 2019 года, когда злоумышленники скопировали голос генерального директора энергетической компании и убедили сотрудников организации перевести 243000 долларов поддельному поставщику [3].

В социальной инженерии искусственный интеллект применяется не только для создания поддельного аудиовизуального контента. Так искусственный интеллект позволяет злоумышленникам более эффективно создавать фишинговые письма для осуществления спам-рассылок. Такие письма трудно отличить от легитимных сообщений, их содержание адаптировано под конкретного получателя, не содержат орфографических и пунктуационных ошибок, оформлены в соответствующей конкретной организации цветовой схеме и стиле, что значительно увеличивает вероятность успеха злоумышленника.

Генеративный искусственный интеллект может использоваться злоумышленниками для дезинформации, например путем создания фейковых новостей и их дальнейшего распространения через социальные сети и иные платформы, в целях оказания влияния на общественное мнение, разжигания ненависти и т.д. Фейковые новости могут подкрепляться созданным с помощью

технологии дипфейк визуальным контентом, что увеличивает эффективность их воздействия на целевую аудиторию. Следует отметить, что дезинформация может использоваться и в коммерческой сфере, например, путем создания ложных отзывов о продуктах и услугах в целях нанесения ущерба репутации коммерческих организаций и их финансовому положению. Часто распространение дезинформации активно поддерживается чат-ботами, управляемыми искусственным интеллектом. Такие чат-боты способны генерировать и распространять сообщения, создавая иллюзию массовой поддержки или осуждения чего-либо. Например, в комментариях к новости могут появиться сотни сообщений, сгенерированных чат-ботами, в которых поддерживается определенная точка зрения. В результате у реальных пользователей контента создается впечатление, что такая точка зрения широко распространена.

Технологии искусственного интеллекта могут использоваться злоумышленниками для анализа больших объемов данных с целью дальнейшего планирования и координации преступных действий. Например, анализ данных из социальных сетей или иных источников может помочь выбрать жертву и определить время, когда она будет отсутствовать дома с целью совершения квартирной кражи.

Искусственный интеллект существенно расширил возможности злоумышленников в области автоматизации кибератак. Так основанные на технологиях искусственного интеллекта нейронные сети уже сегодня используются злоумышленниками для разработки вредоносного программного обеспечения. Искусственный интеллект может использоваться для поиска уязвимостей в программном обеспечении с целью их дальнейшей эксплуатации, анализировать большие объемы данных о сетевом трафике, выявляя слабые места в защите и т.д. Кроме того, он может эффективно применяться для координации проведения атак типа «отказ в обслуживании».

Таким образом, возможности технологий искусственного интеллекта сегодня открывают перед человечеством новые горизонты. Они активно используются в различных сферах жизнедеятельности, улучшая качество жизни и повышая эффективность бизнес-процессов. Вместе с тем наряду с многочисленными преимуществами искусственный интеллект несет в себе и серьезные угрозы, особенно когда его возможности попадают в руки злоумышленников. В связи с этим возникает необходимость принятия комплекса мер, позволяющих противодействовать злоупотреблению возможностями искусственного интеллекта. При этом данные меры должны включать в себя как технологические решения, так и правовые и этические нормы, ограничивающие его использование в преступных целях.

Литература

1. Дремлюга Р.И. использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. №3. С. 153-165.

2. Фролова, М. Рост на 700%: мошенники стали чаще использовать дипфейки в сфере финансов // Известия: [сайт]. – 2024. URL: <https://iz.ru/1679621/mariia-frolova/rost-na-700-moshenniki-stali-chashche-ispolzovat-dipfeiki-v-sfere-finansov> (дата обращения: 15.04.2024).

3. Власенко, А.В. Искусственный интеллект и проблемы кибербезопасности. Технология Deepfake / А. В. Власенко, П. С. Киселёв, Е. А. Складорова. – Текст: непосредственный // Молодой ученый. 2021. № 21 (363). С. 81-86.

Сведения об авторе

Еськин Дмитрий Леонтьевич, кандидат физико-математических наук, заместитель начальника кафедры информатики и математики Волгоградской академии Министерства внутренних дел.

Ефремов Сергей Константинович

СОКРАЩЕНИЕ РАЗМЕРНОСТИ ЗАДАЧИ ПРОГНОЗИРОВАНИЯ УСПЕВАЕМОСТИ КУРСАНТОВ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Задача прогнозирования – одна из задач, успешно решаемых с использованием искусственных нейронных сетей (ИНС) [4]. В работе [3] описана попытка решения задачи прогнозирования успеваемости курсантов при их обучении в Краснодарском университете МВД России по специальности 40.03.02 Обеспечение законности и правопорядка. Обучающая выборка составлена из 70 примеров. В примерах использованы:

- в качестве входных параметров – оценки из школьных аттестатов по 14 основным предметам обучения;
- в качестве выходных, прогнозируемых параметров – оценки, полученные курсантами на экзаменах и зачетах в 1 и 2 семестрах обучения в университете.

После обучения ИНС на этих примерах проведено прогнозирование оценок других 41 курсанта, завершивших обучение на 1 курсе. Спрогнозированные оценки сопоставлены с реальными [2]. В результате выявлено, что ошибки прогноза достаточно велики: среднее значение модуля ошибки прогноза составило 0,55 балла.

Определены основные причины невысокой точности прогноза:

- достаточно грубая пятибалльная, а по сути трехбалльная шкала оценок. Данную причину невозможно устранить;
- большая зашумленность исходных данных по причине высокой степени субъективизма при выставлении оценок. Во-первых, субъективизм проявляется случайным образом, естественен при оценке знаний учеников и курсантов учителями и преподавателями на экзаменах. На оценку также влияет физическое и психологическое состояние экзаменуемого в день экзамена, «везение» в вопросах экзаменационного билета и т.д. Эта причина

компенсируется увеличением количества обучающих примеров, за счет чего нивелируются данные случайности. Во-вторых, выявлены обучающие примеры, в которых оценки отдельных учеников и курсантов явно не соответствуют уровню знаний, как правило завышены по причине «особо лояльного» отношения к этим экзаменуемым.

Данная работа посвящена попытке уменьшения влияния шума в данных на точность прогноза путем исключения из рассмотрения при прогнозировании оценок по конкретной дисциплине тех школьных предметов, оценки по которым оказывают малое влияние на оценки по данной дисциплине, сохраняя эффект шума. Степень такого влияния может быть оценена значениями коэффициентов корреляции между оценками по конкретному школьному предмету и по конкретной вузовской дисциплине.

В таблице 1 представлены значения коэффициентов корреляции между оценками по школьным предметам и по вузовским дисциплинам в обучающей выборке. Табличные данные дополнены максимальными и средними значениями коэффициентов корреляции для каждого рассматриваемого школьного предмета (строки) и каждой вузовской дисциплины (столбцы).

Наиболее удачным для рассмотрения является вузовская дисциплина Информатика (ИИТПД), т.к. в столбце дисциплины присутствует наибольшее среди всех значение коэффициента корреляции (0,5), а среднее значение коэффициента корреляции тоже большое в рамках таблицы (0,3). Обучение нейрона, проведено в нескольких вариантах:

- из обучающих примеров исключены школьные предметы История, ОБЖ и Физическая культура (значение коэффициента 0,2);
 - дополнительно исключены предметы со значением коэффициента 0,3;
 - дополнительно исключены предметы со значением коэффициента 0,4,
- т.е. в качестве прогноза вузовской оценки использована только школьная оценка по информатике.

Таблица 1. Значения коэффициентов корреляции

	ИИТД	Философия	Административное право	Русский язык в деловой	Физическая подготовка	Иностранный язык	Профессиональная этика и служебный	Гражданское право	Криминалистика	Максимальное	Среднее
Русский язык	0,4	0,4	0,3	0,4	0,1	0,3	0,2	0,2	0,2	0,4	0,3
Русская литература	0,4	0,3	0,3	0,2	0,1	0,3	0,1	0,2	0,2	0,4	0,2
Иностранный язык	0,3	0,3	0,2	0,2	0,1	0,3	0,2	0,2	0,1	0,3	0,2
Алгебра и начала анализа	0,3	0,3	0,3	0,2	0	0,2	0,1	0,1	0,1	0,3	0,2
Геометрия	0,3	0,3	0,3	0,2	0,1	0,3	0,2	0,2	0,1	0,3	0,2
История	0,2	0,3	0,3	0,2	0,1	0,2	0,1	0,2	0,2	0,3	0,2
География	0,3	0,1	0,2	0,2	0,1	0,2	0,1	0,1	0,1	0,3	0,2
Физика	0,3	0,2	0,3	0,2	0	0,2	0,1	0,2	0,1	0,3	0,2
Химия	0,4	0,3	0,3	0,2	0,1	0,3	0,2	0,2	0,2	0,4	0,2
Биология	0,4	0,3	0,3	0,3	0	0,3	0,3	0,2	0,4	0,4	0,3
ОБЖ	0,2	0,1	0,2	0,2	0,1	0,1	0,2	0,1	0,1	0,2	0,1
Информатика и ИКТ	0,5	0,2	0,2	0,2	0,1	0,1	0,3	0,2	0,1	0,5	0,2
Физическая культура	0,2	0,2	0,1	-0	0,1	0,1	0,2	0,1	-0	0,2	0,1
Обществознание	0,4	0,4	0,3	0,4	0,1	0,3	0,2	0,2	0,2	0,4	0,3
Максимальное	0,5	0,4	0,3	0,4	0,1	0,3	0,3	0,2	0,4		
Среднее	0,3	0,3	0,3	0,2	0,1	0,2	0,2	0,2	0,2		

При каждом варианте проведен расчет прогнозируемой оценки. Во всех описанных случаях значение ошибки прогноза увеличивалось.

Таким образом, для более высокой точности прогноза необходим учет оценок по максимальному количеству школьных предметов, даже если корреляция между оценками по школьному предмету и по вузовской дисциплине невелика.

Продолжением работы по повышению точности прогноза может быть исследование возможности повышения точности за счет исключения из обучающей выборки примеров, относящихся к случаям выставления оценок, явно не соответствующих знаниям экзаменуемого (как правило, завышенных).

Литература

1. Ефремов С.К. Анализ факторов, влияющих на точность прогноза успеваемости курсантов с помощью искусственной нейронной сети // Математические методы и информационно-технические средства: материалы

XIX Международной. науч.-практ. конф. / ред. кол.: И.Н. Старостенко, Е.В. Михайленко, А.В. Еськов, А.А. Хромых, М.В. Шарпан, К.И. Руденко. – Краснодар: Краснодар. ун-т МВД России, 2023.

2. Ефремов С.К. Анализ ошибок прогнозирования успеваемости курсантов с использованием искусственной нейронной сети // Математические методы и информационно-технические средства: материалы XVII Международной. науч.-практ. конф. / ред. кол.: И.Н. Старостенко, Е.В. Михайленко, А.В. Еськов, А.А. Хромых, М.В. Шарпан, К.И. Руденко. – Краснодар: Краснодар. ун-т МВД России, 2021.

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

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. 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).

Сведения об авторе

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

**Жмурко Даниил Юрьевич,
Лаптев Сергей Владимирович**

ЭВОЛЮЦИЯ ИНТЕРНЕТА: ОТ WEB 3.0 К WEB 4.0 – ПЕРСПЕКТИВЫ РАЗВИТИЯ ГЛОБАЛЬНОЙ СЕТИ

Интернет прошел значительный путь с момента своего создания, превратившись из простой сети для обмена информацией в сложную экосистему, охватывающую все аспекты нашей жизни. Рассмотрим ключевые этапы его развития:

- Web 1.0 (1989–2004), или «Статический Веб», представлял собой первую версию интернета с ограниченной интерактивностью и статическими веб-страницами. Пользователи в основном пассивно потребляли информацию.

- Web 2.0 (2004–2016), известный как «Социальный Веб», изменил характер интернета, сделав его более интерактивным. Пользователи стали активными создателями контента, благодаря социальным сетям, блогам и платформам для обмена информацией.

- Web 3.0 (2016–настоящее время), или «Семантический Веб», направлен на создание более интеллектуальной и персонализированной веб-среды с использованием технологий искусственного интеллекта и машинного обучения.

Хотя Web 3.0 все еще развивается, уже ведутся разговоры о будущем Web 4.0, который обещает еще более персонализированный и иммерсивный опыт. Однако точные характеристики и временные рамки для Web 4.0 пока остаются неясными.

Web 3.0 представляет собой значительный сдвиг в взаимодействии с интернетом, предлагая новые возможности для инноваций и сотрудничества. Разработчикам важно понимать эти концепции, чтобы адаптироваться к меняющемуся технологическому ландшафту. Сеть Интернет продолжает стремительно развиваться, и признаки перехода к Web 4.0 уже начинают проявляться, обещая еще большие изменения и инновации.

Создание интернета в привычном нам виде заняло несколько десятилетий, поэтому существует несколько дат, которые считаются его днем рождения. 29 октября 1969 г. впервые удалось передать сообщение от одного удаленного компьютера к другому. 6 августа 1991 г. был опубликован первый в истории веб-сайт. 1989 г. обычно считается официальным годом рождения Всемирной паутины (WWW). История первого поколения интернета, Web 1.0, началась в начале 1990-х гг.

Первый интернет часто характеризуют как «скучный, медленный и анонимный». Он не принадлежал пользователям – основной контент создавали разработчики сайтов, а обычные люди не могли с ним взаимодействовать. По сути, Web 1.0 представлял собой своеобразную электронную библиотеку. Однако этой эпохе мы обязаны появлением электронной почты, хотя она стала доступна пользователям только в этот период.

В 1995 г. появилась первая социальная сеть Classmates, а с 2003 г. начался ее активный рост. Это ознаменовало начало эпохи Web 2.0. Веб-сайты стали более динамичными и ориентированными на пользователя, позволяя создавать и делиться контентом. В целом Web 2.0 значительно улучшил взаимодействие пользователей с интернетом, перейдя от статичных веб-страниц к динамичным, совместно используемым и социально ориентированным платформам. Однако, несмотря на возможность создавать контент, пользователи не могли им владеть, так как он хранился на централизованных корпоративных платформах.

О концепции нового интернета, или Web 3.0, заговорили еще в 2007 г. Web 3.0 должен решить основные проблемы Web 2.0, предоставив авторам контроль над своим контентом, а пользователям – над своими данными. Ключевые технологии этого поколения интернета должны быть построены на обеспечивающем децентрализованность сети и ее независимость.

С активным развитием искусственного интеллекта, в том числе нейросетей, эксперты заговорили о Web 4.0. Это пока только концепция, и единого мнения о том, что будет представлять собой «будущий интернет

будущего», нет. Однако предполагается, что люди будут взаимодействовать с роботами на симбиотическом уровне, управляя ими голосом и визуально. Качество онлайн-связи станет еще лучше, ИИ станет еще «умнее», а пользователь получит еще больший контроль над своей интернет-жизнью. Появиться Web 4.0 может в течение следующих 10-20 лет.

Появление Web 3.0 является результатом эволюции, вызванной растущими потребностями интернет-пользователей. От изначальной простой потребности в получении и распространении информации, требования теперь включают отсутствие цензуры, неизменность данных, уверенность в контрагенте, полную собственность на активы и независимость от централизованных серверов.

Web 3.0 представляет собой инфраструктурную концепцию, реализуемую с помощью определенных технологий. Она включает три слоя: блокчейны, смарт-контракты и децентрализованные приложения (DApps). Первые два слоя служат основой для создания решений на третьем слое, предназначенном для использования обычными пользователями.

Наиболее известной областью Web 3.0 являются криптовалюты. Их количество точно неизвестно, но на различных криптобиржах оно варьируется от девяти до более чем 12 тысяч, а совокупная капитализация составляет \$2,7 трлн. Наибольшей популярностью пользуется Bitcoin, за ним следуют Ethereum и Tether. Криптовалюты выступают финансовой основой Web 3.0 и являются ключевыми инвестиционными инструментами.

Еще одно направление, пережившее всплеск популярности в начале этого десятилетия – это NFT-маркеты, такие как OpenSea, Rarible и Foundation. Эти платформы позволяют пользователям преобразовывать различные объекты цифрового искусства в уникальные токены, которые можно продавать или обменивать за криптовалюту.

В 2023 году направление NFT значительно просело. К примеру, платформа OpenSea прошлой осенью показала снижение более чем на 98% от своих пиковых значений. Тем не менее, технология NFT остается перспективной, так

как предоставляет новые уровни защиты авторских прав в фильмах, музыке и играх, и может быть применена в любых сферах, где нужно подтвердить владение объектами, например, в недвижимости.

Одновременно с NFT-маркетами популярность приобрел Web3-гейминг. Основанный на блокчейне, он обеспечивает истинное владение игровыми предметами и персонажами. В этом контексте часто используется термин play-to-earn, который предполагает получение вознаграждений за улучшение игровых персонажей и сбор предметов. Хотя концепция "играй-и-зарабатывай" не является новой, она привлекла множество новых участников, обещая им вознаграждения в криптовалюте.

Некоторые ключевые технологии, лежащие в основе Web 3.0, включают:

- Онтологии и языки семантической разметки (RDF, OWL).
- Протоколы децентрализованного хранения данных (IPFS, Filecoin).
- Смарт-контракты и децентрализованные приложения (Ethereum, Polkadot).
- Алгоритмы консенсуса блокчейна (Proof-of-Work, Proof-of-Stake).
- Протоколы децентрализованной идентификации (DID, SSI).
- Инструменты разработки Web3 (Web3.js, Ethers.js).

Эти технологии работают совместно, чтобы создать более открытый, безопасный и инновационный интернет, который ставит пользователей в центр внимания и дает им больший контроль над своими данными и цифровой идентичностью.

Подводя итог, можно сказать, что практически все направления Web 3.0, ориентированные на потребителей, так или иначе связаны с криптовалютой. Например, в метавселенных, NFT и DApps криптовалюта используется в качестве основного средства платежа. Другие направления, такие как криптобиржи и криптокошельки, составляют инфраструктурную часть, включающую платформы для хранения, обмена и торговли криптовалютами.

Переход на новый «уровень» сети Интернет только начинается. Согласно статистике, Web 2.0 уже используют 5,4 млрд человек, тогда как численность пользователей Web 3.0, по крайней мере владельцев криптовалюты, составляет около 420 млн.

Существуют несколько факторов, которые могут повлиять на рост и развитие Web 3.0:

1. Технологический прогресс – развитие блокчейна, ИИ и МО ускорит внедрение и расширит сферы применения Web 3.0.
2. Инвестиции – приток венчурного капитала стимулирует инновации и рост экосистемы.
3. Регуляторная среда – благоприятные регуляции и стандарты увеличат доверие пользователей и привлекут участников.
4. Принятие пользователями – повышение осведомленности о преимуществах Web 3.0, таких как конфиденциальность и безопасность, приведет к его более широкому принятию.
5. Инфраструктура – удобные интерфейсы и инструменты разработки ускорят распространение Web 3.0.
6. Сотрудничество – партнерства между компаниями и сообществами создадут инновационные решения и привлекут новых пользователей.
7. Решение реальных проблем – разработка приложений, удовлетворяющих потребности в сферах финансов, здравоохранения и управления идентификацией, стимулирует спрос на Web 3.0.

Летом 2023 года Европейская комиссия представила стратегию по развитию Web 4.0 и виртуальных миров в соответствии с ценностями ЕС. Основные цели включают:

- расширение прав и возможностей людей в цифровом секторе посредством доступа к достоверной информации и создании кадрового резерва специалистов;
- поддержка европейской экосистемы Web 4.0;

- цифровизация государственных услуг и поддержка общественного прогресса;
- формирование глобальных стандартов для новых технологий.

Web 4.0 пока концепция, но активные разработки и исследования уже ведутся. Прогнозируется выход на рынок крупных проектов с решениями на основе генерирующего искусственного интеллекта (GAI) на блокчейне в 2024 г. Такие модели привлекут разработчиков благодаря отсутствию цензуры, доступности и открытым API, что позволит использовать их для расчетов и обучения больших языковых моделей (LLM).

Он также считает, что персональные ИИ-помощники вскоре станут повсеместными, обучаясь у своих владельцев и предлагая пользовательские решения. Данные, сгенерированные такими помощниками, будут являться собственностью пользователей и защищены от доступа третьих лиц.

Шаги в направлении Web 4.0, такие как развитие метавселенных компаниями META, Microsoft, NVIDIA и др., с прогнозируемым доходом от товаров в метавселенных до 615 млрд \$ к 2030 г. Также наблюдается рост внедрения ИИ-ассистентов и чат-ботов на базе LLM, а также рост децентрализованных приложений и протоколов на блокчейне, например в области DeFi и NFT.

Предполагается, что Web 4.0 будет характеризоваться:

- инновациями в пользовательском опыте и функциональной совместимости;
- симбиозом физического и виртуального миров через технологии AR/VR и метавселенные, использование визуальных инструментов общения;
- широким использованием ИИ для анализа данных и персонализации контента;
- децентрализованной архитектурой на базе блокчейна и технологий Web3 для обеспечения безопасности и прозрачности;
- семантическим вебом для машинной обработки и понимания контента;

- повсеместным доступом в интернет;
- новым уровнем развития Интернета вещей, включая технологии мониторинга здоровья.

Что касается сроков, точную дату появления Web 4.0 предсказать сложно, поскольку это постепенный процесс эволюции веб-технологий. Однако, учитывая быстрый прогресс в области ИИ, виртуальной реальности и IoT, можно ожидать, что Web 4.0 станет реальностью в ближайшие 5-10 лет.

Таким образом, Web 3.0 представляет собой новую концепцию развития интернета, которая может существенно изменить то, как мы взаимодействуем с сетью и друг с другом онлайн.

В целом, Web 3.0 (Web 4.0) обещает сделать сеть Интернет более открытым, умным и удобным для пользователей, стимулировать развитие новых видов цифровой экономики. Но для реализации этого потенциала предстоит решить еще много технических и регуляторных вопросов.

Хотя Web 3.0 еще только начинает входить в нашу жизнь, эксперты уже обсуждают следующую стадию – Web 4.0, которая может принести такие инновации как:

- Повсеместное использование ИИ и машинного обучения.
- Интернет вещей и повсеместная связанность устройств.
- Дополненная и виртуальная реальность как неотъемлемая часть интернета.
- Влияние на IT-индустрию.
- Переход к новым версиям веба потребует специалистов с новыми навыками и знаниями:
- Разработчики децентрализованных приложений (dApps).
- Специалисты по анализу и обработке больших данных.
- Эксперты в области ИИ, IoT, AR/VR технологий.

Web 3.0 и Web 4.0 обещают революционные изменения в том, как мы взаимодействуем с интернетом. Этот переход открывает новые возможности, но и ставит новые вызовы перед IT-индустрией и обществом в целом.

Сеть Интернет стремительно развивается, постоянно возникают новые технологии и разработки, которые влияют на развитие человечества. Авторы исследования рассмотрели тенденции развития интернета через призму его развития в прошлые периоды, когда он воспринимался как «возможность», и в условиях новых реалий.

Аналитический отчет «ИНТЕРНЕТ В РОССИИ в 2022-2023 годах: состояние, тенденции и перспективы развития» показывает, как развитие интернет-отрасли влияет на цифровую экономику России. Новые технологии открывают возможности для бизнеса, образования, здравоохранения, полиции и других сфер жизни общества.

Сеть Интернет продолжит стремительно развиваться, предлагая новые возможности и решения для глобальных вызовов. Будущее за персонализированным, интеллектуальным и безопасным интернетом, который будет неотъемлемой частью жизни людей и двигателем цифровой экономики.

Литература

1. Байрон Д.Л., Брубек С. Блоги и бизнес: Путь к успех / Пер. с англ. – СПб.: Символ-Плюс, 2008.
2. Медведев Д.А. Россия, вперед! // Российская газета. – М., 2009. – № 171.
3. Медведев Д.А. Национальные проекты: От стабилизации – к развитию // Медведев Д.А. Национальные приоритеты: Статьи и выступления. – М.: Европа, 2008.
4. Прончев Г.Б., Муравьев В.И. Эволюция web-технологий интернета в контексте перехода России к инновационному развитию // Социальные сети и виртуальные сетевые сообщества, 2013
5. Рыжов С.В., Рыжов В.А. Эволюция социального пространства как Web-4.0 и 5.0. – Стратегия инновационного развития России как особой цивилизации

в XXI веке: VI Всеросс. науч. конф. Сорокинские чтения – 2010: Сб. тезисов – М.: МАКС Пресс, 2010.

6. Соколова Н.Л. Популярная культура Web 2.0: К картографии современного медиаландшафта. – Самара: Самарский университет, 2009.

7. Чумиков А., Бочаров М., Тишкова М. PR в Интернете: Web 1.0, Web 2.0, Web 3.0. – М.: Альпина Паблишерз, 2010.

8. Ших К. Эра Facebook: Как использовать возможности социальных сетей для развития вашего бизнес / Пер. с англ. – М.: Манн, Иванов и Фербер, 2010.

9. O'Reilly Т. What is Web 2.0 – Режим доступа: <http://oreilly.com/web2/archive/what-is-web-20.html?page=2>

Сведения об авторах

Жмурко Даниил Юрьевич, кандидат экономических наук, доцент, старший преподаватель кафедры информатики и математики Краснодарского университета МВД России.

Лаптев Сергей Владимирович, доцент кафедры компьютерных технологий и систем, кандидат физико-математических наук, доцент Кубанского государственного аграрного университета им. И.Т. Трубилина.

**Иночкина Екатерина Викторовна,
Тютюник Николай Павлович**

ДИФФУЗИОННАЯ НЕЙРОННАЯ СЕТЬ ГЕНЕРАЦИИ НЕОДНОРОДНЫХ ОБЛАКОВ ТОЧЕК

Диффузионные нейронные сети являются одним из самых популярных инструментов машинного обучения, которые широко используются для решения задач генерации данных. Предварительное обучение модели и последующая ее точная настройка продемонстрировали значительный успех в области 2D-изображений и обработка естественного языка. В этой работе продемонстрирован подход к созданию модели и предобучению модели для генерации неоднородного облака точек.

Диффузионные вероятностные модели – это класс генеративных моделей, идея которых взята из неравновесной термодинамики (non-equilibrium thermodynamics). В основе диффузии облака точек лежит цепь Маркова (последовательность случайных событий с конечным или счётным числом исходов, где вероятность наступления каждого события зависит только от состояния, достигнутого в предыдущем событии), которая медленно добавляет шум к исходным данным, а затем обращает процесс диффузии вспять, чтобы получить исходные данные [1].

Целью работы является построить диффузионную нейронную сеть для генерации вероятностного распределения данных, которые мы используем в задаче. Есть два основных этапа: forward process (зашумливание – а именно, потеря своей начальной формы), reverse process (генерация – возвращение к первоначальной форме).

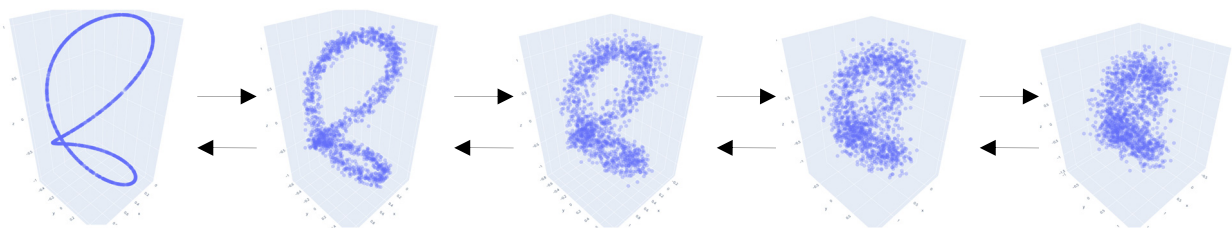


Рис. 1. Схематичное описание forward process, reverse process

Во время forward process случайный шум непрерывно вводится в облако точек через цепь Маркова. И существует взаимосвязь отображения точка-точка между зашумленными облаками точек соседних временных меток [2].

$$q(x_{t:1}|x_0) = \prod_{t=1} q(x_{t-1} \vee x_t)$$

Формально, учитывая чистое облако точек x_0 , содержащее n точек из реального распределения данных, процесс диффузии постепенно добавляет гауссовский шум к x_0 за T временных шагов

$$q(x_t|x_{t-1}) = N(x_t; \sqrt{1 - \beta_t}x_{t-1}, \beta_t I) \quad (1)$$

где гиперпараметры β_t представляют собой некоторые заранее определенные малые константы и постепенно увеличиваются с течением времени. x_t берется из Гауссовского распределения со средним значением $\sqrt{1 - \beta_t}x_{t-1}$ и переменной β_t . То есть, он лежит в пределах от 0 до 1, при этом каждый последующий β_t должен быть больше предыдущего.

Оптимальное значение β_t стремится к нулю, так как исходя из Гауссовского распределения, чем выше β_t , тем больше шума и больше прыжок, который совершит точка. Поэтому сложнее предугадать её изначальное положение.

$$\lim_{t \rightarrow \infty} N(x_t; \sqrt{1 - \beta_t}x_{t-1}, \beta_t I)$$

Количество шагов не должно доходить до бесконечности, так как при t , стремящемся к бесконечности, мы в скором времени получим облака, состоящие только из шума без возможности обратного восстановления. Установлено, что оптимальное значение находится между 500 и 1000 в зависимости от размера исходной выборки и количества различных объектов в ней.

Обратный процесс или reverse process будет иметь ту же функциональную форму, что и зашумливающий процесс, поэтому используем параметризованный вид:

$$p_0(x_{t-1}|x_t) = N(x_{t-1}; \mu_0(x_t, t), \Sigma(x_t, t))$$

В нейронную сеть подается t текущий временной интервал и текущий x_t (текущее зашумленное облако точек). Это нужно для того, чтобы нейронная сеть связала график дисперсии с разными временными интервалами.

$$p_0(x_{0:T}) := p(x_T) \prod_{t=1}^T p_0(x_{t-1} \vee x_t)$$

$$p(x_T) = N(x_T; 0, 1) \quad (2)$$

Параметр (2) $p(x_T)$ является важной частью уравнения, он создаёт sampling steps, то есть выборку от X_t до x_0 . Создавая новое облако точек, мы начинаем с Гауссовского шума, уменьшая параметр t до тех пор, пока не будет получен x_0 .

Для определения этих функций используются многослойные персептроны (полносвязанная нейронная сеть). Так же может быть применим широкий спектр методов регрессии или подбора функций, включая непараметрические методы.

В упрощённом виде данная модель работает следующим образом: forward process выталкивает точки из нужного нам распределения, а reverse process пытается их вернуть обратно.

Для того чтобы вернуть точку обратно, нам нужно получить её траекторию. Но проблема в том, что траекторий может быть бесконечно много, поэтому ограничим их количество. Получим следующее уравнение:

$$p_0(x_{0:T}) = \int p_0(x_{0:T}) dx_{1:T} \quad (3)$$

Прямое вычисление и максимизация вероятности $p(x)$ затруднены, поскольку это требует интегрирования всех скрытых переменных x в уравнении. Поэтому представим как набор параметров.

$X_0, X_1, X_2, \dots, X_t$ будут скрытыми переменными, а X_0 – открытая наблюдаемая константа. Эта идея и лежит в основе нейронной сети.

Рассмотрим архитектуру нейронной сети. На вход Q подаём X_t шум. Далее он попадает в блок *Down*, состоящий из двух слоёв понижающих нейронов. Каждый слой должен уменьшаться на четное число нейронов.

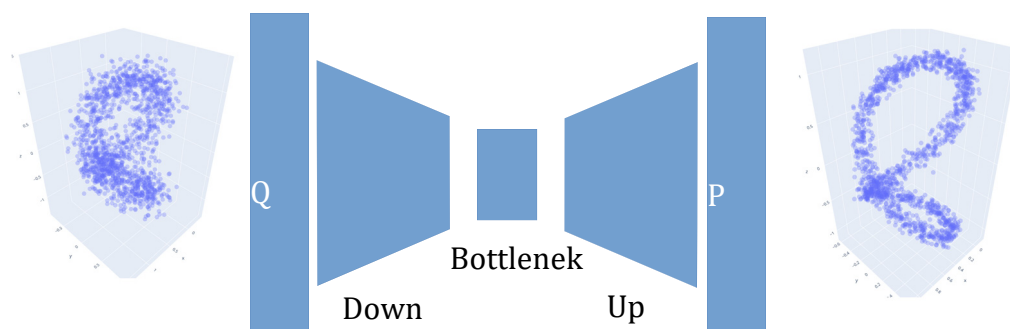


Рис. 2. Схематичное описание модели

После идёт слой сжатия *Bottleneck*, состоящий из самого малого числа нейронов. Он отвечает за запоминание образов, не привязываясь ко всем точкам. Далее идёт слой повышения *Up*, он состоит из двух слоёв нейронов. Каждый слой должен увеличиваться на четное число нейронов. На выходе *P* получим новое облако точек, которое ближе к требуемому. Эта архитектура похожа на VAE или Вариационный Автоэнкодер, но отличается отсутствием вероятностных нейронов [4].

Предложенная архитектура показала удовлетворительный результат генераций и схожесть с исходными данными. Опираясь на вышеописанный математический метод, можно применить другие любые архитектуры.

Обучение нейронной сети происходит следующим образом. В процессе функционирования нейронная сеть формирует выходной сигнал, далее он попадает в ELBO (полезная нижняя граница логарифмической вероятности некоторых наблюдаемых данных). Эта функция помогает нам приближенно оптимизировать параметры ϕ так, чтобы получить наилучшую аппроксимацию (приближение) для истинного распределения латентных переменных $p(z|x)$. ELBO можно записать следующим образом:

$$ELBO(\phi) = E[(\log p(x \vee z))] - KL[(q(z \vee \phi) \parallel p(z))]$$

где $E[\log p(x|z)]$ – математическое ожидание логарифма правдоподобия наблюдаемых данных x при условии латентных переменных z , и $KL(q(z|\phi) \parallel p(z))$ – расстояние Кульбака-Лейблера между приближенным распределением $q(z|\phi)$ и истинным апостериорным распределением $p(z|x)$.

Минимизируя расстояние Кульбака-Лейблера, то есть приближая распределения к истинному, максимизируем ELBO.

$$L_t = E_{x_0, \epsilon} \left[\frac{1}{2 \|\Sigma(x_t, t)\|_2^2} \|\mu_t(x_t, x_0) - \mu_0(x_t, t)\|^2 \right] \quad (4)$$

Подставив формулы (1) и (3) в формулу (4), после преобразований получим

$$L_t = E \left[\left\| \epsilon_t - \epsilon_0 \left(\sqrt{a_t} x_0 + \sqrt{1 - a_t} \epsilon_t \right) \right\|^2 \right]$$

В итоге loss (ошибка) будет равняться Xt-Pt или Шум-Шум полученный после генерации. Это и есть метод оптимизации.

Опираясь на вышеописанные математические подходы, была разработана программа для генерации неоднородных облаков точек. Она включает в себя интерпретацию нейронной сети на языке Python. Результаты были получены с помощью этой программы на примере модели стола, спирали и дерева (Рис. 3).

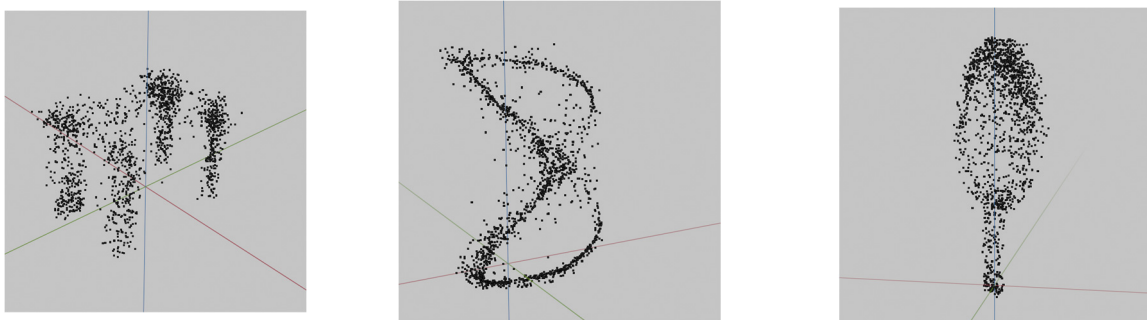


Рис. 3. Облака точек, обозначающие стол, спираль, дерево

В результате исследования была разработана и обучена модель диффузионной нейронной сети для генерации неоднородных облаков точек. В ходе экспериментов было показано, что модель может генерировать облака точек с приемлемой точностью.

Литература

1. Sohl-Dickstein et al., 2015: Deep Unsupervised Learning using Nonequilibrium Thermodynamics [Электронный ресурс] – URL <https://arxiv.org/abs/1503.03585>,
2. Song et al., 2021: Denoising Diffusion Implicit Models [Электронный ресурс] – URL: <https://arxiv.org/abs/2010.02502>

3. Calvin Luo, 2021: Understanding Diffusion Models: A Unified Perspective [Электронный ресурс] – URL: <https://arxiv.org/abs/2208.11970>
4. Kingma et al., 2021: Variational Diffusion Models [Электронный ресурс] – URL: <https://arxiv.org/abs/2107.0063>

Сведения об авторах

Иночкина Екатерина Викторовна, кандидат технических наук, доцент кафедры высшей математики Кубанского государственного технологического университета.

Тютюник Николай Павлович, студент Кубанского государственного технологического университета.

**Камышов Юрий Николаевич,
Печатнова Елена Владимировна,
Егорова Надежда Сергеевна**

СРАВНЕНИЕ РЕЗУЛЬТАТОВ ОПРОСА НАСЕЛЕНИЯ НА РАЗЛИЧНЫХ ЭЛЕКТРОННЫХ РЕСУРСАХ ПО ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

На протяжении длительного периода времени в отношении показателей аварийности наблюдался спад, который замедлился в последние годы и в 2023 году полностью прекратился – значения основных показателей аварийности выросли. Рост отмечился впервые за последние 10 лет [1]. Данная ситуация свидетельствует о том, что необходимы более усиленные меры по снижению аварийности, а также использование новых подходов к выбору этих мер.

Одним из вариантов разработки и определения необходимого комплекса мероприятий, а также оценки их эффективности являются социологические опросы населения [2]. С одной стороны, это связано с тем, что поведение участников дорожного движения во многом определяет уровень аварийности. Определение паттернов поведения, причин и вектора изменения культуры вождения может быть определено на основе социологических опросов. С другой стороны, проведение опроса влияет на мнение населения, акцентирует внимание респондентов на проблеме аварийности, что в свою очередь может положительно повлиять на повышение уровня ответственности в соблюдении ПДД и улучшении культуры вождения. Для получения объективных результатов требуется всесторонний охват респондентов.

Одним из наиболее используемых методов проведения социологического опроса является проведение его с использованием электронных площадок, в том числе социальных сетей.

Цель работы: проанализировать результаты опросов населения по вопросу обеспечения безопасности дорожного движения на различных электронных платформах.

Среди основных платформ выбраны: телеграм, социальная сеть вконтакте, официальный сайт национального проекта «Безопасные и качественные дороги». Выбирались вопросы, близкие к следующему: «Какие меры обеспечения безопасности дорожного движения Вы считаете наиболее эффективными?».

В первую очередь проанализированы опросы, связанные с выбранной тематикой на официальном сайте национального проекта «Безопасные и качественные дороги» [3]. Найдены подходящие опросы, которые были проведены в 2020 и 2022 году. В 2020 году проведен опрос на тему «Снижение аварийности – одна из ключевых целей нацпроекта. Дорожникам предстоит ещё много работы. А какие меры вы считаете самыми эффективными?» (рис. 1).



Рис. 1. Результаты опроса на сайте БКД, 2020

Определено, что более четверти респондентов считают, что основным фактором безопасности является обустройство освещения.

В 2022 году проводился опрос на тему «Как нужно повышать безопасность движения?» (рис. 2).

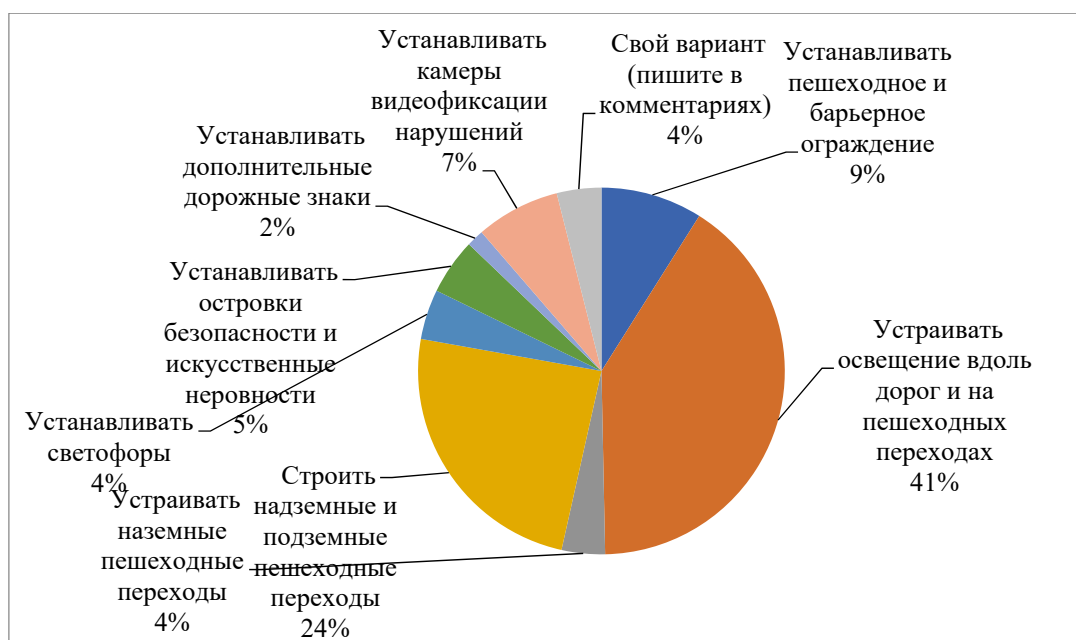


Рис. 2. Результаты опроса на сайте БКД, 2022

В 2022 году доля респондентов, разделяющих мнение о том, что освещение – основная мера предупреждения аварийности увеличилась.

Схожий опрос проведен в ноябре 2023 в телеграме [4] – респонденты отвечали на вопрос «Какие меры, на ваш взгляд, позволили бы ликвидировать очаги аварийности?» (рис. 3). Его отличительной чертой являлась возможность выбора нескольких вариантов ответа.

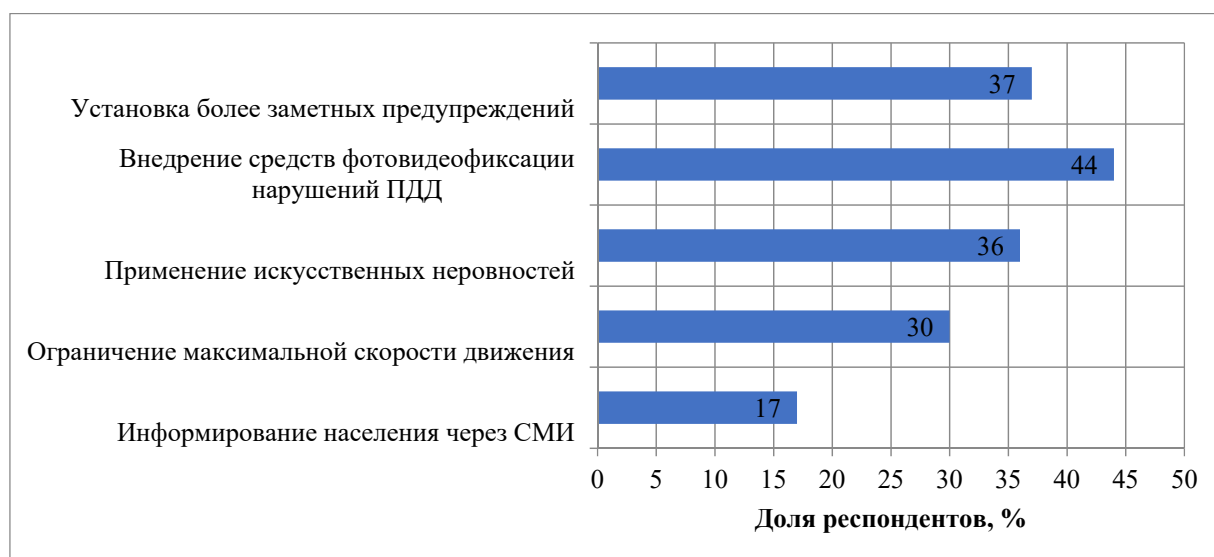


Рис. 3. Результаты опроса в телеграме

На платформе телеграм большая часть респондентов выбрали внедрение фотовидеофиксации нарушений ПДД.

Аналогичный опрос проводился в социальной сети Вконтакте (официальная страница национального проекта «Безопасные и качественные дороги» [5], рис. 4). Опрос также предполагал несколько вариантов ответов.



Рис. 4. Результаты опроса в социальной сети Вконтакте

Более половины респондентов (70%) также выбрали освещение как одну из мер обеспечения безопасности. Около трети отметили островки безопасности и искусственные неровности (40%) и надземные и подземные пешеходные переходы (38%).

Анализируя результаты можно сделать следующие выводы. На всех электронных ресурсах наиболее распространенным вариантом улучшения безопасности дорожного движения является обустройство освещения (при наличии такого варианта ответа). Однако процентное соотношение среди респондентов отличается на различных ресурсах и изменяется по истечению определенного времени. Также распространенным ответом является обустройство участков УДС островками безопасности и искусственными неровностями. Предупреждение ДТП за счет внедрения систем фото-видеофиксации нарушений ПДД также представляет собой распространенный ответ, однако наиболее выражен он среди пользователей телеграма.

С помощью проведения социальных опросов определяются основные запросы общества в области повышения безопасности дорожного движения.

Однако для получения объективных результатов необходимо проводить опрос на различных электронных площадках, включая социальные сети и мессенджеры, поскольку они в настоящее время являются одними из наиболее посещаемых электронных ресурсов.

Литература

1. Дорожно-транспортная аварийность в Российской Федерации в 2023 году. Информационно-аналитический обзор. М.: ФКУ «НЦ БДД МВД России», 2024, 154 с.

2. Печатнова, Е.В. Особенности аварийности в пригородной зоне / Е.В. Печатнова, Е. О. Усольцева // Автомобильные дороги и транспортная инфраструктура. – 2023. – № 4(4). – С. 122-129.

3. Безопасные и качественные дороги [Электронный ресурс]. URL:<https://bkdrf.ru/Reception/SurveyList?ysclid=lwfwvjgqcv77717406>.

4. «Какие меры, на ваш взгляд, позволили бы ликвидировать очаги аварийности?» / страница // страница телеграм. 12 ноября 2023. URL: <https://web.telegram.org/a/#-1001783096004> (дата обращения: 10.03.2024).

5. Официальная страница национального проекта «Безопасные и качественные дороги» // страница группы рос. соц. сети ВКонтакте 14 декабря 2020. URL: https://vk.com/bkdnational?w=wall-147894890_8469 (дата обращения: 13.04.2024).

Сведения об авторах

Камышов Юрий Николаевич, кандидат технических наук, доцент кафедры информатики и специальной техники Белгородского юридического института МВД России.

Печатнова Елена Владимировна, кандидат технических наук, доцент кафедры «Организация и безопасность дорожного движения» Алтайского государственного технического университета им. И.И. Ползунова.

Егорова Надежда Сергеевна, студент Алтайского государственного технического университета им. И.И. Ползунова.

Карпика Анатолий Григорьевич

АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ

Развитие алгоритмов машинной обработки и распознавания изображений, звуков, естественной речи, а также алгоритмов обучения нейронных сетей распознаванию не только синтаксической, но и семантической информации (т.е. появление у нейронных сетей способности обращать «внимание» на вес отдельных элементов, например, степени важности и эмоциональной нагруженности слов в длинном нарративе открыло дорогу для появления нового направления в цифровой трансформации общества, а именно интернета поведения. Интернет поведения (ИП) представляет собой технологии машинного распознавания паттернов человеческого поведения, проявляющегося через жесты, речь и выражение лица, отражающее эмоции и настроение человека. Термин «интернет поведения» стал результатом синтеза различных задач анализа человеческого поведения. Сам термин появился в 2012 г. в блоге финского профессора психологии в форме «интернет поведений» в качестве «аналога интернета вещей» и выражал возможность сбора больших данных о паттернах человеческого поведения для целей развития психологического знания [1]. Предложенный термин достаточно быстро был интегрирован в начавшиеся в 2000-х годах исследования поведения людей в интернете. Стремительное развитие в 2010-х годах интернета вещей как технологии подключения к интернету материальных предметов и их взаимодействия между собой и человеком в рамках интегрированных платформ – умных жилищ, автомобилей, фабрик, клиник и городов придало новое звучание ИП. Условием взаимодействия предметов с человеком является возможность воспринимать и оценивать его явные голосовые или жестовые команды, а также скрытые сигналы, выраженные в биометрических показателях, эмоциях и настроении.

Технологические модели и подходы к оценке поведения используются в различных областях человеческой деятельности. В рамках решения различных прикладных задач в мире были разработаны модели и правила с использованием

новых технологий принятия решений, которые учитывают факторы, способные повлиять на процессы принятия, например, теория аргументированного действия, теория запланированного поведения, теория межличностного поведения, мотивационная модель и другие.

Рассмотрим некоторые подходы, применяющиеся в рамках указанных теорий и моделей.

Модель аргументированного действия (МАД) была разработана в 1975 году Фишбейном и Аздженом для социологических и психологических исследований. Несмотря на это, недавно она стала основой для изучения поведения людей, использующих информационные технологии. В этой модели любое человеческое поведение прогнозируется и объясняется тремя основными когнитивными компонентами, включая склонность к определенному поведению, социальные нормы (социальное влияние) и намерения (решение индивидуума совершать, или не совершать определенные поступки). Для применения МАД человеческое поведение должно быть волевым, систематическим и рациональным. Более того, три фактора границ: волевой контроль; стремление к стабильности с течением времени; измерение намерения с точки зрения цели, времени, контекста, действия и специфичности, определены для параметров и оценки МАД.

Кроме того, для улучшения надежности оценок связей между соответствующим намерением и отношением использовались такие параметры, как общность, цель, действие, контекст и временной горизонт. При этом следует учитывать тот факт, что основными недостатками МАД являются отсутствие учета роли привычки, когнитивного обсуждения, ошибок при опросе респондентов (их отношение к определенному явлению, субъективные нормы, их намерения и разделяемые ими моральные факторы) [2].

Модель запланированного поведения (МЗП). Расширяет МАД путем использования новой переменной, учитывающей поведенческий контроль. По сути, возможность ее использования определяется доступностью ресурсов, возможностей и навыков, а также значимостью этих ресурсов, возможностей и

навыков. Несмотря на то, что обе модели основаны на учете поведения и намерений человека, МЗП использует параметры для оценки действий индивидуума, который не находится под волевым управлением. Поэтому в модели запланированного поведения учитываются три основных фактора, влияющих на поведение индивидуума: воспринимаемый поведенческий контроль, субъективная норма и поведенческое отношение.

Вместе этим, существуют две основные проблемы с моделью МЗП:

1. Оценка отношения к информационным технологиям не будет в значительной степени адекватна, если компьютерная система недоступна.
2. Пересмотренная модель может рассматриваться как более подходящая теоретическая структура, которая влияет на степень добровольности индивидуума, которая выбирает или не выбирает использование информационных технологий на рабочем месте.

Модель межличностного поведения (ММП). Учитывает социальные и эмоциональные факторы. Следовательно, эта модель не только содержит все аспекты МАД и МЗП, но и учитывает привычки, изменение условий и наличие воздействий в интересах улучшения прогнозирования.

У ММП имеется три уровня оценки поведения. На первом уровне – личные убеждения, отношение и социальные факторы, связанные с поведением, формируются личными характеристиками и предыдущим опытом. На втором уровне описывается, как влияние, познание и социальные детерминанты плюс личные убеждения влияют на намерения конкретного поведения.

На третьем уровне возможность выполнения конкретного поведения предсказывается поведенческими намерениями, ситуационными условиями и прошлым опытом. Основным недостатком ММП является сложность по сравнению с МАД и МЗП. Кроме того, рассматриваемая модель не содержит простой процедуры оперативного определения переменных модели, поэтому решение этой задачи перекладывается на исследователя.

Мотивационная модель (ММ). Ее использование определяется двумя факторами: внутренней и внешней мотивацией. Внешняя мотивация

определяется как инструмент, способствующий достижению нужных результатов, которые отличаются от самой деятельности, например, повышение производительности труда. Внутренняя мотивация определяется как восприятие того, что пользователи захотят выполнить деятельность без видимого стимулирования, кроме процесса выполнения деятельности как таковой.

Таким образом, попытки применить различные теории и модели оценки к поведению пользователей компьютерных технологий с одной стороны вдохновляют различных исследователей и это понятно, поскольку в условиях развивающегося информационного общества большинство сфер человеческой деятельности напрямую, либо опосредовано связано с различными информационными технологиями. Одним из факторов, который может возникнуть при внедрении моделей, является «автоматическая предвзятость», т.е. чрезмерное доверие к модели при игнорировании правильной и релевантной информации. Это может привести к принятию неверных решений. С другой стороны, прямое применение готовых моделей связано с известными сложностями построения моделей в условиях неопределенности.

Литература

1. Шаткин М.А., Орлов М.О. Интернет поведения: виды, модели, принципы // Вестник Санкт-Петербургского университета. Философия и конфликтология. 2023. Т.39. Вып. 2. С. 368–380. <https://doi.org/10.21638/spbu17.2023.212>.

2. Карпика А.Г. Анализ направлений применения искусственного интеллекта в правоохранительной деятельности // Юрист-Правовед. 2023. №1. С. 130–135.

Сведения об авторе

Карпика Анатолий Григорьевич, кандидат технических наук, доцент кафедры информационного обеспечения ОВД Ростовского юридического института МВД России.

Кенжалиева Светлана Заировна
Алексеев Антон Дмитриевич
Белов Аркадий Викторович

НАПРАВЛЕНИЯ КРИПТОАНАЛИЗА И ИХ МАТЕМАТИЧЕСКАЯ ОСНОВА

Обеспечение защищенности информации является одной из важнейших задач криптографии. Для этой используются различные алгоритмы шифрования, которые в свою очередь подвергаются атаке, предпринимаются попытки взлома. Совершенствованием стойкости шифров, изучением способов атак и методов защиты от них занимается наука криптоанализ. Атака – попытка криптоанализа, а успешная атака – взлом.

Основная проблема достижения стойкости заключается в неопределенности самих критериев стойкости и в недоказанности существования шифра, которого невозможно взломать как в теории, так и на практике.

Учитывая эту неопределенность, основным методом по оценке стойкости шифра является разработка атак на него с целью выявления уязвимостей. Шифр считается стойким, пока против него неизвестно ни одной атаки, работающей эффективнее метода полного перебора ключей. Следующим этапом после проверки на атаки криптограмма подвергается доработке с учетом результатов атаки, либо полностью переделывается. Основным показателем эффективности атаки является ее сложность, которая оценивается по следующим критериям:

- количество пробных расшифрований/зашифрований;
- объем памяти компьютера, требуемый для реализации атаки;
- количество требуемых открытых/шифрованных текстов (блоков, сообщений);
- вероятность успеха атаки;
- сценарий, в котором реализуется атака.

Существующие направления криптоанализа: статистический,

алгебраический, дифференциальный, линейный, – ориентированы на разработку атак. Произведём краткий обзор направлений криптоанализа, рассмотрим достоинства и недостатки каждого из них.

Статистический криптоанализ исследует возможности взлома криптосистем на основе изучения криптографических закономерностей исходных и зашифрованных сообщений.

В идеале шифр должен преобразовывать информацию так, чтобы она была неотличима от случайной последовательности, в которой частота появления каждой буквы алфавита была одинаковой. Следовательно, одним из важных требований является неотличимость зашифрованных данных от случайной последовательности символов. Если удастся отличить зашифрованный текст от равномерно распределенной последовательности символов, то это указывает на недостатки в стойкости шифра.

Чтобы обнаружить эти недостатки применяется несколько методов:

1. Частотный анализ. Основывается на том, что вероятность появления каждой буквы в сообщении различна, так первенство по частоте появления в русском языке занимает буква «о», среди согласных – «н». Проводя анализ длинного зашифрованного сообщения методом замены текста, производится сравнение частоты появления тех или иных шифробозначений и, сопоставив их с известными частотами букв алфавита восстанавливается исходный текст. Кроме того, порядок букв в словах и фразах естественного языка подчиняется определенным статистическим закономерностям. Частотный анализ также учитывает частоту появления различных буквосочетаний: например, пара стоящих рядом букв «ся» в русском языке более вероятна, чем «цы», а «оь» не встречается никогда. Для большинства естественных языков такая статистика документирована. Однако, этот метод не подходит для шифров перестановки, в которых число символов текста остается постоянным, они просто меняются местами, поэтому все методы, основанные на нахождении частот появлений символов не способны вернуть текст в исходное состояние.

2. Статистический тест «Стопка книг». Тест предназначен для проверки гипотезы о том, что элементы выборки $Z=(z_1, z_2, \dots, z_n)$ из алфавита $A=\{a_1, a_2, \dots, a_s\}$ имеют равномерное распределение и $P(z_n=a_i)=1/S$, где $n=1, \dots, N$; $i=1, \dots, S$.

Перед тестированием выборки в алфавите A фиксируется произвольный порядок. Порядок меняется после анализа каждого выборочного элемента z_n следующим образом:

- буква z_n получает номер 1;
- номера тех букв, которые меньше номера этой буквы, увеличиваются на 1;
- у остальных букв номера не меняются.

Формально эту процедуру можно описать так:

пусть $\omega_n(a)$ – номер буквы $a \in A$ после анализа элементов $z_1, z_2, \dots, z_{n-1}$, тогда:

$$\omega_{n+1}(a) = \begin{cases} 1, & \text{если } z_n = a \\ \omega_n(a) + 1, & \text{если } \omega_n(a) < \omega_n(z_n) \\ \omega_n(a), & \text{если } \omega_n(a) > \omega_n(z_n) \end{cases}$$

Такая конструкция похожа на стопку книг, если считать, что номер книги совпадает с ее положением в стопке. Книга извлекается из стопки и после чтения кладется наверх, ее номер становится первым. Книги, которые первоначально были над ней, сдвигаются вниз, а остальные остаются на месте. Множество всех номеров $\{1, \dots, S\}$ разбивается на две непересекающиеся части – $A_1=\{1, 2, \dots, K\}$ и $A_2=\{K+1, \dots, S\}$, где $K \in \{1, \dots, S\}$ – параметр. Затем по выборке $(z_1, z_2, \dots, z_n)$ подсчитывается v_n – количество номеров $\omega_n(z_n)$, принадлежащих подмножеству A_1 , т.е. количество попаданий букв в «верхнюю часть» «стопки книг». $(n-v_n)$ – это количество попаданий в «нижнюю часть». Далее вычисляется статистика:

$$x^2 = \frac{(v_n - nP_1)^2}{nP_1} + \frac{(n - v_n) - n(1 - P_1)^2}{n(1 - P_1)}, \text{ где } P_1 = \frac{A_1}{S}.$$

Если x^2 меньше критического уровня $X^2_{1,1-\alpha}$, то гипотеза о равномерности распределения элементов выборки принимается, иначе – отвергается. Величина $X^2_{1,1-\alpha}$ – квантиль распределения хи-квадрат уровня значимости $(1-\alpha)$ с одной степенью свободы. Если шифртекст не подчиняется равномерному

распределению, то будем говорить, что имеют место «отклонения от случайности», и чем больше x^2 , тем отклонения от случайности «больше». Алгоритм реализации теста «Стопка книг» на основе хеш-таблицы позволяет реализовать тест с помощью порядка 4 Кбайт памяти и трудоемкостью $O(N)$.

Алгебраический криптоанализ основан на решении систем уравнений над конечным полем. На практике часто применяется совместно с булевыми функциями, которые служат в качестве источников преобразований.

Метод линейного разложения применяется как к дискретным, так и к бесконечным объектам. Особенность данного метода заключается в том, что он находит ключ или передаваемое сообщение без нахождения секретных параметров, которые были применены для зашифрования.

Метод работает в тех случаях, когда платформа шифрования G является частью линейного пространства V , например, группой матриц над некоторым полем F , рассматриваемой в качестве подмножества линейного пространства $M(n, F)$ матриц размера $n \times n$.

Базовыми элементами метода являются:

- построение основы линейного подпространства, порождённого подмножеством из G определенного вида в пространстве V ;
- использование свойств этого подпространства для определения секрета.

Линейный span-метод как и в методе линейного разложения предполагает построение базисов некоторых линейных подпространств, определяемых матричной группой G над конечным полем F_q порядка q .

Рассмотрим использование метода на примере алгоритма типичной задачи. Необходимо решить проблему поиска сопрягающего элемента X для данных матриц A и $B = XAX^{-1}$ из группы $GL(n, F_q)$.

1. Производится замена матричного уравнения $XA=BX$ на систему линейных однородных уравнений.

2. Строится базис $E=\{e_1, ..., e_s\}$ пространства решений и записывается

общее решение $X = \sum_{i=1}^s a_i e_i$.

3. Варьируя коэффициенты $a_i, i=1, \dots, s$, среди всех решений производится поиск невырожденной матрицы X .

Существование обозначенной матрицы гарантируется леммой обратимости.

Лемма (лемма обратимости). Пусть элементы $e_1, \dots, e_s$ кольца матриц $M(n, F_q)$ таковы, что некоторая их линейная комбинация $\sum_{i=1}^s a_i e_i$ с коэффициентами из F_q является обратимой матрицей. Если коэффициенты выбираются в соответствии с равномерным распределением на F_q , то вероятность получения невырожденного решения будет не меньше, чем $p=1-n/q$.

Метод эффективен, если n существенно мало по отношению к q .

Метод нелинейного разложения работает в случаях, когда платформу шифрования G либо невозможно представить в виде матриц, либо эти матрицы не удобны в использовании в виду слишком большой размерности. Далее необходимо соблюдение ряда условий, которые, как правило, выполняются в конечно порождённых нильпотентных и полициклических группах, часто предлагаемых для такого применения в последние годы. Метод нелинейного разложения эффективно решает проблемы, аналогичные проблеме Диффи – Хеллмана.

Проблема Диффи-Хеллмана (формализация проблемы дискретного логарифмирования): пусть известны $p, \alpha, \delta, \gamma$, где p – простое число, α – порождающий элемент группы U_p , $\delta, \gamma \in U_p$. Требуется найти: $\delta^{\log_{\alpha} \gamma} \bmod p$.

Сложность проблемы Диффи – Хеллмана основывается на невозможности решения за полиномиальное время задачи дискретного логарифмирования. Шифрсистему принято считать условно стойкой, если её дешифрование вычислительно эквивалентно решению данной проблемы.

Дифференциальный криптоанализ заключается в атаке с подобранным открытым текстом. Применение дифференциального криптоанализа предполагает возможность зашифрования любых текстов в любом количестве с

целью получения некоторой информации о ключе.

Вкратце алгоритм работы дифференциального криптоанализа выглядит следующим образом:

1. Заранее подбираются два шифртекстов P_1 и P_2 .
2. Вычисляется «дифференциал» $\Delta P = P_1 \oplus P_2$.
3. С помощью ΔP пытаются определить каким должен быть «дифференциал» шифртекстов $\Delta C = C_1 \oplus C_2$.

Вероятность угадать со 100% точностью значение ΔC очень мала. Но возможно определение частоты возврата шифром различных значений ΔC для заданного заранее ΔP . Это знание позволяет атакующему вскрыть часть ключа или ключ целиком.

Оценка стойкости шифра к достаточно разнообразным типам криптоаналитических нападений является основой при разработке любого шифра. Также необходима периодическая перепроверка стойкости с целью исключения случаев использования криптоалгоритмов, потерявших свою стойкость.

При проведении криптоанализа для вскрытия некоторого конкретного шифра возможно построение математической модели решаемой задачи, что позволяет использование многих методов алгебры и теории чисел. Такой способ постановки задачи уже привёл к раскрытию многих криптосистем.

С развитием математики и средств вычислительной техники вполне естественно уменьшение стойкости криптоалгоритма. Влияние роста мощности компьютеров на стойкость алгоритмов можно предсказать с той или иной степенью точности, до настоящего момента каждое десятилетие скорость вычислений вырастала на порядок. Однако оценить перспективы научного прогресса на данном этапе не решаемая задача со множеством неизвестных.

Литература

1. <https://cyberleninka.ru/article/n/statisticheskiiy-analiz-sovremennyh-blochnyh-shifrov/viewer>

2. <https://cyberleninka.ru/article/n/effektivnye-metody-algebraicheskogo-kriptoanaliza-i-zaschita-ot-nih/viewer>
3. <https://www.hse.ru/data/712/315/1234/%D0%90%D0%B2%D0%B4%D0%BE%D1%88%D0%B8%D0%BD.%D0%A1%D0%B0%D0%B2%D0%B5%D0%BB%7.pdf>

Сведения об авторах

Кенжалиева Светлана Заировна, кандидат педагогических наук, доцент, старший преподаватель кафедры математики (и математических основ криптографической защиты информации) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Алексеев Антон Дмитриевич, курсант Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Белов Аркадий Викторович, курсант Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

**Кирюшин Иван Иванович,
Печатнова Елена Владимировна,
Шадып Аялга Олеговна**

АКТУАЛЬНЫЕ ВОПРОСЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ БВС САМОЛЕТНОГО ТИПА VTOL В МВД РОССИИ

Беспилотные воздушные суда (далее – БВС) самолетного типа вертикального взлета и посадки (далее – VTOL) представляют собой разновидность БВС, сочетающих в себе технологии вертикального взлета и посадки. Их основной особенностью является контролируемость изменения вектора тяги. Существуют различные конструктивные схемы, позволяющие сочетать указанные технологии. Их разработка и совершенствование является одним из актуальных направлений развития беспилотной авиации. В частности, в настоящее время используются аппараты, функционирование которых основано на изменении положения фюзеляжа (тейлситтеры), а также БВС, использующие поворотные крылья или поворотные двигатели (конвертопланы).

Использование перечисленных технологий позволяет сочетать в себе лучшие качества БВС самолётного типа и конвертоплана. Особенностью устройства является то, что полет происходит полностью в автоматическом режиме, по окончании выполнения задания самолет возвращается домой. Взлет и посадка происходят в вертикальном режиме практически с любой поверхности, не требуется использование катапульты и парашюта. Для составления полетного задания достаточно указать область на карте, далее производится автоматический расчет траектории полета, после чего загружается схема полета и запускается БВС. Каждому снимку будут присвоены координаты точки, в которой он был сделан.

Упрощенно можно сказать, что VTOL взлетают «по-вертолетному» за счет двигателей с пропеллерами, установленными в горизонтальной плоскости, а затем перемещаются «по-самолетному», например, за счет толкающего или тянущего винта, установленного в вертикальной плоскости. Такие аппараты обладают тем неоспоримым преимуществом, что подобно вертолетам, не требуют ВПП или пусковой катапульты для взлета и парашюта для приземления.

Перечисленные особенности конструкции БВС VTOL и преимущества перед рядом других БВС отрывают широкие перспективы их использования в подразделениях МВД России.

В первую очередь можно отметить большее удобство их использования в лесистой местности – за счет времени и дальности полетов, которое зачастую оказывает решающее влияние ввиду удаленности от основных дорог, и дальности по расстоянию. Время полета БВС квадрокоптерного типа составляет 30-50 минут, а его увеличение непосредственно связано с заменой аккумулятора, что приводит к нарушению непрерывности фиксации; решение обозначенной проблемы содержится в применении метода карусели, однако он сопряжен с увеличением числа судов и пилотов и соответствующими затратами. Этих недостатков лишены БВС VTOL, что может стать решающим преимуществом при пресечении и расследовании нарушений, связанных с незаконной вырубкой, ловлей или охотой.

Также преимущества БВС VTOL очевидны при решении задач по поиску украденных автомобилей и работе с подразделениями по контролю за оборотом наркотиков. Это связано с тем, что квадрокоптеры направлены на решение более узких задач, что связано с менее широкими возможностями. Основное преимущество БВС VTOL при решении данной задачи заключается в возможности полетов на дальние расстояния без нарушения непрерывности съемки.

БВС VTOL эффективны при работе на большой площади. С их помощью можно обследовать территорию включающую в себя несколько населенных пунктов. Система, используемая в БВС VTOL позволяет подробно осмотреть все интересующие точки с большим увеличением и требуемым качеством картинки, за один полет. Подобная работа с помощью квадрокоптера требует больше времени, а также большее число полетов, включая переезд с места на место, время на обратный полет, посадку, свертывания системы и обратное развертывание на новом месте.

Кроме того, в сравнении с БВС самолетного типа, для работы с БВС VTOL не требуется наличие взлетной посадочной площадки, что является важным фактором в пользу использования VTOL в подразделениях МВД России.

Следует отметить достоинство, связанное с системой управления с базовой станцией и большими антеннами, которая дает возможность без проблем наблюдать за интересующими точками на большом удалении. При этом сигнал не ослабевает, как на квадрокоптерах. Большим плюсом базовой станции является поддержка и обеспечение Real Time Kinematic (далее – RTK) – это особый метод спутникового позиционирования, который может давать результаты измерений с точностью до сантиметра. Аппарат с большой точностью совершает посадку, что снижает риски, если приходится работать на ограниченной площадке.

При этом можно выделить ряд нерешенных вопросов, связанных с использованием БВС VTOL в МВД России.

Не решена до сих пор проблема с транспортировкой подразделений и оборудования БВС. Данные подразделения необходимо комплектовать соответствующими транспортными средствами, обязательно сочетающими в себе компактность (но имеющим возможность разместить все необходимое оборудование), функциональность и автономность, что, в свою очередь, включает возможность работать в комфортных условиях, не выходя из автомобиля и имея возможность подключения большого монитора, стационарно установленного и не требующего дополнительного времени для его развертывания.

Кроме того, не проработан вопрос, связанный с требованиями по обучению БВС VTOL, в частности достаточно ли наличия обучения на применение беспилотных воздушных судов коптерного типа с максимальной взлетной массой 30 кг и менее или требуется дополнительное обучение.

При использовании БВС VTOL следует учитывать ограничения по высоте полета: наиболее эффективна работа на высоте от 300 метров. Это ведет к необходимости регулярного формирования навыков пилотирования.

С БВС VTOL, как и с БВС самолетного типа существует проблема, связанная с тем, что на каждую модель (а не только на тип) необходимо пройти обучение и получать допуск отдельно. В то же время отмечается фактическое отсутствие возможности обучения на ряд моделей БВС VTOL.

Правовое регулирование полетов в МВД России является одним из проблемных вопросов, который регулируется приказом №1111 от 29 декабря 2022 г. «Об утверждении Курса поддержания летной натренированности авиационного персонала МВД России на беспилотных воздушных судах». В настоящее время наблюдаются многочисленные нарушения требований полетов, что ведет к увеличению вероятности авиационного происшествия.

Рассмотрев достоинства и недостатки использования БВС VTOL в МВД России предлагаются следующие рекомендации. Необходима разработка методических рекомендаций, которые позволят решать типовые технические задания. При этом важно описание особенностей работы с основными видами БВС VTOL, что позволит работать с различными моделями. Также предлагается на образовательных площадках проводить первоначальное обучение в очной форме для всех операторов БВС, а в дальнейшем при необходимости повышать квалификацию в дистанционной форме или очно на базе специализированных центров по подготовке операторов БВС VTOL. Это позволит оперативно повышать квалификацию сотрудников. Кроме того, в связи с значимыми достоинствами для решения задач в деятельности МВД рекомендуется внести БВС VTOL в таблицу положенности подразделений МВД России.

В заключении можно отметить, что БАС VTOL имеют большой технический потенциал в рамках совершенствования работы правоохранительных органов, но необходимо четко определить стандарты и требования к данной технике, обеспечив качественную подготовку персонала и оснастив его современным оборудованием, что позволит постоянно повышать его эффективность.

Литература

1. Баранов, А.Р. Основы применения беспилотных летательных аппаратов подразделениями органов внутренних дел / А.Р. Баранов, М.А. Ускова // Вопросы

совершенствования тактико-специальной подготовки сотрудников правоохранительных органов, Москва, 29 июня 2022 года / Московский университет МВД России имени В.Я. Кикотя. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. – С. 10-14.

2. Бидзян, Д.Р. О внедрении технологий цифровой трансформации в правоприменительную деятельность с последующей оценкой их эффективности / Д. Р. Бидзян // Синергия. – 2022. – № 3-4. – С. 5-16.

3. Кирюшин, И.И. Об использовании беспилотных летательных аппаратов в МВД России / И.И. Кирюшин, Н.А. Иванов // Вестник Барнаульского юридического института МВД России. – 2015. – № 1(28). – С. 109-112.

4. Кирюшин, И.И. Актуальные вопросы практического применения беспилотных авиационных систем в МВД России // Вестник учебного отдела Барнаульского юридического института МВД России. – 2023. – № 39. – С. 36-39

5. Коваленко, Д.Н. Использование беспилотных летательных аппаратов в деятельности Государственной инспекции безопасности дорожного движения / Д.Н. Коваленко, И.И. Кирюшин // Альтернативные источники энергии в транспортно-технологическом комплексе: проблемы и перспективы рационального использования. – 2017. – Т. 4, № 1(7). – С. 149-152.

6. Косовский, В.Б. Актуальные вопросы практического применения беспилотной техники в органах внутренних дел Российской Федерации / В.Б. Косовский, С.Н. Мартынюк // Общество: политика, экономика, право. – 2020. – № 3(80). – С. 25-29. – DOI 10.24158/per.2020.3.4.

Сведения об авторах

Кирюшин Иван Иванович, старший преподаватель кафедры информатики и специальной техники Барнаульского института МВД России.

Печатнова Елена Владимировна, кандидат технических наук, доцент кафедры «Организация и безопасность дорожного движения» Алтайского государственного технического университета им. И.И. Ползунова.

Шадып Аялга Олеговна, курсант Барнаульского юридического института МВД России.

**Копыткова Людмила Борисовна,
Фурсов Алексей Алексеевич**

МОДЕЛИ МОДУЛЯРНОГО КОДИРОВАНИЯ ЦЕЛЫХ ЧИСЕЛ РАЗНЫХ ЗНАКОВ

Идея модулярного кодирования зародилась в трудах Гаусса, Эйлера, Ферма, Мерсенна по теории чисел. Поэтому, прежде всего, выделим необходимые сведения теории делимости и теории сравнений, которые нам понадобятся для построения системы счисления в остаточных классах.

Возьмем попарно взаимно простые числа $p_1, p_2, \dots, p_n$, их произведение $P = p_1 p_2 \dots p_n$. Далее подберем числа $m_1, m_2, \dots, m_n$ так, что справедливо сравнение $\frac{P}{p_i} m_i \equiv 1 \pmod{p_i}$. Тогда для нахождения решения системы сравнений

$$A \equiv \alpha_i \pmod{p_i} \text{ находим число } A \equiv A_0 \pmod{P}, \text{ где } A_0 = \sum_{i=1}^n \frac{P}{p_i} m_i \alpha_i, i = \overline{1, n} \text{ [2].}$$

Роль этой теоремы в установлении взаимно-однозначного соответствия между целыми числами некоторого диапазона и множеством классов вычетов.

Для нахождения вычета числа применим метод Б. Паскаля (1623-1662) [2]. Идея которого состоит в замене степеней основания позиционной системы остатками от деления на модуль m .

Система остаточных классов (СОК) представляет собой непозиционную систему счисления, для которой характерен переход к системе вычетов по выбранным модулям. Если $p_1, p_2, \dots, p_n$ — основания системы, то

$$A = (\alpha_1, \alpha_2, \dots, \alpha_n), \text{ где } \alpha_i = A - \left\lfloor \frac{A}{p_i} \right\rfloor \cdot p_i, (i = \overline{1, n}) \text{ [1, 3].}$$

Можно показать, что для взаимно-простых оснований p_i представление числа A является единственным.

Представление числа в модулярном коде для целых неотрицательных чисел может быть расширено для целых чисел разных знаков. Для построения подобной модели необходимо отобразить отрицательный диапазон в

положительную область. Существуют различные способы построения этого отображения, каждый из которых порождает свою арифметику, т.е. получаем различные модели модулярного кодирования. Для представления отрицательных целых чисел в СОК возможны два подхода.

Первый подход – зашифровать знак числа в одном из разрядов. В качестве модуля здесь удобно взять 2, учитывая два возможных варианта. Число неотрицательное – приписываем значение 0, число отрицательное – приписываем – 1. Плюс этого метода – определить знак числа можно визуально. Минус этого метода – для модуля, в котором зашифрован знак, арифметика будет строиться по другим алгоритмам, в отличие от других оснований.

Второй подход – знак числа не связан с определенным модулем (говорят о скрытом знаке). Он предполагает разбиение основного диапазона на две области – положительную и отрицательную. При этом работа для всех модулей строится по одним алгоритмам, однако, тогда знак визуально мы не увидим. В этом случае операция определения знака числа будет немодульной операцией. Основоположники модулярной арифметики Акушский И.Я. и Юдицкий Д.И. в [1] описали такой подход, введя понятие искусственной формы числа.

Рассмотрим модель модулярной системы, в которой содержится четный модуль. Для разбиения диапазона на две области положительную и отрицательную возьмем $p_1, \dots, p_n$ – основания СОК, где $p_1 = 2$, величина

$\rho = \prod_{i=1}^n p_i$ характеризует объём диапазона. Числа поддиапазона $[0, P)$ будем

считать отрицательными, а числа поддиапазона $[P, \rho)$ – неотрицательными,

число $\frac{\rho}{2} = \prod_{i=2}^n p_i = P$ играет роль нуля. Согласно [1], введём искусственную

форму представления N' :

– если $N = |N|$ (положительные числа), то $N' = P + |N|$;

– если $N = -|N|$ (отрицательные числа), то $N' = P - |N|$.

Искусственная форма представления кодов СОК используется для выполнения модульных операций, т.е. сложения (вычитания) и умножения чисел.

Для нахождения суммы чисел N_1 и N_2 находим их искусственные формы $N'_1 = P + N_1$, $N'_2 = P + N_2$. Легко показать, что формула $(N_1 + N_2)' = N'_1 + N'_2 + P$ и будет определять сложение этих чисел.

Для вычисления произведения двух чисел N_1 и N_2 опять совершаем переход к искусственным формам, однако здесь четность или нечетность искусственных форм операндов определит вид результата:

$$(N_1 N_2)' = N'_1 N'_2 + P(N'_1 + N'_2).$$

Отсюда, если N'_1 , N'_2 - одинаковой четности, то $(N_1 N_2)' = N'_1 N'_2$; если же N'_1 , N'_2 - разной четности, то $(N_1 N_2)' = N'_1 N'_2 + P(N'_1 + N'_2)$. Таким образом, если N'_1 и N'_2 разной четности, то результат умножения уже представлен в искусственной форме, а если N'_1 и N'_2 одинаковой четности, то для получения искусственной формы к результату необходимо прибавить $P = (1, 0, 0, K, 0)$. Для определения четности N'_1 и N'_2 при наличии основания $p_1 = 2$ необходимо учитывать цифру по этому модулю (нечетные числа будут иметь по этому модулю 1, четные числа – 0). Если необходима будет коррекция результата, то она будет заключаться в инвертировании остатка результата по основанию p_1 .

Например, в системе с основаниями $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $P = 3 \cdot 5 \cdot 7 = 105$, найдем сумму и произведение $N_1 = -9$ и $N_2 = -11$.

Подсчитываем искусственные формы заданных чисел.

$$N'_1 = (1, 0, 0, 0) - (1, 0, 4, 2) = (0, 0, 1, 5),$$

$$N'_2 = (1, 0, 0, 0) - (1, 2, 1, 4) = (0, 1, 4, 3).$$

$$(N_1 + N_2)' = (0, 0, 1, 5) + (0, 1, 4, 3) + (1, 0, 0, 0) = (1, 1, 0, 1).$$

Проверим результат, переходя к десятичной системе:

$$(-9-11)' = (-20)' = 105 - 20 = (1, 0, 0, 0) - (0, 2, 0, 6) = (1, 1, 0, 1).$$

Для нахождения произведения, обратим внимание, что числа одинаковой чётности.

$$N'_1 N'_2 = (0, 0, 1, 5) \cdot (0, 1, 4, 3) = (0, 0, 4, 1)$$

Можно заметить, что $(0, 0, 4, 1) = (9 \cdot 11)' = (-9 \cdot (-11))'$

Отметим, что решаемые задачи не всегда предполагают наличие четного основания. Рассмотрим, как можно ввести знак числа в этом случае, тем самым построим модель модулярного кодирования с системой из нечетных оснований.

Пусть основания системы есть p_1, p_2, K, p_n , причем $p_1 = 2t + 1$.

Разобьем диапазон $P = p_1 \cdot p_2 \cdot K \cdot p_n$ на две части: $\left[0, \frac{P-1}{2}\right)$ и $\left[\frac{P-1}{2}, P\right)$. Число

$\frac{P-1}{2} = (\rho_1, \rho_2, K, \rho_n)$ примем в качестве нуля. Тогда положительные числа

$N = |N|$ представим в виде $N' = \frac{P-1}{2} + |N|$, а отрицательные числа $N = -|N|$ в

виде $N' = \frac{P-1}{2} - |N|$, т.е. общий вид искусственной формы числа будет

$$N' = \frac{P-1}{2} + N.$$

В этой модели сумма определяется соотношением

$$(N_1 + N_2)' = N'_1 + N'_2 + (\bar{\rho}_1, \bar{\rho}_2, K, \bar{\rho}_n),$$

где $\left(-\frac{P-1}{2}\right) = \frac{\overline{P-1}}{2} = (\bar{\rho}_1, \bar{\rho}_2, K, \bar{\rho}_n)$, $\bar{\rho}_i = p_i - \rho_i$, $i = 1, 2, K, n$.

Для нахождения произведения в этой модели справедлива формула

$$(N_1 N_2)' = \frac{P-1}{2} + N'_1 N'_2 - \frac{P-1}{2} \varphi, \text{ где } \varphi = N'_1 + N'_2 + \frac{P-1}{2}.$$

Заметим, что здесь как и в предыдущей модели результат будет зависеть от четности φ .

Для выполнения немодульных операций требуется определить с позиционные характеристики разрабатываемых моделей СОК.

К числу немодульных операций при неявном введении знака числа прежде всего можно отнести операцию определения этого знака. Эта задача связана с определением принадлежности числа $(\alpha_1, \alpha_2, \dots, \alpha_n)$ к той или иной половине диапазона. Проведем анализ метода интервальных оценок для определения знака числа, который опирается на позиционную характеристику номер интервала $l_A = \left\lceil \frac{A}{p_i} \right\rceil$ [3] ($p_1, p_2, \dots, p_n$ – система оснований, p_i – дробящий модуль), на следующем примере.

Пусть задана СОК с основаниями $p_1=2, p_2=3, p_3=5, p_4=11$. Для числа $A = (0,1,4,3)$ найдем номер интервала.

Объём диапазона $\rho = 330$, число $P = \rho/2 = 165$ примем в качестве нового нуля. Заметим, что рассматриваемый пример содержит четное основание $p_1 = 2$. Целые числа из интервала $[165; 330)$ будут означать целые неотрицательные числа интервала $[0; 165)$. Целые числа из интервала $[0; 165)$ есть отрицательные целые числа промежутка $[-165; 0)$. Пусть дробящий модуль $p_4 = 11$, тогда $P_4 = 30$. Для определения номера интервала вычисляем

$$\varphi(p_1) = 2 - 1 = 1, \varphi(p_2) = 3 - 1 = 2, \varphi(p_3) = 5 - 1 = 4, \varphi(p_4) = 11 - 1 = 10,$$

$$l_{A_1} = \left\lceil \frac{165}{11} \right\rceil_{30}^+ = 15, l_{A_2} = \left\lceil \frac{110^2}{11} \right\rceil_{30}^+ = 20, l_{A_3} = \left\lceil \frac{66^4}{11} \right\rceil_{30}^+ = 6, l_{A_4} = \left\lceil \frac{30^{10} - 1}{11} \right\rceil_{30}^+ = 19.$$

$$\text{Тогда } l_A = \left\lceil 15 \cdot 0 + 20 \cdot 1 + 6 \cdot 4 + 19 \cdot 3 \right\rceil_{30}^+ = \left\lceil 101 \right\rceil_{30}^+ = 11.$$

$$\text{Далее, учитывая, что } l_\rho = l_1 = \frac{P_1^{\varphi(p_1)}}{p_n} = \frac{165}{11} = 15, \text{ делаем вывод, что } l_A < l_\rho,$$

следовательно, наше число $A \in \left[0; \frac{P-1}{2}\right)$, т.е. при выбранном способе кодирования и построении отображения диапазонов число $A = (0,1,4,3)$ – отрицательное. Действительно, $A = 11 \cdot 11 + 3 = 124$ есть при наших допущениях изображение числа $124 - 165 = -41$.

Следует заметить, если все основания нечетные, то диапазон разбивается на нечетное число интервалов по выбранному p_i . Тогда имеется критический интервал, который является границей между положительным и отрицательным интервалами. При попадании числа в критический интервал, этот интервал необходимо разделить на две части. Далее для определения знака числа необходимо сравнить остатки по модулю p_i .

Таким образом, можно сделать следующие выводы. Расширение моделей модулярного кодирования на случай целых чисел разных знаков связано с построением отображения отрицательного диапазона в положительную область, причём существуют различные способы построения этого отображения, которые порождают свою арифметику. Для построения модели важен выбор системы оснований и определение базовых позиционных характеристик. Алгоритмы выполнения немодульных операций в СОК для чисел разных знаков можно построить, используя известные алгоритмы этих операций для неотрицательных чисел и алгоритмы определения знака числа.

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Советское радио, 1968. 440 с.
2. Бухштаб А.А. Теория чисел. М.: Изд-во «Просвещение», 1966. 384 с.
3. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов (СОК). Учебное пособие. – Ставрополь: Изд-во СКФУ, 2016. 225 с.

Сведения об авторах

Копыткова Людмила Борисовна, кандидат физико-математических наук, доцент кафедры Математического анализа, алгебры и геометрии Северо-Кавказского федерального университета.

Фурсов Алексей Алексеевич, магистр Северо-Кавказского федерального университета.

**Коренева Ольга Владимировна,
Алланов Артем Евгеньевич**

ПРИМЕНЕНИЕ ОПЕРАЦИОННОГО ИСЧИСЛЕНИЯ В ИССЛЕДОВАНИИ ПЕРЕДАТОЧНОЙ ФУНКЦИИ

Операторный метод является мощным инструментом для анализа переходных процессов в электрических цепях. Этот подход включает преобразование расчетов из временной области, где функции зависят от времени $h\ t$, в область комплексной переменной, известной как операторная переменная. В результате дифференциальные уравнения, описывающие систему, становятся алгебраическими, что значительно упрощает их решение. В основе операторного метода лежит использование комплексных чисел для представления операторов, связанных с функциями времени. Функция, определенная во временной области, называется оригиналом, тогда как её представление в комплексной области называется изображением.

Одним из ключевых понятий в теории автоматического управления и электротехнике является передаточная функция. Она служит для математического описания динамического поведения системы. Передаточная функция выражает соотношение между входом и выходом линейной стационарной системы через дифференциальный оператор. Конкретно, это отношение преобразования Лапласа выходного сигнала к преобразованию Лапласа входного сигнала при условии, что начальные условия равны нулю. В теории управления, передаточная функция используется для анализа и синтеза систем автоматического регулирования. Она позволяет определить устойчивость и качество системы, а также разработать корректирующие устройства для достижения желаемого поведения. В электротехнических приложениях передаточная функция также играет важную роль. Например, она помогает в анализе электрических цепей, включая фильтры, усилители и системы передачи сигналов. Используя передаточную функцию, можно легко оценить, как цепь

реагирует на различные входные воздействия и как изменяются характеристики системы при изменении параметров компонентов.

Преобразование Лапласа, являясь неотъемлемой частью операторного метода, представляет собой интегральное преобразование, которое переводит функции времени в функции комплексного переменного. Это преобразование широко применяется в инженерных дисциплинах для решения задач, связанных с дифференциальными уравнениями, что существенно облегчает анализ и синтез сложных систем. Таким образом, операторный метод и преобразование Лапласа являются фундаментальными инструментами, которые находят широкое применение в электротехнике и теории автоматического управления. Они обеспечивают мощные средства для анализа и синтеза систем, что способствует развитию и совершенствованию современных технологий. Определим передаточную функцию для схемы, представленной на рисунке 1.

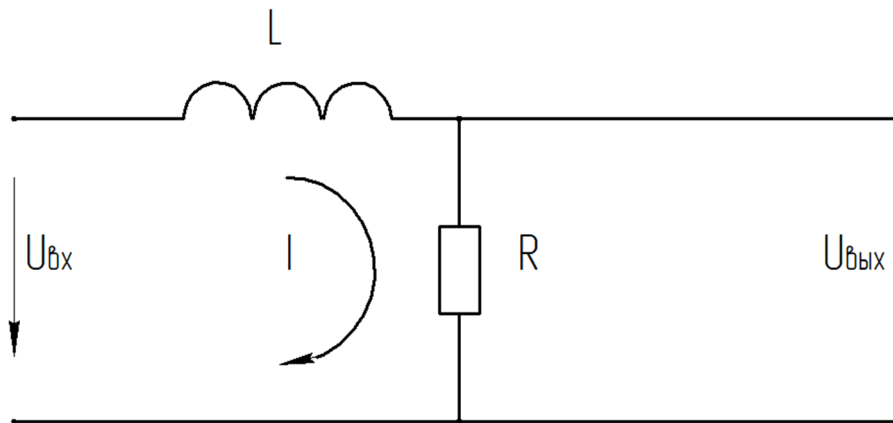


Рис. 1. Схема электрической цепи

Математическая модель для этой схемы во временной характеристике:

$$\begin{cases} U_{вх}(t) = L \frac{di}{dt} + R \times i(t) \\ U_{вых}(t) = R \times i(t) \end{cases}$$

Математическая модель для этой схемы в операторной форме:

$$\begin{cases} U_{вх}(p) = Lp \times I(p) + R \times I(p) \\ U_{вых}(p) = R \times I(p) \end{cases}$$

Передаточная функция схемы, представленной на рисунке 1, имеет вид:

$$W(p) = \frac{U_{\text{ВЫХ}}(p)}{U_{\text{ВХ}}(p)} = \frac{R \times I(p)}{Lp \times I(p) + R \times I(p)} = \frac{1}{\frac{L}{R} \times p + 1} = \frac{1}{Tp + 1}$$

$$\text{где } T = \frac{L}{R}.$$

Кривая переходного процесса (переходная характеристика) электротехнической системы может быть построена разными методами, среди которых операторный метод является одним из основных. Для анализа динамического поведения различных систем важно использовать стандартизированные входные воздействия. Одним из таких воздействий является мгновенное изменение входного сигнала от нуля до единицы, что соответствует единичной ступенчатой функции. Реакция системы на это изменение при нулевых начальных условиях называется переходной характеристикой $h(t)$. Переходная функция $h(t)$ описывает изменение выходной переменной $y(t)$ при подаче на вход единичной ступенчатой функции времени $1(t)$ при нулевых начальных условиях. Переходная характеристика системы отражает её временное поведение в ответ на единичный скачок напряжения или тока на входе, при отсутствии начальной энергии. Это отклик системы на входной сигнал, позволяющий оценить её динамические свойства. Для обратного преобразования Лапласа существует специальная таблица оригиналов и изображений, которая значительно упрощает процесс нахождения оригиналов функций по их изображениям. Эта таблица содержит широкий спектр стандартных функций, а также их изображения в виде выражений с оператором p . При нахождении обратного преобразования Лапласа для конкретной функции изображения необходимо найти соответствующую строку в таблице и применить соответствующее правило обратного преобразования. Такой подход делает процесс нахождения переходной характеристики или оригинала других функций более простым и эффективным.

Если передаточная функция системы имеет вид: $W(p) = \frac{1}{Tp+1}$,

Изображение переходной функции: $h(t) = 1 - e^{-at}$, где $a = \frac{1}{T}$.

По таблице оригиналов и изображений оригинал переходной функции представляет собой выражение: $-L^{-1} \left[\frac{1}{p(Tp+1)} \right]$

$$p(Tp + 1) = 0$$

$$p_2 = 0 \text{ или } Tp + 1 = 0$$

$$Tp = -1 \qquad p_1 = -\frac{1}{T}$$

$$W(p) = \frac{k_1}{p - p_1} + \frac{k_2}{p - p_2}$$

$$k_1 = \left[\left(p - \frac{1}{T} \right) \times \frac{1}{p(p - p_1)} \right]_{p=\frac{1}{T_1}} = -T$$

$$k_2 = \left[p \times \frac{1}{p(p - p_1)} \right]_{p_2=0} = \frac{1}{p}$$

$$W(p) = -T \times \frac{1}{p + \frac{1}{T}} + \frac{1}{p}$$

Для нахождения обратного преобразования Лапласа L^{-1} воспользуемся следующим выражением: $L^{-1} \left[\frac{1}{p+a} \right] = b \times e^{-at}$.

$$h(t) = -e^{-\frac{1}{T} \times t} + 1$$

Постоянная времени T – это время, в течение которого выходная величина достигла бы своего установившегося значения, если бы она изменялась с постоянной скоростью, равной скорости изменения ее в начальный момент времени.

Теоретически время переходного процесса $t_{np} = \infty$. Фактически переходный процесс считается законченным, когда выходной сигнал входит в 5%-й «коридор», т.е. $x_{\text{вых}}(t) = 0.95x_{\text{вых.уст}}$.

Время переходного процесса определяется из уравнения

$$x_{\text{вых}}(t) = k \left(1 - e^{-\frac{t_{np}}{t}} \right).$$

Очевидно, $e^{-\frac{t_{np}}{t}} = 1 - 0,95 = 0,05$.

Решая полученное уравнение относительно времени переходного процесса $t_{нп}$, получим $t_{нп} = 3T$.

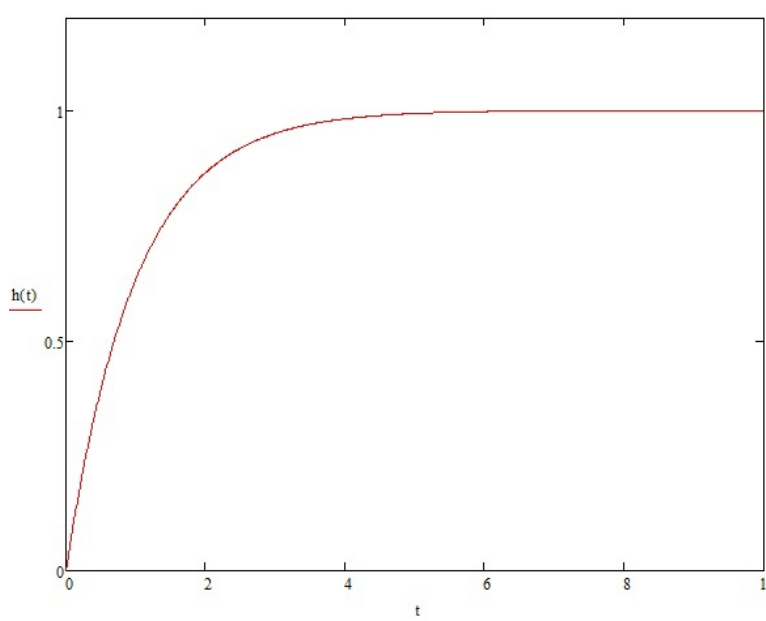


Рис. 2. Переходная функция апериодического звена

В итоге делаем вывод, что во всех случаях расчета переходных процессов в электрических цепях операторным методом:

1. Определяются начальные условия.
2. Записывается уравнение или система уравнений для заданной цепи в операторной форме.
3. Находятся изображения искомых токов или напряжений.
4. По полученным изображениям отыскиваются оригиналы, которые являются мгновенными значениями токов или напряжений переходного процесса.

Операционное исчисление имеет важное прикладное значение, в частности, позволяет рассчитывать переходные режимы в электрических цепях при любых внешних источниках напряжений и токов. Кроме рассмотренной задачи электротехники методы операционного исчисления находят широкое применение в механике, автоматике и в других самых разнообразных отраслях науки и техники [2].

Литература

1. Плескунов, М.А. Операционное исчисление: учебное пособие для вузов / М. А. Плескунов; под научной редакцией А. И. Короткого. – Москва: Издательство Юрайт, 2024. – 141 с.
2. Теория функций комплексного переменного: учеб. пособие / Н.В. Гредасова, Н.И. Желонкина, М.А. Корешникова [и др.]. – Екатеринбург: Изд-во Урал. ун-та, 2018.– 128 с.
3. Корзников, А.Д. Операционное исчисление: учебно-методическое пособие для студентов специальностей «Электрические станции», «Электроэнергетические системы и сети», / А.Д. Корзников, О.М. Королева. – Минск: БНТУ, 2021. – 85 с.

Сведения об авторах

Коренева Ольга Владимировна, кандидат технических наук, доцент кафедры высшей математики Кубанского государственного технологического университета.

Алланов Артем Евгеньевич, студент Кубанского государственного технологического университета.

**Коренева Ольга Владимировна,
Огарев Артем Александрович**

МЕТОД ОПЕРАТОРОВ И ПРЕОБРАЗОВАНИЕ ЛАПЛАСА, ИХ ПРИМЕНЕНИЕ В ЭЛЕКТРОТЕХНИКЕ И ТЕОРИИ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

Операторный метод является мощным инструментом для анализа переходных процессов в электрических цепях. Этот подход включает преобразование расчетов из временной области, где функции зависят от времени t , в область комплексной переменной, известной как операторная переменная. В результате дифференциальные уравнения, описывающие систему, становятся алгебраическими, что значительно упрощает их решение.

В основе операторного метода лежит использование комплексных чисел для представления операторов, связанных с функциями времени. Функция, определенная во временной области, называется оригиналом, тогда как её представление в комплексной области называется изображением.

Одним из ключевых понятий в теории автоматического управления и электротехнике является передаточная функция. Она служит для математического описания динамического поведения системы. Передаточная функция выражает соотношение между входом и выходом линейной стационарной системы через дифференциальный оператор. Конкретно, это отношение преобразования Лапласа выходного сигнала к преобразованию Лапласа входного сигнала при условии, что начальные условия равны нулю.

В теории управления, передаточная функция используется для анализа и синтеза систем автоматического регулирования. Она позволяет определить устойчивость и качество системы, а также разработать корректирующие устройства для достижения желаемого поведения.

В электротехнических приложениях передаточная функция также играет важную роль. Например, она помогает в анализе электрических цепей, включая фильтры, усилители и системы передачи сигналов. Используя передаточную

функцию, можно легко оценить, как цепь реагирует на различные входные воздействия и как изменяются характеристики системы при изменении параметров компонентов.

Преобразование Лапласа, являясь неотъемлемой частью операторного метода, представляет собой интегральное преобразование, которое переводит функции времени в функции комплексного переменного. Это преобразование широко применяется в инженерных дисциплинах для решения задач, связанных с дифференциальными уравнениями, что существенно облегчает анализ и синтез сложных систем.

Таким образом, операторный метод и преобразование Лапласа являются фундаментальными инструментами, которые находят широкое применение в электротехнике и теории автоматического управления. Они обеспечивают мощные средства для анализа и синтеза систем, что способствует развитию и совершенствованию современных технологий. Определим передаточную функцию для схемы, представленной на рисунке 1.

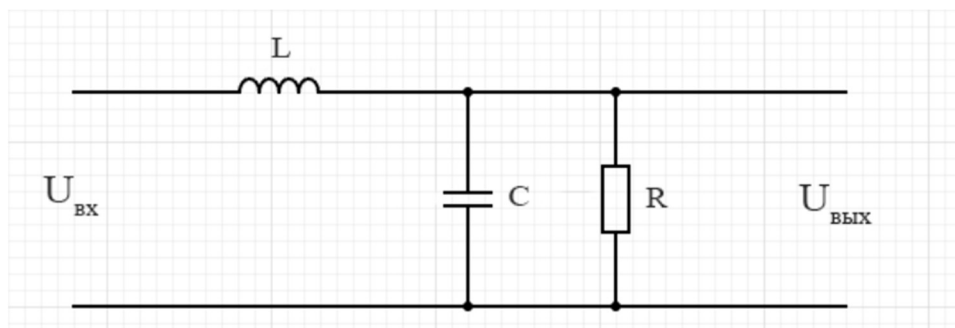


Рис. 1. Схема электрической цепи

Для рассматриваемой электрической цепи характеристики в операторной форме можно выразить следующими уравнениями:

$$\left\{ \begin{array}{l} U_{ВХ}(p) = L * p \times I(p) + \frac{\frac{1}{C * p} * R}{\frac{1}{C * p} + R} \times I(p) \\ U_{ВЫХ}(p) = \frac{\frac{1}{C * p} * R}{\frac{1}{C * p} + R} \times I(p) \end{array} \right.$$

Передаточная функция для схемы, изображенной на рисунке 1, определяется следующим образом:

$$W(p) = \frac{U_{\text{ВЫХ}}(p)}{U_{\text{ВХ}}(p)} = \frac{\left(\frac{1}{Cp} \cdot R\right) / \left(\frac{1}{Cp} + R\right) \cdot I(p)}{Lp \cdot I(p) + \left(\frac{1}{Cp} \cdot R\right) / \left(\frac{1}{Cp} + R\right) \cdot I(p)} = \frac{R/(RCp + 1)}{Lp + R/(RCp + 1)}$$

Упрощая выражение, получаем:

$$W(p) = \frac{1/(RCp + 1)}{L/R \cdot p + 1/(RCp + 1)} = \frac{1}{LCp^2 + \frac{L}{R}p + 1}$$

В обобщенной форме передаточная функция записывается так:

$$W(p) = \frac{1}{T_2^2 p^2 + T_1 p + 1}$$

где $T_1 = \frac{L}{R}$, $T_2^2 = LC$

Преобразование к стандартной форме.

Чтобы привести эту функцию к виду $W(p) = \frac{1}{(Tp+1)^2}$

делаем следующие предположения: $T_2 = T$, $T_1 = 2T$

Подставив эти значения, получаем:

$$W(p) = \frac{1}{T^2 p^2 + 2Tp + 1} = \frac{1}{(Tp + 1)^2}$$

Кривая переходного процесса (переходная характеристика) электротехнической системы может быть построена разными методами, среди которых операторный метод является одним из основных. Для анализа динамического поведения различных систем важно использовать стандартизированные входные воздействия. Одним из таких воздействий является мгновенное изменение входного сигнала от нуля до единицы, что соответствует единичной ступенчатой функции.

Реакция системы на это изменение при нулевых начальных условиях называется переходной характеристикой $h(t)$. Переходная функция $h(t)$

описывает изменение выходной переменной $y(t)$ при подаче на вход единичной ступенчатой функции времени $1(t)$ при нулевых начальных условиях.

Переходная характеристика системы отражает её временное поведение в ответ на единичный скачок напряжения или тока на входе, при отсутствии начальной энергии. Это отклик системы на входной сигнал, позволяющий оценить её динамические свойства.

Для обратного преобразования Лапласа существует специальная таблица оригиналов и изображений, которая значительно упрощает процесс нахождения оригиналов функций по их изображениям. Такие таблицы можно найти в любой книге по операционному исчислению. Эта таблица содержит широкий спектр стандартных функций, а также их изображения в виде выражений с оператором p . При нахождении обратного преобразования Лапласа для конкретной функции изображения необходимо найти соответствующую строку в таблице и применить соответствующее правило обратного преобразования. Такой подход делает процесс нахождения переходной характеристики или оригинала других функций более простым и эффективным.

Если передаточная функция системы имеет вид:

$$W(p) = \frac{1}{(Tp + 1)^2} = \frac{1}{T^2} * \frac{1}{(p + \frac{1}{T})^2}$$

Для нахождения переходной функции $h(t)$ системы воспользуемся таблицей оригиналов и изображений.

$$h(t) = \mathcal{L}^{-1} \left[\frac{1}{p} W(p) \right] = \mathcal{L}^{-1} \left[\frac{1}{T^2} \cdot \frac{1}{p(p + 1/T)^2} \right]$$

Используя свойства преобразования Лапласа и соответствующую строку таблицы, мы получаем:

$$h(t) = \frac{1}{T^2} \cdot T^2 \left(1 - e^{-t/T} - \frac{t}{T} e^{-t/T} \right) = 1 - \left(1 + \frac{t}{T} \right) e^{-t/T}$$

Постоянная времени T характеризует время, за которое выходная величина системы достигла бы своего установившегося значения, если бы она изменялась

с постоянной скоростью, равной скорости изменения в начальный момент времени. Теоретически, время переходного процесса (t_{Π}) стремится к бесконечности. Однако, практически, переходный процесс считается завершённым, когда выходной сигнал входит в 5%-й «коридор» установившегося значения. Это означает, что выходная величина ($x_{\text{вых}}(t)$) достигает 95% от своего установившегося значения ($x_{\text{вых.уст}}$).

Окончательная формулировка

$$h(t) = 1 - \left(1 + \frac{t}{T}\right) e^{-t/T}$$

Эта функция описывает изменение выходного сигнала во времени при подаче единичного ступенчатого воздействия на вход системы.

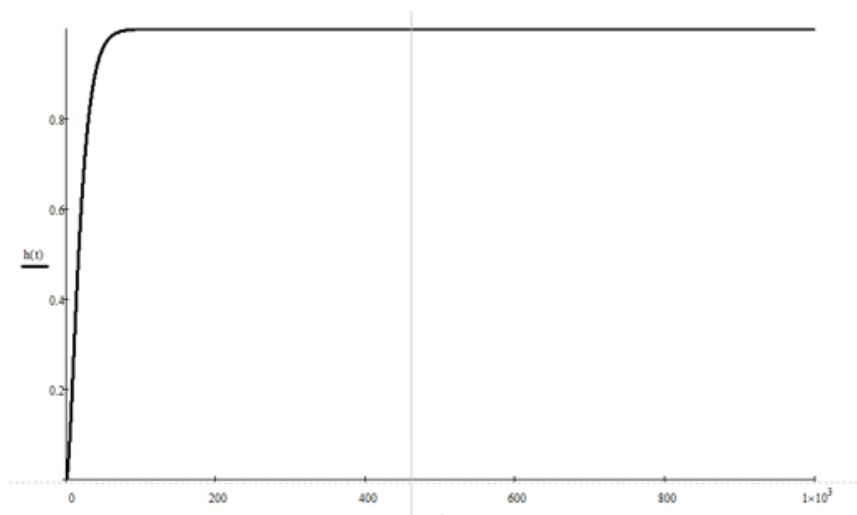


Рис. 2. График переходной функции второго порядка

В заключение, операторный метод является важным инструментом для инженеров и исследователей в области электротехники и автоматического управления. Его применение позволяет проводить более глубокий анализ и проектирование электротехнических систем, что способствует развитию новых технологий и повышению эффективности существующих.

Литература

1. Плескунов, М.А. Операционное исчисление: учебное пособие для вузов / М.А. Плескунов ; под научной редакцией А.И. Короткого. – Москва: Издательство Юрайт, 2024. – 141 с.
2. Теория функций комплексного переменного: учеб. пособие / Н.В. Гредасова, Н.И. Желонкина, М.А. Корешникова [и др.]. – Екатеринбург: Изд-во Урал. ун-та, 2018. – 128 с.
3. Корзников, А.Д. Операционное исчисление: учебно-методическое пособие для студентов специальностей «Электрические станции», «Электроэнергетические системы и сети», / А.Д. Корзников, О.М. Королева. – Минск: БНТУ, 2021. – 85 с.

Сведения об авторах

Коренева Ольга Владимировна, кандидат технических наук, доцент кафедры высшей математики Кубанского государственного технологического университета.

Огарев Артем Александрович, студент Кубанского государственного технологического университета.

**Корчагина Елена Васильевна
Ярцева Анна Александровна**

ОПТИМИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ УИС С ПОМОЩЬЮ МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ

Аудит информационной безопасности является важным шагом при оптимизации системы безопасности в учреждениях уголовно-исполнительной системы (УИС). Он предоставляет собой объективную оценку текущего уровня безопасности информационной системы и помогает выявить потенциальные риски, связанные с конфиденциальными данными. Аудит информационной безопасности подразделяется на две основные категории: внешний аудит и внутренний аудит.

Если внешний аудит представляет собой разовое мероприятие (либо график регулярных разовых мероприятий), то внутренний аудит информационной безопасности организации является системным процессом, процедуры которого выполняются постоянно в процессе функционирования объекта [1].

Организация аудита и анализа безопасности информационной системы производится в рамках ИТ-аудита учреждения и курируется руководством, начальником отдела информационной безопасности или специалистом по информационной безопасности. Оценка состояния безопасности информационной системы организации производится в несколько этапов, включающих сбор и анализ информации, подготовку отчёта и выработку рекомендаций по оптимизации уровня информационной безопасности организации и защиты данных в организациях от утечки [2].

Оптимизация систем безопасности в инфокоммуникационных системах УИС может быть достигнута с использованием моделирования информационных потоков с использованием системы Arcsight и сканера уязвимостей XSpider [3]. Применение ArcSight совместно с XSpider в рамках

модернизации информационной системы безопасности (ИСБ) в Интернет-клиент-сервер (ИКС) УИС позволяет создать эффективную систему мониторинга и анализа информационных потоков, обеспечивая высокий уровень защиты от внутренних и внешних угроз. Это объясняется тем, что ArcSight позволяет производить:

1. Централизованный сбор и анализ данных. ArcSight собирает данные о событиях безопасности из различных источников (сетевые устройства, серверы, приложения и т.д.) в единую платформу. Это позволяет получить целостное представление о происходящем в информационной системе УИС.

2. Корреляция событий. ArcSight анализирует собранные данные, выявляет взаимосвязи между событиями и обнаруживает аномалии, которые могут указывать на наличие угрозы.

3. Визуализация данных. ArcSight предоставляет инструменты для визуализации данных, что упрощает анализ и понимание ситуации в области безопасности.

4. Автоматическое реагирование. ArcSight может быть настроен на автоматическое выполнение определенных действий при обнаружении угрозы, например, блокировка доступа к определенному ресурсу или запуск антивирусной проверки.

XSpider в свою очередь обеспечивает:

1. Моделирование информационных потоков. XSpider позволяет создавать модели информационных потоков в УИС, что помогает выявить уязвимости и потенциальные пути проникновения злоумышленников.

2. Анализ уязвимостей. XSpider проводит автоматический анализ уязвимостей в инфраструктуре и приложениях УИС.

3. Оценка рисков. XSpider помогает оценить риски информационной безопасности и определить приоритеты в работе по их снижению.

Важным аспектом в ходе моделирования информационных потоков с использованием Arcsight и XSpider является наличие синергетического эффекта. Это явление заключается в следующем:

- Комплексный анализ. Совместное использование ArcSight и XSpider позволяет получить комплексное представление о состоянии информационной безопасности УИС, включая анализ событий, уязвимостей и рисков.
- Проактивное реагирование. Интеграция XSpider с ArcSight позволяет автоматически запускать процессы реагирования на инциденты, выявленные при анализе уязвимостей.
- Повышение эффективности. Автоматизация процессов анализа и реагирования позволяет снизить нагрузку на сотрудников службы безопасности и повысить эффективность их работы.

Практическая значимость обеспечения ИБ на основе моделирования информационных потоков с использованием Arcsight и XSpider на объектах УИС состоит в том, что:

1. XSpider выявляет уязвимость в веб-приложении, используемом для управления доступом к информационным ресурсам УИС. ArcSight обнаруживает попытку эксплуатации этой уязвимости и автоматически блокирует доступ злоумышленника.
2. XSpider строит модель информационных потоков, которая показывает, что определенный сервер является критически важным для функционирования УИС. ArcSight настраивается на более пристальный мониторинг этого сервера и быстрое реагирование на любые инциденты, связанные с ним.

Таким образом, применение ArcSight совместно с XSpider позволяет создать в ИКС УИС эффективную систему мониторинга и анализа информационных потоков, обеспечивая высокий уровень защиты от внутренних и внешних угроз. Этот подход способствует повышению эффективности работы службы безопасности и снижению рисков информационной безопасности в целом.

Литература

1. Симонов С.В. Технологии аудита информационной безопасности / С.В. Симонов // Конфидент. Защита информации. – 2002. – № 2. – С. 36-41.
2. Петренко С.А. Аудит безопасности корпоративных информационных систем / С.А. Петренко // Защита информации. – 2002. – С. 30-37.
3. Никулин С.А. Разработка методик и алгоритмов обеспечения безопасности информации в автоматизированных системах управления специального назначения / С.А. Никулин, С.С. Никулин // Вестник Воронежского института ФСИН России. – 2015. – № 1, январь–март. – С. 57 64.

Сведения об авторах

Корчагина Елена Васильевна, кандидат физико-математических наук, доцент, начальник кафедры математики и естественно-научных дисциплин Воронежского института Федеральной службы исполнения наказаний.

Ярцева Анна Александровна, курсант Воронежского института Федеральной службы исполнения наказаний.

**Кошелев Дмитрий Александрович,
Ромашов Арсений Александрович,
Корза Евгений Александрович**

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МОДУЛЯЦИИ С
ИСПОЛЬЗОВАНИЕМ СТОХАСТИЧЕСКИХ СИГНАЛОВ ДЛЯ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ
В КРУ РТК ВН**

В современном мире все чаще для выполнения различных работ, включая выполнение боевых задач, используют роботов, оснащенных различного рода датчиками, приемниками, средствами обратной связи и навигации.

В наземной робототехнике специального назначения основными направлениями по обеспечению защиты информации является защита передаваемой информации по каналам радиопередачи (КРУ), потому что на данном этапе существует множество угроз безопасности информации, при реализации которых противник может завладеть как самой информацией, так и завладеть роботом или целым комплексом.

Дистанционное управление роботами (комплексами роботов) реализуется за счет беспроводной системы связи, которая является одним из наиболее уязвимых мест в данных комплексах, так как есть вероятность реализации различных угроз: просмотр информации, подмен управляющих команд, перехват и подавление передаваемой информации с помощью помех.

Целью данной статьи является продемонстрировать возможности основных методов модуляции для обеспечения защиты передаваемой телеметрической информации, а также обосновать необходимость и актуальность применения их в системах радиосвязи группы роботов.

Достаточно много разработано различных методов модуляции, а также вариантов обработки стохастических сигналов. Прежде всего стохастический сигнал – это шумоподобный сигнал и поэтому развитие систем связи с применением таких сигналов тормозилось отсутствием возможности

математического анализа потенциальной помехоустойчивости этих систем, а также несовершенством элементов радиотехнических устройств. Но с развитием цифровых технологий, а также с ростом вычислительного потенциала персональных компьютеров в настоящее время появилась возможность адекватно оценивать описанные выше параметры, однако за последнее десятилетие не публиковались работы, на основании которых можно сделать вывод о вероятности возникновения возможных ошибок при применении соответствующих методов.

Полученные в 60-х годах результаты оценки помехоустойчивости ошибочно базировались на предположении о гауссовом распределении величины на входе детектора (это предположение базировалось на аналогии с классическими системами связи, в основе которых лежит взаимно-корреляционный прием).

В настоящей статье мы хотим показать основные методы модуляции, а также, что уровень помехоустойчивости позволяет использовать данные сигналы в целых радиосетях групп роботов, где необходимо обеспечить конфиденциальность и безопасность информации.

Анализ методов модуляции.

Основными методами внесения информации в стохастический сигнал являются бинарные методы. В свою очередь они подразделяются на классические и модифицированные.

Классическими считаются методы: амплитудной, частотной, фазовой (угловой) модуляции. Однако на практике используются улучшенные или модифицированные версии, которые мы также рассмотрим в данной главе.

Амплитудная манипуляция.

Амплитудная манипуляция стохастического сигнала (АМСС). В этом способе символ «0» заменяется пассивной паузой, а символ «1» наоборот фрагментом стохастического сигнала. Прием такого сигнала осуществляется энергетическими методами, а именно если на выходе демодулятора в конце

символьного интервала продолжительностью T наблюдается величина, которая превышает пороговое значение, то детектор выдает информации о приеме символа «1», иначе «0».

Частотная манипуляция.

Частотная манипуляция стохастического сигнала (ЧМСС). Передатчик при таком методе содержит два генератора шумоподобных сигналов, которые различаются между собой полосой частот. Параметры таких генераторов подбираются так, чтобы мощности выходных сигналов были равны, а частоты у них не пересекались.

Прием сигнала осуществляется также с помощью энергетических методов, а именно с помощью сравнения энергий выработанных генераторами сигналов. Необходимо отметить, что современные энергетические приемники позволяют выявить признаки модуляции при достаточно высоком соотношении сигнал-шум. А соответственно АМСС и ЧМСС имеют сравнительно небольшую структурную скрытность в шуме. Этого минуса нет в моделях с корреляционно-временной модуляцией (передача опорного сигнала). Они рассмотрены дальше.

Однако, простота реализации приемника и возможность передачи информации без опорного сигнала привели к развитию идей, заложенных в АМСС и ЧМСС, в различных направлениях, а именно:

- изменение характеристик стохастического сигнала на протяжении одного блока передающейся информации;
- изменение показателей мощности или дисперсии как основы переноса информации;
- применение многопозиционных импульсных схем модуляции.

Система Ланге-Мюллера.

Система Ланге-Мюллера (СЛМ). Передатчик при таком методе содержит два элемента с помощью которых организовывается задержка опорного сигнала на время T , t – при этом для каждого символа информации указывается один из

выбранных интервалов. Передатчик будет излучать сумму опорного и информационного сигнала.

Приемник в своем составе содержит два автокорреляционных блока с соответствующим временем задержек – по максимуму их выхода принимается решение о приеме символа.

Упрощенная система Ланге-Мюллера.

Упрощенная система Ланге-Мюллера (УСЛМ). Передатчик при таком методе содержит только один блок с помощью которых организовывается задержка опорного сигнала на время T , а вместо второго блока используется пассивная пауза, при этом устанавливается ненулевой порог автокорреляционной функции выходного сигнала (аналог работы с АМСС).

Автокорреляционная система с противоположными сигналами.

Автокорреляционная система с противоположными сигналами (по О.О. Воронину). В таком построении исходящий информационный сигнал всегда задерживается на установленное время T . Только при передаче символа «1» сигнал принимается форму опорного, а при передаче символа «0» принимает противоположное значение опорному сигналу.

Определение сигнала приемником осуществляется с помощью автокорреляционного устройства с соответствующей задержкой, при этом устанавливается рекомендуемый пороговый уровень детектора равным нулю, независимо от помех в среде.

Рассмотренные последние три типа модуляции имеют высокую структурную скрытность, но при этом имеется довольно большой минус – в системах образуется высокий уровень внутренних помех, что сказывается на помехоустойчивости данных систем.

Возможность применения методов модуляции для обеспечения конфиденциальности передаваемой информации.

Как было отмечено выше классические методы модуляции имеют достаточно много плюсов, но в тоже время имеют существенные минусы.

Поэтому на данном этапе развития технологий в сетях передачи информации, где необходимо обеспечить достаточный уровень скрытности сигнала, а также его помехоустойчивости используются модернизированные методы модуляции стохастических сигналов:

- САР-модуляция;
- алгоритм модуляции 2B1Q;
- алгоритм модуляции TCM;
- OFDM модуляция.

Эти методы позволяют максимально минимизировать описанные в данной работе минусы классических методов, а также реализовать и создать такие условия для противоборствующей стороны, при которых ей будет наиболее трудно и в каком-то смысле невозможно быстро получить информацию, передающуюся в канале радиопередачи (КРУ), а также информацией которой обмениваются роботы при выполнении задач. Также при этом противник не будет иметь возможности сразу же определить к какому роду относится информация, завладеть роботами, и определить наличие группировки роботов из-за высокой структурной скрытности сигналов передающихся между ними.

Таблица 1.

Сравнительная характеристика основных методов модуляции

Название метода	Преимущества	Недостатки
Амплитудная манипуляция (АМСС)	- возможность изменения характеристик стохастического сигнала - простота и дешевизна реализации	- низкая структурная скрытность - высокий уровень перекрестных помех
Частотная манипуляция (ЧМСС)	- возможность изменения характеристик стохастического сигнала - простота реализации в системах связи - высокая помехоустойчивость - высокая скорость передачи данных относительно других методов	- низкая структурная скрытность - высокая мощность излучения
Система Ланге-Мюллера (СЛМ)	- Высокая структурная скрытность - возможность использования в сетях широкополосной связи	- высокий уровень внутренних помех - дороговизна производства приемо-передающих устройств

Название метода	Преимущества	Недостатки
		- необходима высокая производительность вычисляющих устройств
Упрощенная система Ланге-Мюллера (УСЛМ)	-Высокая структурная скрытность - возможность использования в сетях широкополосной связи	- высокий уровень внутренних помех - дороговизна производства приемо-передающих устройств
Автокорреляционная система с противоположными сигналами	-Высокая структурная скрытность - низкая избыточность сигнала - большая дальность связи	- высокий уровень внутренних помех - сложность реализации приемо-передающих устройств
Фазовая манипуляция (ФМСС)	- низкий уровень внутренних помех - высокая структурная скрытность сигнала - высокая помехоустойчивость	- сложность реализации приемо-передающих устройств

Выявлено, что предпочтительной всего использовать систему с ФМСС (фазовой манипуляцией) для обеспечения конфиденциальности информации. Однако преимуществом ФМСС является относительная простота реализации передатчика и приемника, а также указанный метод обладает высокой скоростью передачи данных, что более предпочтительно в условиях быстроменяющейся обстановки.

Таким образом, в работе рассмотрены основные классические методы модуляции стохастических (шумоподобных) сигналов, проведен их анализ, выявлены положительные и отрицательные стороны при применении их в системах связи группы роботов. Исходя из результатов, можно сделать вывод, что использование и применение стохастических сигналов в современных системах связи является перспективным путем развития защиты конфиденциальной информации в таких системах, а также являются относительно недорогим решением.

Литература

1. Горюнов А.Г., Ливенцов С.Н., Чурсин Ю.А. Телеконтроль и телеуправление: учебное пособие. Томск: Изд-во Томского политехнического университета, 2011. 139 с.

2. Иванов М.Т., Сергиенко А.Б., Ушаков В. Н. Радиотехнические цепи и сигналы: Учебник для вузов. Стандарт третьего поколения / под ред. В.Н. Ушакова. Спб.: Питер, 2014. 336 с.

3. Жук А.П., Осипов Д.Л., Гавришев А.А., Бурмистров В.А. Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // Научные технологии в космических исследованиях Земли. 2016. Т. 8. № 2. С. 38–42.

Сведения об авторах

Кошелев Дмитрий Александрович, старший преподаватель кафедры Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Ромашов Арсений Александрович, слушатель Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Корза Евгений Александрович, слушатель Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко.

Кубасов Игорь Анатольевич

ПЕРСПЕКТИВЫ РАЗВИТИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМ ОБЕСПЕЧЕНИИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Современные математические методы превратились в неизменный атрибут эффективного информационно-аналитического обеспечения деятельности органов внутренних дел. Эти методы представляют собой мощный научно-методический инструмент для качественного решения сложных оперативно-служебных задач, начиная от профилактики, раскрытия, расследования преступлений и до оказания социальной, правовой помощи населению [1, 2, 3].

Одним наиболее важным преимуществом применения математических методов, как инструментария информационно-аналитического обеспечения деятельности органов внутренних дел, является возможность с их помощью оперативно и полно извлекать значимую информацию из больших наборов данных различных источников. Ведь органы внутренних дел в своей деятельности постоянно осуществляют сбор и анализ больших данных, да еще и сами генерируют огромное количество информации, включая отчеты о преступности, данные о трафике, отснятый материал наблюдений, посты в социальных сетях и т.п. А применение математических методов позволяет своевременно идентифицировать паттерны, различные тенденции и аномалии, которые в противном случае могли бы остаться незамеченными.

В настоящее время математические методы применяются в информационно-аналитическом обеспечении деятельности органов внутренних дел для решения следующих задач:

1) Сбор, обобщение и оценка информации о качественно-количественных характеристиках преступности и ее причинном комплексе.

Математические методы используются в различных криминалистических дисциплинах, таких как анализ отпечатков пальцев, профилирование ДНК и

баллистика. Например, в методах профилирования ДНК используются сложные статистические алгоритмы для соответствия генетическим образцам, предоставляя убедительные доказательства в уголовных расследованиях. Активно развиваются и методы ДНК-фенотипирования [4]. Другие методы, такие как анализ изображений и распознавание схем, позволяют идентифицировать подозреваемых из кадров с помощью видеонаблюдения, реконструкции сцен преступления.

Математические методы широко используются и в сетевой анализе для картирования преступных сетей и определения ключевых игроков. Сложные отношения между людьми и преступными организациями могут быть нанесены на карту и проанализированы с использованием теории графов, предоставляя ценную информацию о нарушениях.

Само развитие информационных технологий приводит к увеличению объема данных, которые необходимо обрабатывать. Это требует новых подходов к хранению и обработке информации. Особо востребованными становятся методы облачных технологий и Big Data.

2) Всесторонний анализ тенденций развития преступности.

Применение таких математических методов, как регрессионный анализ, прогнозирование временных рядов и пространственная автокорреляция позволяет определить тенденции, потенциальные «горячие» точки преступности и предсказать возможные преступления.

Прогнозное моделирование, основанное на продвинутых статистических алгоритмах и алгоритмах машинного обучения, играет решающую роль в профилактике преступности. Анализируя исторические данные о преступности, социальные показатели и факторы окружающей среды, с помощью моделей можно прогнозировать совершение преступления в конкретных областях и выявлять потенциальных преступников [5].

3) Аналитический поиск реальных и потенциальных угроз внутренней безопасности государства, характерных признаков преступлений и

правонарушений в сфере компетенции органов внутренних дел, наиболее распространенных схем и способов их совершения.

Математические методы позволяют выполнить количественную оценку факторов риска и прогноз потенциальных угроз, оценить вероятности возникновения конкретных преступлений, потенциальные уязвимости безопасности и обосновать необходимость реализации соответствующих мероприятий [6].

4) Комплексная оценка организационно-управленческой и оперативно-служебной деятельности органов внутренних дел, определение приоритетных направлений [7, 8].

Методы математической оптимизации также необходимы для осуществления оптимального распределения имеющихся ресурсов. Анализируя исторические данные и оперативные ограничения, применяя эти методы можно назначить оптимальное развертывание персонала, транспортных средств и других ресурсов для максимизации эффективности оперативно-служебной деятельности. Например, методы линейного программирования позволяют решать задачи оптимизации патрульных маршрутов и распределения ресурсов на основе моделей преступности и доступных ресурсов.

Разработка моделей и деловых игр для обучения и отработки навыков сотрудников в различных условиях оперативно-служебной деятельности, анализ и интерпретация данных в образовательном процессе и т.д. – все это возможно на основе применения математических методов.

5) Разработка мер реагирования на негативные изменения оперативной обстановки и эффективных алгоритмов управления органами внутренних дел.

Математические методы принятия управленческих решений весьма многочисленны и разнообразны. Это следующие методы: теории игр, теории массового обслуживания, управления запасами, модели линейного программирования, балансовый метод, платежная матрица, дерево решений, прогнозирования (экстраполяции) и др. [5, 9].

Как показывает выше приведенный анализ, современные математические методы эволюционно преобразуют деятельность органов внутренних дел, существенно повышая уровень информационно-аналитического обеспечения. При этом в перспективе роль математических методов в их деятельности станет еще более важной, поскольку объем данных, доступных для органов внутренних дел, продолжает только расти.

В целом, перспективными математическими методами в информационно-аналитическом обеспечении деятельности органов внутренних дел являются те методы, которые будут способствовать развитию следующих технологий, указанных в Концепции технологического развития на период до 2030 года:

- искусственный интеллект, включая технологии машинного обучения и когнитивные технологии;
- технологии хранения и анализа больших данных;
- технологии распределенных реестров;
- нейротехнологии, технологии виртуальной и дополненной реальностей;
- квантовые вычисления;
- квантовые коммуникации;
- новое промышленное и общесистемное программное обеспечение;
- геоданные и геоинформационные технологии;
- технологии доверенного взаимодействия;
- современные и перспективные сети мобильной связи.

Интеграция искусственного интеллекта с математическими методами еще больше повысит прогнозирующие возможности, автоматизирует рутинные задачи и поможет в принятии решений в реальном времени [10]. Математические модели будут и далее играть решающую роль в обнаружении и предотвращении киберпреступности, анализе сложных цифровых следов и выявлении нарушителей. Обмен данными и передовые практики в различных

правоохранительных органах обеспечат более комплексный анализ и будут способствовать более упреждающему подходу к предотвращению преступности.

Следовательно, развитие математических методов в информационно-аналитической деятельности органов внутренних дел имеет большой потенциал для успешной цифровой трансформации МВД России. Применение математических методов позволит существенно повысить уровень информационно-аналитического обеспечения оперативно-служебной деятельности органов внутренних дел и, соответственно, повысить эффективность самой деятельности.

Литература

1. Пьянков, О.В. Методология моделирования информационно-аналитических систем органов внутренних дел / О.В. Пьянков // Вестник Воронежского института МВД России. – 2018. – № 2. – С. 76-84. – EDN XRLXIL.

2. Терентьев, А.А. Математическая модель аналитической деятельности ситуационных центров органов внутренних дел / А.А. Терентьев // Вестник Воронежского института ФСИН России. – 2020. – № 3. – С. 91-97. – EDN IEMZIU.

3. Кубасов, И.А. Математические методы исследования социальных систем как основной инструментарий информационно-аналитического обеспечения деятельности органов внутренних дел / И.А. Кубасов // Математические методы и информационно-технические средства: Материалы XIX Международной научно-практической конференции, Краснодар, 22 июня 2023 года. – Краснодар: Краснодарский Университет МВД России, 2023. – С. 145-150. – EDN GFRFVY.

4. Кубасов, И.А. Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений / И.А. Кубасов // Вестник Воронежского института МВД России. – 2022. – № 2. – С. 166-172. – EDN GTSQNB.

5. Кубасов, И.А. Порядок выбора и применения математических методов решения задач управления в организационных системах / И.А. Кубасов, В.Ф. Гапоненко, И.В. Гурлев // Вестник Воронежского института МВД России. – 2023. – № 3. – С. 70-79. – EDN BGGQXT.

6. Северцев, Н.А. Исследование рисков в деятельности человека / Н.А. Северцев, И.А. Кубасов, О.А. Бобр // Труды международного симпозиума «Надежность и качество». – 2006. – Т. 2. – С. 172-175. – EDN NDWQQJ.

7. Гонов, Ш.Х. Актуальные вопросы анализа данных, характеризующих результаты деятельности органов внутренних дел / Ш.Х. Гонов, И.В. Горошко. – Академия управления МВД России: Академия управления МВД России, 2022. – 128 с. – ISBN 978-5-907530-05-8.

8. Меньших, В.В. Описание математических методов оценки показателей работы органов внутренних дел / В.В. Меньших, В.О. Морозова // Охрана, безопасность, связь. – 2021. – № 6-2. – С. 94-99. – EDN AXBTVB.

9. Баторов Б.О., Кубасов И.А., Торопов Б.А. Управление в социальных и экономических системах: курс лекций. – Москва: Академия управления МВД России, 2022. – 116 с.

10. Иванов, А.И. Тестирование больших нейронных сетей на малых выборках / А.И. Иванов, И.А. Кубасов, А.М. Самокутяев // Надежность и качество сложных систем. – 2020. – № 3(31). – С. 72-79. – DOI 10.21685/2307-4205-2020-3-9. – EDN SVWQKV.

Сведения об авторе

Кубасов Игорь Анатольевич, доктор технических наук, доцент, профессор кафедры информационных технологий Академии управления МВД России.

**Кулиш Ольга Александровна,
Джураев Эдуард Сергеевич**

МЕТОДИКА КРИПТОАНАЛИЗА ТЕКСТА, ЗАШИФРОВАННОГО ШИФРОМ ПРОСТОЙ ПЕРЕСТАНОВКИ

Криптоанализ имеет долгую историю, восходящую к древним цивилизациям, где коды и шифры использовались для военной и дипломатической связи. Сегодня криптоанализ является важным аспектом современной криптографии и играет важную роль в области кибербезопасности. Есть два основных подхода к криптоанализу: взлом кода, предполагающий анализ структуры и закономерностей кода для определения исходного сообщения; взлом шифра – анализ процессов шифрования и дешифрования для определения ключа, использованного для шифрования сообщения [1].

Криптоаналитики используют различные методы и инструменты для взлома кодов и шифров, включая статистический анализ, атаки методом перебора [2] и математические алгоритмы. Криптоанализ постоянно развивается, поскольку разрабатываются новые алгоритмы и технологии шифрования. Сейчас криптоанализ имеет столько же разновидностей, сколько разновидностей имеют и сами шифры.

Цель статьи – рассмотреть методику криптоанализа текста, зашифрованного шифром простой перестановки, с помощью Excel.

История криптоанализа начинается с ручных методов разгадывания шифров, когда для дешифровки использовались бумага и перо. Со временем, по мере усложнения шифров, методы криптоанализа стали более сложными и технологичными. Сегодня криптоанализ невозможен без использования мощных компьютеров и сложных алгоритмов.

Первыми криптоанализу стали подвергаться классические шифры. Чтобы понять принцип работы криптоанализа рассмотрим такой шифр, как табличная перестановка.

Пример 1: Шифртекст «ч яууик рпнотаа илзслн уя».

Известно только то, что криптограмма была получена шифром простой перестановки. Какой ключ был выбран не известно. Однако можно заметить, что символов в шифртексте 25, а это значит, что вероятнее всего была выбрана таблица размером 5×5 . Можно расчертить такую таблицу и внести недостающие данные (таблица 1) [3]. Пробелы будут обозначаться знаком «_».

Таблица 1. Шифртекст в таблице 5×5

1	2	3	4	5
ч	_	я	у	у
и	к	_	р	п
н	о	т	а	а
_	и	л	з	с
л	н	_	у	я

Кроме метода грубого перебора, для упрощения задачи можно использовать таблицу оценок – численные оценки возможности взаимного следования столбцов шифрующей таблицы [4]. Будем считать, что она известна (таблица 2).

Таблица 2. Таблица оценок шифртекста

		Следующий столбец				
Предыдущий столбец		1	2	3	4	5
	1	-	1971	8272	1360	15047
	2	1492	-	346	2993	1745
	3	111	5105	-	1454	0
	4	4001	1944	26	-	4
	5	813	3194	26	4	-

Для рассматриваемого примера может быть следующий вариант порядка следования столбцов: 2 - 4, 1 - 5, 3 - 2, 4 - 1, 5 - 2. Можно заметить, что 2 столбец может следовать в двух случаях 5 - 2 и 3 - 2. Возьмём наиболее вероятное значение. Тогда получается следующая последовательность: 3 - 2, 2 - 4, 4 - 1, 1 - 5. После нахождения последовательности заполняем таблицу новыми значениями (таблица 3).

Таблица 3. Попытка нахождения исходного текста

3	2	4	1	5
я	—	у	ч	у
—	к	р	и	п
т	о	а	н	а
л	и	з	—	с
—	н	у	л	я

Попытка оказалась удачной. Исходный текст: «Я учу криптоанализ с нуля».

Кроме таблицы оценок, задачу нахождения исходного текста может упростить программная реализация таблиц шифртекста и нахождения исходного текста [5].

Для этого в среде MS Excel нужно создать книгу «Криптоанализ».

На листе книги MS Excel выделим таблицу, размером 5×5 для записи криптограммы, пронумеруем её столбцы и строки. Ниже нужно выделить ещё одну таблицу такого же размера, пронумеровать её столбцы и строки (рисунок 1). В ячейку второй таблицы занести функцию ИНДЕКС, которая будет заполнять значениями вторую таблицу, осуществляя поиск соответствующего символа в первой таблице согласно номеру строки и столбца.

Функция ИНДЕКС имеет следующую структуру:

ИНДЕКС(массив; номер_строки; [номер_столбца])

В качестве значения первого параметра функции (*массив*) нужно назначить ссылку на таблицу с текстом криптограммы, сделать ссылку абсолютной (\$_\$_:\$_\$_);

в качестве значения второго параметра функции (*номер_строки*) необходимо указать адрес ячейки с текущим номером строки второй таблицы, зафиксировать указатель столбца (\$_ _);

в качестве значения третьего параметра функции (*номер_столбца*) нужно указать адрес ячейки с текущим номером столбца второй таблицы, зафиксировать указатель строки (_\$_), примерный результат выполнения:

=ИНДЕКС(\$C\$4:\$G\$8;\$B13;C\$12) (рис. 2), скопировать созданную формулу на весь диапазон ячеек второй таблицы.

Теперь появится возможность переставлять столбцы второй таблицы, просто изменяя их номера.

Занесем побуквенно криптограмму в строки первой таблицы. Текст криптограммы без изменений должен отобразиться во второй таблице.

После этого нужно проанализировать таблицу оценок и высказать гипотезы об истинном порядке следования столбцов шифрующей таблицы. Критерием верности гипотезы о порядке следования столбцов шифрующей таблицы является получение осмысленного текста. Далее необходимо производить все действия в той же последовательности, как и при ручном способе дешифрования, просто меняя номера таблиц, согласно выдвинутых гипотез.

	A	B	C	D	E	F	G	H	I
1			Криптограмма						
2			номера столбцов						
3			1	2	3	4	5		
4	номера строк	1							
5		2							
6		3							
7		4							
8		5							
9									
10									
11			Перестановка столбцов - новый порядок						
12			4	1	5	3	2		
13		1							
14		2							
15		3							
16		4							
17		5							
18									
19									

Рис. 1. Пример внешнего вида таблиц

	A	B	C	D	E	F	G	H
1			Криптограмма					
2			номера столбцов					
3				1	2	3	4	5
4	номера строк	1						
5		2						
6		3						
7		4						
8		5						
9								
10								
11			Перестановка столбцов - новый порядок					
12				1	2	3	4	5
13		1	=ИНДЕКС(\$C\$4:\$G\$8;\$B13;\$C\$12)					
14		2						
15		3						
16		4						
17		5						
18								
19								

Рис. 2. Пример заполнения второй таблицы

Шифры могут усложняться, а значит и способы криптоанализа также должны совершенствоваться. Например, шифр простой перестановки может усложниться двойной перестановкой: первой перестановкой столбцов, и второй – строк. И если перестановку столбцов можно обнаружить через таблицы оценок, то нужную перестановку строк придётся искать вручную. Однако и в этом случае задачу также может облегчить программная реализация.

Таким образом, с помощью средств среды Excel возможно осуществлять криптоанализ классических шифров. В статье рассмотрена методика криптоанализа текста, полученного шифром простой перестановки. Приведен пример криптоанализа с помощью функций среды Excel, который может быть использован в ходе проведения лабораторных работ по дисциплине «Математические основы криптографической защиты информации».

Литература

1. Бабаш, А.В. История криптографии. Учебное пособие. / А.В. Бабаш, Г.П. Шанкин. – Текст: непосредственный – М.: «Гелиос АРВ», 2001. – 240 с.
2. Бескид, П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии. Учебное пособие. / П.П. Бескид, Т.М. Татарникова. – Текст: непосредственный – СПб.: изд. РГГМУ, 2010. – 95 с.

3. Столингс, В. Криптография и защита сетей. Принципы и практика. 2-е изд. / В. Столингс. – Текст: непосредственный – М.: Вильямс, 2001. – 672 с.

4. Алферов, А.П. Основы криптографии. Учеб. пособие. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Текст: непосредственный – М.: Гелиос-АРВ, 2002. – 480 с.

5. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Текст: непосредственный – Москва: Издательство Юрайт, 2024. – 349 с.

Сведения об авторах

Кулиш Ольга Александровна, кандидат физико-математических наук, доцент кафедры математики (и математических основ криптографической защиты информации) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознамённого училища имени генерала армии С.М. Штеменко.

Джураев Эдуард Сергеевич, курсант Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознамённого училища имени генерала армии С.М. Штеменко.

**Лаптев Сергей Владимирович,
Лаптев Владимир Николаевич**

О ГЛАВНОМ КРИТЕРИИ ОЦЕНКИ ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРОФЕССИОНАЛОВ

Рассмотрим обобщенную схему процесса гармоничного стоп-кадрового взаимодействия открытой системы (ОС) с изменяющейся внешней средой (ВС), в течении одинаковых временных интервалов $\Delta t_n = \text{const}$, который позволяет правильно трактовать термин информатика. Этот термин, представляет собой симбиоз двух терминов информация и автоматика. Первый трактуется нами как однозначное уникальное модельное описание конкретного объекта или процесса [6-8], а второй общепринятый, как отрасль науки и техники, которая разрабатывает технические средства (ТС) и методы для реализации конкретных технологических процессов (ТП) без участия человека [4].

Общепринятая трактовка термина информации как сообщение или сигнал, совокупность данных, сведения, рассматриваемые в контексте их содержания, структурной организации, динамики (процессов создания, передачи, восприятия, использования, анализа, хранения и т.п.) нас не устраивает [6], ибо в ней отсутствует главная характеристика модели объекта или процесса – их однозначное уникальное качество. Конкретным уникальным качеством обладают конкретные стоп-кадровые математические модели, которые представляются в алфавитно-цифровом коде, позволяющем людям и автоматическим устройствам компьютерами и цифровыми средствами связи однозначно понимать. Чтобы хитро скрыть (или наоборот выявить) истинное уникальное содержание любого информационного сообщения используется наука криптография. В дальнейшем информация трактуется нами с позиций ее правильного понимания и применения в процессе выживания любой ОС в постоянно изменяющейся ВС [6-9].

Функционирование и развитие ОС, базируется на успешном использовании созданных ею «типовых» $Y_k(x_n)$ «улучшенных» $Y_{opt_m}(x_n)$ и «новых» $Y_{new_m}(x_n)$ математических моделях, обеспечивающих выживание ОС за

счет создания мозгом человека типичных ($+R_m$), оптимальных ($+R_m^{opt}$) и новых ($+R_m^{new}$) «эффектов системы», обеспечивающих, как правило, выживание ОС в новых для нее условиях.

При этом информация о таких полезных для развития ОС случаях передается в управляющий центр организма человека – его мозг [1,7]. Здесь возможны 2 варианта взаимодействия $BC_k \leftrightarrow OC_m$: 1) совпадение $Y_k(x_n) = Y_m(x_n)$ или 2) не совпадение $Y_k(x_n) \neq Y_m(x_n)$, указанных выше моделей с допустимой при этом погрешностью ε . В первом случае в работу автоматически запускается модель $Y_m(x_n)$, которая обеспечивает выживание ОС в типичной для ОС ситуации. Иначе ОС осуществляет ускоренный поиск улучшенной (т.е. оптимальной) $Y_m^{opt}(x_n)$ или принципиально новой $Y_m^{new}(x_n)$ дискретной математической модели, которая обеспечивает ее выживание в неординарной для нее стоп-кадровой ситуации.

Как правило, при этом используется разложение некоторой непрерывной функции $Y(x)$ в ряд на единичном отрезке $[0,1]$, с использованием других ее частных конкретных значений, где улучшенное или новое качество конкретной непрерывной математической функции $Y(x)$ с помощью суммирования M уточненных $Y_m^{opt}(x_n)$ или новых $Y_m^{new}(x_n)$ дискретных их значений на единичном отрезке $[0,1]$. Таким образом ОС устанавливаются улучшенные (оптимальные) и принципиально новые представления функций $Y_k(x_n)$, $Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$, реально повышающие выживаемость ОС. Иначе, как правило ОС, погибает [4]. В такой описанной критической для ОС ситуации организация или конкретный человек, обращается к специалистам по естественному (человеческому) и искусственному (компьютерному) интеллекту, чтобы с их помощью успешно разрешить эти коллизии [10].

Под естественным интеллектом (ЕИ) понимаются познавательные способности человека, думать, рассуждать и учиться, которые на базе психических процессов и функций восприятия, внимания, памяти, позволяют ему успешно решать, стоящие перед ним задачи и проблемы. Искусственный интеллект (ИИ) – это комплекс технологических решений, позволяющий

имитировать познавательные функции человека и получать при этом решения конкретных управленческих задач результаты, сопоставимые (как минимум), с результатами интеллектуальной деятельностью человека [10]. Перспективные методы ИИ направлены на создание принципиально новой научно-технической продукции, а также на разработку универсального (сильного) ИИ. С помощью ЕИ и бурно развивающихся, на базе модели коллектива вычислителей, новых возможности ИИ (за счет его развития, нацеливается на создание интеллектуальных компьютерных систем, способных автоматически (машинально), без вмешательства человека решать типовые задачи. При этом необходимо обязательно учитывать, что ИИ:

- создан людьми, в то время как ЕИ является продуктом эволюции природы;
- предназначен для решения конкретных задач и выполнения конкретных функций, в то время как ЕИ более гибкий и адаптируемый;
- учится на основе анализа данных и выявленных закономерностей, в то время как ЕИ учится на опыте своего взаимодействия с окружающей ее его внешней средой;
- позволяет программировать определенных творческие способности ЕИ, который гораздо более креативен и инновационен, чем ИИ.

Таким образом, с помощью комплексного использования непрерывной и дискретной математики человек и компьютер однозначно (при допустимой на практике погрешности ε) могут на отрезке $[0,1]$ быстро преобразовывать конкретное значение непрерывной функции $Y(x)$ в «штaketник», описываемый формулой (1), площадь которой легко вычисляется и используется в процессе сличения дискретной функций $Y_k(x_n)$ с функциями $Y_m^{opt}(x_n)$, $Y_m^{new}(x_n)$ и $Y_m^{new}(x_n)$. Здесь также необходимо отметить теорему Колмогорова [3] закон резонанса [11], открытый Н. Тесла. Теорема Колмогорова утверждает, что любая непрерывная функция $Y(x_1, x_2, \dots, x_N)$ может быть представлена в виде суперпозиций непрерывных функций одной и двух переменных. С ее помощью человек можно

посчитать площадь «штакетника», состоящего $2N+1$ «штакетин», имеющих одинаковые основанием Δx_m , но разные высоты $h_m(x_n)$ (смотри формулу 2).

$$Y(x_1, x_2, \dots, x_N) = \sum_{n=1}^{2N+1} \left(g_n \sum_{m=1}^N (h_{mn}(x_m)) \right) = \sum_{n=1}^{2N+1} \left(\log_2 \sum_{m=1}^N (h_{mn}(x_m)) \right), \quad (2)$$

где $x = (x_1, \dots, x_N)$, $0 \leq x_n \leq 1$.

Эта формула, с помощью компьютерной программы быстрого преобразования Фурье (БПФ) позволяет человек (или автомату) быстро /в реальном масштабе времени - РМВ/ посчитать собственные частоты $\omega_1, \omega_2, \dots, \omega_N$ всех N столбиков $h_{mn}(x_n)$, а затем используя закон резонанса по формуле $y=2^q$ (где q это синхронно работающие функциональные, т.е. исполнительные элементы ОС) создавать нужный человеку «эффект системы», уравнивающий в текущем временном интервале Δt_n воздействие ВС, обеспечивая тем самым реальное выживание ОС (себя или предприятия).

Кратко опишем суть закон резонанса. Резонанс (от французского *resono* - откликаюсь) – это частотно-избирательный отклик колебательной ОС на частотное внешнее воздействие внешнее воздействие ВС ω_N , проявляющееся в резком увеличении амплитуды ее стационарных колебаний при совпадении частоты внешнего воздействия $\omega_{вс}$, с определённым значением $\omega_{ос}$, т.е. при $\omega_{вс}=\omega_{ос}$, характерным для данной ОС.

Под действием резонанса ОС, как колебательная система оказывается, максимально отзывчивой на такие воздействия ВС. Практика доказала, что закона резонанса позволяет выделить и/или усилить даже весьма слабые периодические колебания, присущие ОС. Впервые явление резонанса было описано Галилео Галилеем в его работах по исследованию маятников и музыкальных струн, а гениальный Никола Тесла установил, что все связи между явлениями в природе (в т.ч. и между ОС и ВС) устанавливаются исключительно путем разного рода простых и сложных резонансов – согласованных вибраций, когда $\omega_{вс}=\omega_{ос}$. Таким образом закон резонанса обеспечивает: 1) обязательный отклик ОС на частотные воздействия ВС и 2) резко увеличивает «эффект системы» при совместной

(синхронной) работе q функциональных элементов ($\Phi\mathcal{E}_q$) ОС со спектром частот $\omega_1, \omega_2, \dots, \omega_q$.

Еще раз отметим, что используемый нами механизм адаптивного управления ОС (МАУ ОС) использует закон резонанса и степенную функцию $y=2^q$, описывающий «эффект системы», который обеспечивает ее выживание (за счет уравнивания различных импульсных воздействий ВС на ОС) в течение временного интервала $\Delta t_n = \text{const}$. Незначительные уменьшения Δt_n имеют место в течение весьма длительного временного интервала и поэтому это обстоятельство нами не учитывается. Закон резонанса используется нами как закон частотно-избирательного отклика ОС на различные воздействия извне (от ВС). Он уравнивает их за счет коллективной синхронной работы q функциональных элементов ($\Phi\mathcal{E}_q$), обладающих собственными колебательными частотами $\omega_1, \omega_2, \dots, \omega_q$. Если в текущем временном интервале длительностью Δt_n , часть этих частот $\omega_1, \omega_2, \dots, \omega_q$ совпадает с частотами $\omega_1, \omega_2, \dots, \omega_m$, внешнего воздействия, то ОС автоматически откликается на эту ситуацию созданием должного векторного «эффекта системы» ОС_m , уравнивающего текущее векторное воздействие извне (ВС_k) по закону резонанса $y=2^q$ в течение единого (для всех стоп-кадров) временного интервала Δt_n .

В нашей точки зрения все Δt_n -известные человеку способы решения задач и проблем, описывается процессом, содержащий 4 основных этапа: 1) четкое понимание сути задачи и проблемы как вопроса имеющего или не имеющего решения; 2) поиск типичных $Y_m(x_n)$, оптимальных $Y_m^{\text{opt}}(x_n)$ или новых $Y_m^{\text{new}}(x_n)$ дискретных функций с помощью матрицы типовых знаний (МТЗ), где каждая из M строк, обладает требуемыми для ОС «эффектами системы», обеспечивающими ее выживание в а) типичной, б) оптимальной и в) проблемной ситуациях; 3) отладка механизма автоматической работы одной или нескольких моделей $Y_m(x_n)$, $Y_m^{\text{opt}}(x_n)$ и $Y_m^{\text{new}}(x_n)$, обеспечивает автоматическую (машинальную) работу ОС на базе указанных математических моделей; 4) успешное применение улучшенной $Y_m^{\text{opt}}(x_n)$ или принципиально новой модели $Y_m^{\text{new}}(x_n)$ обеспечивает выживание ОС за счет улучшения типовой модели $Y_m(x_n)$,

а применение модели $Y_m^{new}(x_n)$ решает проблему, которую до этого никто пока не смог решить.

На рисунке 1 представлен эффект резонанса, позволяющая человеку успешно решать задачи и проблемы. Задача – это вопрос, имеющий одно или несколько решений (ответов), которые необходимы умело применять, а проблема – это вопрос, ответ на который никто пока не знает. Известно, что успешное функционирование и развитие ОС в изменяющейся ВС обеспечивается уравниванием любых внешних векторных воздействий на нее извне F_k адекватными им противодействиями R_m со стороны ОС. В типичных ситуациях $F_k=R_m$, в оптимизируемых $F_k^{opt} \approx R_m$, а в проблемных $F_k \neq R_m$.

Следовательно, любой сотрудник предприятия, правильно понимающий суть закона резонанса, может самостоятельно и успешно совершенствовать свои профессиональные навыки, которые и делают его прекрасным работником профессионалом.

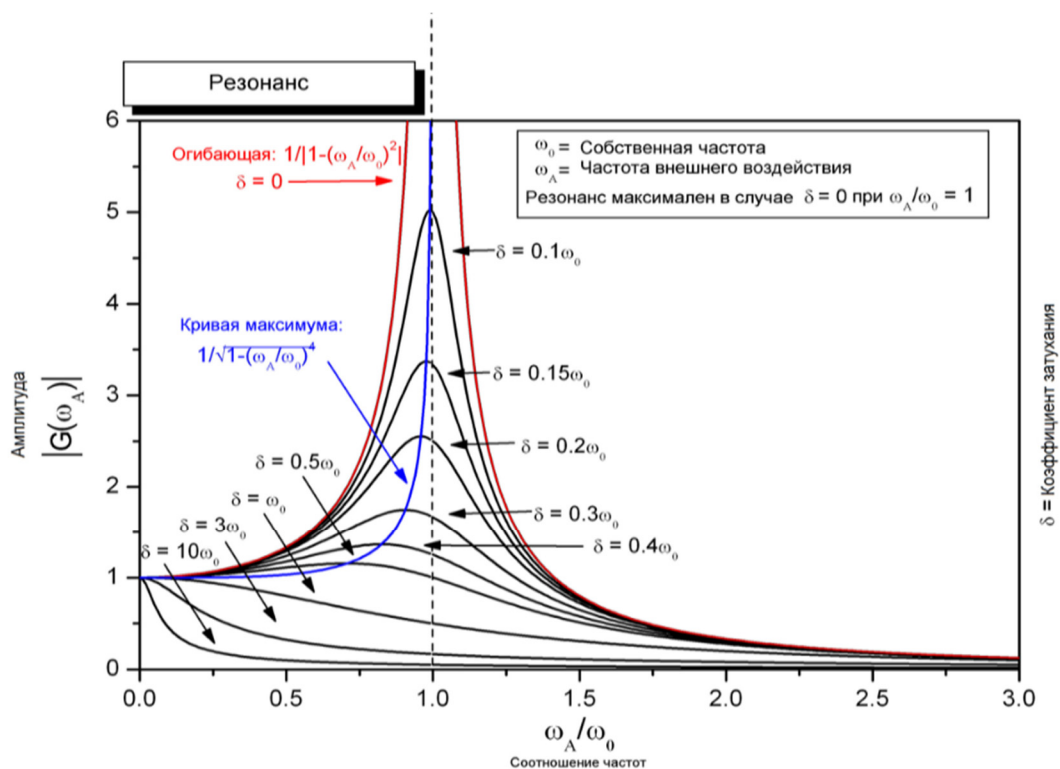


Рис. 1. Эффект резонанса для разных соотношений частот ω_A/ω_0 и коэффициента затухания δ

На рисунке 1 видно, что при $\omega_A/\omega_0=1$, когда коэффициенте затухания $\delta=0$ достигается максимальный «эффект системы». Эта закономерность присуща

всем ОС. Поэтому, только постоянное повышение «эффекта системы», т.е. производительности своего труда, путем уменьшения Δt , позволяет творческому человеку реально совершенствовать свою профессиональную деятельность. Именно неуклонное повышение производительности своего труда является самым главным критерием успешной творческой деятельности профессионала.

Как правило проблема кардинального улучшения производительности своего труда формулируется в понятном для человека виде: «знаю, что надо, но не знаю, как это сделать» в течение одного и того же единого (для всех стоп-кадров) временного интервала Δt_n . Здесь необходимо особо отметим, что в начале шестидесятых годов прошлого столетия советский ученый Евреинов Э.В. разработал и успешно реализовал модель коллектива вычислителей, являющуюся теоретической основой высоко производительной компьютерной системы Internet a (таблица 1).

Таблица 1. Сравнение моделей вычислителя и коллектива вычислителей

Модель вычислителя	Модель коллектива вычислителей
Последовательное выполнение операций; Фиксированная логическая структура вычислений. Конструктивная неоднородность элементов и их связей Имеет ограничение по росту производительности ВТ.	Параллельное выполнение операций; Переменная логическая структура вычислений. Конструктивная однородность элементов и их связей Не имеет ограничений по росту производительности ВТ.

В таблицы 1 четко видно, что модель коллектива вычислителей (сети Internet) не имеет ограничений по произвольности вычислений. Здесь необходимо указать на наличие гармонической взаимосвязи теоремы Колмогорова с однозначной идентификацией количества информации и ее органичной связи с вычислением, с помощью БПФ уникальных, собственных частот $\omega_1, \omega_2, \dots, \omega_m$ каждого из этих M столбиков формулы (1). При разложении этих функций в соответствующие тригонометрические ряды (синусоиды) с помощью с помощью компьютерной программы – Быстрого Преобразования Фурье (БПФ) [13], которая с помощью «столбиков» высотой $h_{mn}(x_n)$ легко и быстро вычисляет их собственные резонансные частоты $\omega_1, \omega_2, \dots, \omega_q$, которые

позволяет обеспечить создание, в течение текущего временного интервала длительностью Δt_n , требуемый для выживания ОС «эффекты системы», обеспечивающий, с помощью закона резонанса, выживание ОС. Площади, описывающие суммарные значения «штaketников» – $Y_m(x_n)$, $Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$ уникальны, что позволяет, с допустимой на практике погрешностью ε , однозначно идентифицировать сходство математических моделей с текущей моделью $Y_k(x_n)$ с одной из математических моделей $Y_m(x_n)$, $Y_k^{opt}(x_n)$ и $Y_k^{new}(x_n)$, обеспечить вычисления спектров резонансных частот $\omega_1, \omega_2, \dots, \omega_q$, с помощью синхронной работы исполнительных ФЭ_q создание требуемого «эффекта системы».

Рисунок 2 представляет концептуальную алгоритмическую модель работы МАУ ОС, МТЗ– это матрица типовых знаний.

Исходя их установки великого русского математика Чебышева П.Л., «Теория без практики мертва и бесплодна, а практика без теории бесплодна и пагубна», мы считаем, что новизна и результативность взаимодействия двух противоположностей естественного и искусственного интеллектов (ЕИ и ИИ) обязательно должна базироваться

- 1) на стоп-кадровом описании взаимодействия открытых систем (ОС) с изменяющейся внешней средой (ОС) и
- 2) безусловном выполнении 3 основных законов диалектики природы:
 - а) единства и борьбы противоположностей (ОС и ВС),
 - б) перехода количества в качество и обратно и
 - в) отрицания.

математических символов, наделяющих образы (математические модели) реальных объектов и действий с ними уникальными конкретными качества. А это существенно снижает эффективность работы людей и средств автоматизации, их творческой деятельности. Хотя все прекрасно знают, что для сокрытия сути любого информационного сообщения весьма успешно используется наука криптография.

Эти примеры убедительно подтверждают, что творческое использование человеком ЗУН-ов в процессе их практической отработки и применения в своей профессиональной деятельности является самым и надежным инструментом обеспечения эффективной деятельности отдельного специалиста и коллектива из них. Следовательно, постоянная отработка, поддержание и совершенствование своих индивидуальных профессиональных навыков является главным атрибутом практической деятельности профессионала. Их реализация является главной задачей профессионала в течение всей его жизни (начиная с детского сада). Ибо только постоянное совершенствование своих профессиональных навыков всегда обеспечит такому специалисту достойную заработную плату.

На рисунке 2 представлены реальные связи знаний–умений–навыки, реально способствующие ускоренному развитию творческих способностей профессионала. То есть человека, который с помощью МАУ ОС, быстро выявляет и грамотно использует новые эффективные способы и методов решение типовых задач, обеспечивает, по возможности, их оптимизацию. В конечном итоге, ускоренному поиску неординарных новых способов и методов решения реальных (а не надуманных) проблем, опираясь при этом на комплексное использование новейших достижений в области естественного и искусственного интеллектов (ЕИ и ИИ). Попутно заметим, что специалистов готовят различные учебные заведения, а вот профессионалами их выпускники становятся самостоятельно, путем постоянного самосовершенствования себя.

Литература

1. Анохин П.К. Избранные труды. Принципиальные вопросы общей теории функциональной системы / П.К. Анохин. – М.: Наука, 1978. – 400 с.
2. Грэхмен Р. Конкретная математика: Основания информатики / Р. Грэхмен, Д. Кнут, О. Паташник. – М.: Мир, 2006. – 703 с.
3. Евреинов Э. В. Однородные вычислительные системы, структуры и среды / Э. В. Евреинов. – М.: Радио и связь, 1981. – 208 с.
4. Информационная безопасность: учеб. пособие / В.И. Лойко, В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с.
5. 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.
6. Лаптев В.Н. Исследование путей совершенствования управленческой деятельности дежурных частей органов внутренних дел на основе использования сети мини-ЭВМ. Дисс. канд.техн.наук. / В.Н. Лаптев. – М.: Академия МВД СССР, 1986. – 254с.
7. Лаптев В.Н. Место и роль информации в обеспечении успешного функционирования и развития открытых систем. // 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. – С.83-88.
8. Лаптев С.В. Нелинейные дисперсионные волны в вязкоупругих тонкостенных конструкциях. Дисс. канд. физ.-мат. наук / С.В. Лаптев. – Саратов: СГУ, 2000. – 132 с.
9. Луценко Е.В. Универсальная автоматизированная система распознавания образов "Эйдос" (версия 4.1). – Краснодар: КЮИ МВД РФ, 1995. – 76с.

10. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ № 490 от 10 октября 2019 г.

11. Сато Ю. Без паники! Цифровая обработка сигналов. / Ю. Сато; пер. с японского Т. Г. Селиной. – М.: Додэка-XXI, 2010. – 176 с.

12. Свидетельство о государственной регистрации программы для ЭВМ № 2008610098. Адаптивная автоматизированная система управления «Эйдос-АСА» (Система "Эйдос-АСА"). Правообладатели: Луценко Евгений Вениаминович (RU) Лаптев Владимир Николаевич (RU). Авторы: Луценко Е.В., Лаптев В.Н. (RU). Заявка № 2007613723. Дата поступления 17.09.2007 г. Зарегистрировано в Реестре программ для ЭВМ 9.01.2008 г. – 50с.

Сведения об авторах

Лаптев Сергей Владимирович, кандидат физико-математических наук, доцент, доцент кафедры компьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина.

Лаптев Владимир Николаевич, кандидат технических наук, доцент, доцент кафедры компьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина.

Левачева Юлия Валерьевна

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

В результате интенсивного развития такой информационной технологии, как искусственный интеллект, а также различного рода цифровых платформ, современное общество стало высоко информатизированным, что не могло сказаться на образовательном процессе для подготовки будущих специалистов.

Основным принципом модернизации высшего образования является интеграция информационных технологий в учебный процесс. Данное направление регулируется различными нормативно-правовыми актами, включая федеральные образовательные стандарты для высшего образования.

Важным этапом для модернизационной реформации системы образования является комплексное внедрение информационных технологий в учебный процесс. Данный процесс регулируется рядом нормативных актов, включая федеральные законы, постановления и федеральные стандарты высшего профессионального образования. В соответствии с Федеральным законом № 273-ФЗ [1], при осуществлении образовательных программ с использованием дистанционных технологий обучения, необходимо создавать условия для использования электронной информационно-образовательной среды, которая включает в себя электронные ресурсы, электронные образовательные материалы и документы.

Законодательством определены данные, которые требуют защиты от незаконного доступа со стороны посторонних лиц. Среди таких информации можно выделить персональные данные, конфиденциальную информацию, официальные, профессиональные и коммерческие секреты. Порядок обеспечения безопасности персональных данных регламентируется нормативно-правовыми документами, такими как Трудовой кодекс, Гражданский кодекс, Закон Российской Федерации «О защите персональных данных», «Об информации».

Согласно Стратегии развития информационного общества в Российской Федерации на период с 2017 по 2030 год, целью и стратегическими приоритетами национального уровня является создание безопасной информационной среды в образовательных организациях. В настоящее время федеральными органами власти ведется реализация плана действий в соответствии с Указом Президента Российской Федерации от 9 мая 2017 года №203. Минкомсвязи России, в своем приказе от 27 февраля 2018 года №88, утвердило план мероприятий по реализации Концепции обеспечения безопасности информации детей на 2018-2020 годы [2].

Обеспечение безопасности информации в современной образовательной среде, согласно действующему законодательству, охватывает защиту данных и сведений, относящихся к следующим трем категориям:

- Личные данные и информация, связанная с обучающимися, преподавателями, административным персоналом учебного заведения, а также цифровые архивные документы;
- Образовательные программы, базы данных, библиотеки и другие структурированные материалы, используемые в процессе обучения;
- Интеллектуальная собственность, защищенная законом [5].

Для обеспечения защиты от действий злоумышленников, предотвращения кражи данных и уничтожения информационных хранилищ целесообразно применять следующие меры безопасности:

1. Использование сильных паролей, двухфакторной аутентификации и ограничение доступа только для авторизованных пользователей – такие меры помогут предотвратить несанкционированный доступ к данным и системам.

2. Регулярное создание резервных копий данных и хранилищ информации позволит восстановить информацию в случае ее потери или повреждения.

3. Регулярное обновление программного обеспечения и операционных систем поможет устранить уязвимости, которые могут быть использованы злоумышленниками.

4. Проведение обучения сотрудников по вопросам информационной безопасности способствует повышению их осведомленности о возможных угрозах и методах их предотвращения.

Один из важных аспектов обеспечения информационной безопасности в учебных заведениях заключается в предотвращении действий киберпреступников. Киберугрозы могут выражаться в попытках взлома систем, краже или повреждении данных, а также нарушении работы сети. Для защиты от таких угроз принимаются разнообразные меры, включая применение передовых антивирусных программ, брандмауэров, систем обнаружения вторжений и шифрования данных.

Обеспечение безопасности информации в учебных учреждениях также включает защиту от типичных угроз, представленных как киберпреступниками, так и обучающимися. Это значимая задача, требующая использования соответствующих методов и политики безопасности.

Технологии обеспечения информационной безопасности учебного заведения включают в себя защиту на пяти уровнях.

1. Нормативно-правовой. Осуществляется разработка и применение законодательных и нормативных актов, регулирующих информационную безопасность образовательной организации.

2. Морально-этический. Происходит формирование этических принципов и правил использования информационных ресурсов. Повышается осведомленность сотрудников и обучающихся о последствиях нарушения данного принципа.

3. Административно-организационный. Осуществляется организация работы по обеспечению информационной безопасности, назначаются ответственные лица, разрабатывается политика безопасности, проводится аудит и обучается персонал.

4. Физический уровень. Защита физического доступа к информационным ресурсам (через контроль доступа к помещениям и оборудованию);

5. Технический уровень. Применение технических средств обеспечения информационной безопасности (антивирусное программное обеспечение брандмауэры, системы обнаружения вторжений и шифрование данных) [4].

Для эффективной работы системы обеспечения информационной безопасности в учебном заведении необходимо наличие специалистов с высоким профессиональным уровнем и опытом. Им поручены такие задачи, как:

- гарантирование сохранности защищаемых данных;
- поддержание информации в постоянно доступном состоянии для авторизованных пользователей;
- обеспечение конфиденциальности сведений, требующих защиты, и предотвращение несанкционированного доступа к ним.

Информационная безопасность образовательного учреждения охватывает широкий спектр мероприятий, направленных на достижение двух основных целей. Первая цель связана с обеспечением защиты персональных данных и информационной среды от несанкционированных вторжений, утечек информации и изменений в системе, производимых сторонними лицами. Вторая цель заключается в обеспечении безопасности студентов путем предотвращения разнообразных форм пропаганды, нежелательной рекламы и распространения запрещенной законом информации.

Для обеспечения безопасного функционирования системы в образовательной организации необходимо проводить аудит информационной безопасности.

Аудит – это процесс оценки уровня безопасности информационно-технической инфраструктуры путем использования определенных показателей информационной безопасности. При проведении аудита анализируются различные аспекты, включая документацию, настройки сетевых устройств, журналы событий, и другие элементы, цель которых зависит от поставленных целей. Оценка позволяет определить уровень защищенности информационной системы от внешних угроз и несанкционированного доступа, а также

устанавливает соответствие уровня информационной безопасности требованиям нормативных актов, стандартов и принятой практики в данной отрасли [3].

Важно отметить, что проведение аудита помогает выявить уязвимости и пробелы в системе безопасности, что позволяет принять меры по их устранению и повышению уровня защиты информации. Аудит информационной безопасности включает в себя проверку соответствия системы безопасности стандартам и требованиям, таким как ISO 27001, PCI DSS и GDPR. Также аудит помогает обнаружить и предотвратить атаки, такие как DDoS-атаки.

Литература

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N273-ФЗ (последняя редакция) // – URL: https://www.consultant.ru/document/cons_doc_LAW_140174 (дата обращения 29.05.2024).

2. Приказ Минкомсвязи России «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы» // - URL: <https://digital.gov.ru/ru/documents/5994/> (дата обращения 03.06.2024)

3. Аверченков В.И. Аудит информационной безопасности//Учебное пособие / 4-е издание. – М.: Флинта, 2016. – С. 270.

4. Волков А. В. Обеспечение ИБ в вузах // Информационная безопасность. – 2006. – № 3, 4 / <http://www.litsec.ru/articles2/bepub/insec-3-2006>.

5. Информационная безопасность в образовательной организации: Блог [Электронный ресурс] // Smart-SoftTeam. – Электрон. дан. – URL: https://www.smart-soft.ru/blog/informatsonnaja_bezopasnost_v_obrazovateljnoj_organizatsii/ (дата обращения: 10.06.2024).

Сведения об авторе

Левачева Юлия Валерьевна, преподаватель кафедры информатики и математики Волгоградской академии МВД России.

Лемайкина Светлана Владимировна

ПРОБЛЕМЫ ДЕАНОНИМИЗАЦИИ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТ В ПРЕСТУПНОЙ СФЕРЕ

Идея использования криптографических преобразований для проведения анонимных платежей возникла и была реализована в виде централизованной системы в 1990 году. В 1998 году компания, предоставляющая подобные услуги обанкротилась. В своем современном виде идея возродилась в 2009 году в виде децентрализованной распределенной системы обращения криптографических валют. Использование онлайн-технологий в сочетании с криптографией привело к созданию совершенно новой системы переводов, в которой безопасный платеж может быть отправлен напрямую, без использования посредника, такого как центральный банк или другой государственный орган [1].

Криптовалюты и инновационная технология блокчейн не могли быть упущены преступниками, которые всегда первыми используют самые современные технологические инструменты для сокрытия доходов от своей незаконной деятельности. С помощью криптовалют сегодня отмываются практически все виды нелегального дохода. Преступники используют анонимность блокчейна, чтобы скрыть источники незаконных средств и конвертировать их в наличные, которые затем могут быть заведены в легальный оборот через банковскую систему. Согласно «Отчету о криптопреступности за 2024 год» от Chainalysis, за 2023 год суммарно через криптовалюту было отмыто более 22 млрд долларов [2].

Однако, согласно исследованиям, использование криптовалют для незаконной деятельности, является лишь небольшой частью общей экономики криптовалют, и эта часть, меньше, чем объем незаконных средств, задействованных в традиционных финансовых операциях. [3] Исследования показывают, что наличные остаются предпочтительным методом отмывания денег номер один, поскольку они полностью анонимны и не оставляют следов.

Но тем не менее не стоит переоценивать объем нелегальных транзакций, совершенных на блокчейне. За несколько кликов преступник могут создать

неограниченное количество цифровых кошельков, состоящих из комбинации цифр и букв. В результате транзакция, записанная в блокчейне, является адресом кошелька, а не именем. Выполнение переводов между кошельками занимает секунды. Это позволяет быстро проводить транзакции и переводить средства в нескольких юрисдикциях в течение очень короткого периода времени, что позволяет преступникам быстро перемещать свои средства, чтобы скрыть контрольный след.

Криптовалютный сектор все еще относительно нерегулируемый по сравнению с традиционными фиатными валютами и поэтому традиционные методы отслеживания движения средств в сфере криптовалют неэффективны. Для проведения расследования в блокчейне требуются специальные аналитические инструменты. С развитием биткоина, преступники чувствовали себя в безопасности при обработке своих транзакций в биткоинах из-за их псевдонимного характера. Каждая транзакция в биткоинах регистрируется в блокчейне, из-за неизменности блокчейна транзакцию практически невозможно стереть или изменить из блокчейна сразу после ее регистрации. Однако развитие аналитических инструментов блокчейна на протяжении многих лет позволило правоохранительным органам и криптокомпаниям идентифицировать и деанонимизировать данные в блокчейне. Эти инструменты, используя сложный алгоритм, визуально представляют данные в блокчейне. Разработка аналитических инструментов блокчейна привела к нескольким успешным крипторасследованиям правоохранительных органов путем отслеживания следов в блокчейне. Например, специальный агент ФБР Ильван Йам в 2013 г. отчитался о том, что за 12 месяцев он отследил 3760 биткойн-транзакций с серверов Silk Road на ноутбук Росса Ульбрихта. Для достижения своей цели он отследил перемещение более чем 700 000 биткойнов с кошельков маркета Silk Road на личные кошельки Ульбрихта. Это был первый случай использования потенциала аналитического инструмента блокчейна для раскрытия уголовных дел [4]. В результате преступники поняли, что простого перевода биткойнов с

одного кошелька на другой недостаточно для обеспечения анонимности плательщика и получателя платежа.

Преступники использовали и продолжают использовать дополнительные инструменты для повышения анонимности. Так криптосервисы микшеры или тумблеры, которые смешивают криптовалюты различных пользователей и затем отправляют криптовалюты на другой кошелек в соответствии с инструкциями их «клиента». В результате правоохранительные органы могут видеть, что человек отправил некоторое количество криптовалют на микшер, а другой человек получил криптовалюту, но они не могут увидеть, есть ли прямая связь между ними.

Вложенная биржа поддерживает счета на различных популярных криптовалютных платформах и позволяет своим клиентам торговать с использованием этих счетов. Вложенный обмен обычно предлагает немедленный доступ ко всем функциям без требований проверки персональных данных клиента. Этот тип обменов во многих случаях предоставляет услуги по отмыванию денег мошенникам и потенциально может использоваться для платежей с целью вымогательства.

Нерегулируемые биржи, которые не регулируются и, следовательно, не подпадают под требования набора мер, предпринимаемых финансовыми и другими участниками рынка, чтобы обнаружить попытки получения и легализации средств, происходящих от незаконной деятельности (далее – AML) [5].

Биткоин работает на базе публичного блокчейна, транзакции в котором можно отследить с помощью различных сервисов. Поэтому, многие преступники обращаются к анонимным монетам с функциями конфиденциальности, такие как Monero. Monero работает на анонимном блокчейне, то есть шифрует адрес получателя в блокчейне и генерирует поддельные адреса, чтобы скрыть реального отправителя [6]. Хотя эти монеты и более устойчивы к отслеживанию, чем другие криптовалюты, однако правоохранительные органы с наиболее

продвинутым оборудованием и методами всё же могут отследить их движение, хоть это и требует куда больше времени и усилий.

Широкое распространение технологии сети P2P позволяют пользователям обмениваться криптовалютами или криптоактивами без участия криптовалютной биржи. Именно в этих случаях преступники используют ничего не подозревающих пользователей для отправки средств на другие адреса.

Также для криминальной деятельности преступники используют крипто-банкоматы для покупки криптовалют наличными, с помощью дебетовой или кредитной карты. Криптовалютный банкомат выдает QR-код, который можно отсканировать и отправить криптовалюту на свой цифровой кошелек. Данная операция позволяет преступникам переводить наличные на адреса кошельков, хранящихся в другом месте, вместо физического перевода наличных за границу.

Многие платформы азартных игр могут принимать платежи в криптовалюте. Для этого преступники могут использовать сайты онлайн-игр для отправки криптовалют из одной страны на адрес кошелька, контролируемого преступником в другой стране. В результате преступник может приобрести чипы за криптовалюты, провести несколько транзакций, а затем «обналичить» их на адрес кошелька, который контролируется тем же преступником, другим сообщником или «вложенным поставщиком услуг» [7].

Невзаимозаменяемые токены (далее – NFT) хранят данные в различных блокчейнах, большинство из них в блокчейне Ethereum. Эти данные могут быть связаны с цифровыми произведениями искусства или другими цифровыми предметами и дают владельцу NFT неизменное право собственности на данные, с которыми связан токен. Их можно покупать и продавать с помощью криптовалют на специализированных торговых площадках. Недавнее исследование Министерства финансов США показало, что быстро развивающийся рынок NFT может стать мишенью для отмывания денег и финансирования терроризма, которые хотят «отмыть» незаконно полученные средства.

DeFi расшифровывается как децентрализованные финансы. Это финансовый инновационный инструмент, основанный на блокчейне, который позволяет своим пользователям предоставлять кредиты, торговать, занимать финансовые средства на основе P2P и без традиционных посредников, таких как банки. Хакеры во многих случаях используют уязвимости в недавно разработанных платформах DeFi и умудряются красть деньги пользователей протоколов DeFi. После кражи преступники во многих случаях обменивают украденные активы на чистые активы на другой платформе DeFi или обеспечивают залог незаконно полученных активов для получения другого токена [8].

Независимо от того, какие методы используют преступники для повышения анонимности своих транзакций и адресов кошельков, во многих случаях правоохранные органы начинают с подозреваемого и пытаются выяснить, какие криптовалютные адреса контролирует подозреваемый, посредством криминалистического анализа устройств подозреваемого. В других случаях могут быть использованы аналитические инструменты блокчейна. С помощью этих инструментов могут получать информацию о геолокации. Если речь идет о криптовалютной бирже, правоохранные органы могут запросить информацию о владельцах адресов кошельков, как они делают в традиционных финансовых фирмах. Однако в некоторых юрисдикциях стоимость этих инструментов блокчейн-анализа является препятствием для успешных расследований в криптосреде.

Криптоиндустрия продолжит расти и преступники продолжат отмывать доходы от своих преступлений с использованием криптовалют. Продолжающийся прогресс в криптоиндустрии усложнит правоохранным органам выявление преступной деятельности и борьбу с ней, а преступникам – отмывание незаконно полученных средств. В результате правительствам, компетентным органам и правоохранным органам важно быть в курсе методов, применяемых преступниками, и использовать преимущества

аналитических инструментов блокчейна для эффективной борьбы с отмыванием денег с использованием криптовалют и криптоактивов.

Группа разработки финансовых мер по борьбе с отмыванием денег (далее – ФАТФ) учреждена «семеркой» при участии Европейской комиссии в ходе Парижской встречи G7 в июле 1989 года. (Российская Федерация принята в члены в июне 2003 года) и другие международные организации признают потенциальные преимущества блокчейна и соответствующих инновационных продуктов и услуг. Однако эти органы стремятся принять эффективные меры для смягчения последствий злоупотребления блокчейном со стороны преступников. В результате, хотя и ожидается, что криптоиндустрия значительно вырастет в будущем, в то же время она будет жестко регулироваться на глобальном уровне, как и другие финансовые организации.

Литература

1. Карпика, А. Г. Вопросы обеспечения информационной безопасности в глобальной сети / А. Г. Карпика, С. В. Лемайкина // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 8-й Всероссийской научно-практической конференции, Белгород, 21 мая 2021 года. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2021. – С. 101-105.
2. Криптопреступность – Нож [Электронный документ] <https://knife.media/cryptocriminal/> Дата ознакомления: 28.05.2024.
3. Chainalysis: отчет по крипто преступлениям 2021 [Электронный документ] <https://vc.ru/money/251237-chainalysis-otchet-po-kripto-prestupleniyam-2021>. Дата ознакомления: 28.05.2024.
4. Лучшие инструменты для блокчейн-анализа и как они работают. [Электронный документ] <https://investfuture.ru/articles/id/luchshie-instrumenty-dlya-blokcheyn-analiza-i-kak-oni-rabotayut>. Дата ознакомления: 28.05.2024.
5. Что такое AML и почему важно проверять криптовалюту. [Электронный документ] <https://habr.com/ru/articles/756526/>. Дата ознакомления: 28.05.2024.

6. «Выбор хакеров». Что такое Monero и как работает эта монета. [Электронный документ] <https://www.rbc.ru/crypto/news/60d1f5949a7947df6c879994>. Дата ознакомления: 28.05.2024.

7. Роль криптовалют в онлайн-гемблинге и high-risk платежей [Электронный документ] <https://mayfray.top/blog/rolj-cryptovaljut-v-online-gambleng>. Дата ознакомления: 28.05.2024.

8. За взломы DeFi зачастую ответственны инсайдеры [Электронный документ] <https://www.block-chain24.com/articles/za-vzlomy-defi-zachastuyu-otvetstvenny-insaydery>. Дата ознакомления: 28.05.2024.

Сведения об авторе

Лемайкина Светлана Владимировна, старший преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России.

Лихобабина Анна Викторовна

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ ОРГАНИЗАЦИИ
РАСПРЕДЕЛЕНИЯ ПО ГРУППАМ СПЕЦИАЛИСТОВ, ПРОХОДЯЩИХ
ПОДГОТОВКУ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ**

В настоящее время многие специалисты обязаны проходить специализированную подготовку и переподготовку в образовательных организациях. Особенно важно это для организации подготовки специалистов к действиям в чрезвычайных обстоятельствах. Чрезвычайные обстоятельства носят стихийный характер, поэтому необходимо осуществлять обучение специалистов максимально быстро и качественно [1, 2]. Кроме того, эффективность обучения значительно возрастает, если осуществляется групповое обучение специалистов различного профиля для совместных действий в зоне чрезвычайного обстоятельства. Это объясняется тем, что специалисты, включённые в группу, должны обладать как общими, так и уникальными компетенциями [4, 5].

Математические методы организации распределения специалистов по группам помогают оптимизировать процесс обучения, учитывая различные факторы, такие как уровень знаний специалистов, их компетенции, а также доступные ресурсы учебного заведения [6].

Большое внимание уделяется оптимизации процесса формирования групп с учетом множества параметров. Например, при формировании группы необходимо учитывать такие факторы, как имеющиеся у специалистов компетенции. Математические методы могут помочь автоматизировать и оптимизировать этот процесс, уменьшая время и трудозатраты на его подготовку [3, 7].

Кроме того, математические методы организации распределения специалистов по группам также могут помочь в планировании учебного процесса и оптимизации расписания занятий. Например, можно использовать алгоритмы оптимизации расписания занятий, которые учитывают предпочтения

специалистов по времени и дням недели, а также доступность преподавателей и аудиторий. Это позволяет снизить количество пересечений в расписании, обеспечивая более комфортные условия обучения.

Для распределения специалистов по группам будем использовать генетический алгоритм [8]. Его основным преимуществом является способность к эффективному поиску глобального оптимума в сложных многомерных пространствах, даже при наличии множества локальных оптимумов. Это достигается благодаря механизмам параллельного поиска в пространстве решений и использования концепций естественной эволюции [9, 10].

Основные этапы реализации генетического алгоритма включают:

1. Кодирование решений в виде хромосом.
2. Формирование начальной популяции решений.
3. Оценка качества решений с использованием целевой функции.
4. Применение генетических операторов (селекция, кроссовер, мутация)

для создания новых поколений решений.

5. Проверка условия останова алгоритма и, при необходимости, возврат к шагу 3.

Рассмотрим задачу распределения специалистов по направлениям подготовки к действиям при чрезвычайных обстоятельствах в образовательной организации. Пусть имеется множество специалистов $S = \{s_1, s_2, \dots, s_n\}$, каждый из которых обладает определенным набором компетенций и может быть распределен по одному или нескольким направлениям подготовки $D = \{d_1, d_2, \dots, d_m\}$.

Каждое направление подготовки d характеризуется следующими параметрами:

- требуемое количество специалистов N_d , необходимое для обеспечения подготовки по данному направлению;

- минимальный уровень компетенций C_d , необходимый для успешного освоения программы подготовки по направлению;
- время T_d , необходимое для подготовки специалистов по данному направлению.

Задача заключается в том, чтобы распределить специалистов из множества S по направлениям подготовки D таким образом, чтобы:

- 1) для каждого направления d было назначено N_d подходящих специалистов, обладающих требуемым уровнем компетенций C_d ;
- 2) суммарное время подготовки специалистов по всем направлениям было минимизировано.

Для решения задачи был разработан вариант генетического алгоритма, в котором в качестве «хромосомы» использовалась двоичная матрица $X = (x_{ij}), i = 1, \dots, n; j = 1, \dots, m$, где

n - количество специалистов,

m - количество направлений подготовки.

Каждый элемент x_{ij} этой матрицы будет принимать значение 1, если специалист i распределен на направление j , и 0 в противном случае.

Начальная популяция решений формируется случайным образом [3].

Качество каждого решения (хромосомы) в популяции оценивается с использованием целевой функции, которая учитывает два критерия:

- 1) соответствие количества специалистов, назначенных на каждое направление подготовки, требуемому количеству;
- 2) суммарное время подготовки специалистов по всем направлениям.

Для этого используются разработанные в [11] алгоритмы построения оптимального расписания.

После применяются следующие генетические операторы для создания новых поколений:

- селекция: из текущей популяции выбираются наиболее «приспособленные» решения для участия в дальнейших операциях;
- кроссовер: для пар отобранных решений-родителей генерируются новые решения-потомки путем комбинации частей их хромосом;
- мутация: с небольшой вероятностью в хромосомах решений могут происходить случайные изменения отдельных битов, что позволяет избежать преждевременной сходимости к локальному оптимуму.

На каждой итерации алгоритма формируется новое поколение решений, обладающих в среднем более высоким качеством.

Алгоритм продолжает работу до тех пор, пока не будет достигнут заданный критерий остановки, например, определенное число итераций или достижение требуемого значения целевой функции. После этого, лучшее решение из последнего поколения выбирается в качестве окончательного результата.

Для оценки эффективности предложенного подхода на основе генетического алгоритма, были проведены экспериментальные исследования.

В качестве начальных данных были сгенерированы начальные данные, варьирующиеся по количеству специалистов ($n = 50, 100, 150, 200$) и направлений подготовки ($m = 10, 20, 30, 40$).

Для каждого случая был реализован генетический алгоритм с различными настройками параметров. Полученные результаты сравнивались с решениями, полученными с использованием методов целочисленного линейного программирования.

Результаты экспериментов показали, что генетический алгоритм способен находить решения, близкие к оптимальным, за приемлемое время. Так, для задач с 50 специалистами и 10 направлениями подготовки, время решения с помощью генетического алгоритма составляло в среднем 2-3 минуты, в то время как точное

решение методом целочисленного линейного программирования требовало более 30 минут.

При увеличении размерности задачи (до 200 специалистов и 10 направлений), точное решение методом целочисленного линейного программирования становилось практически неосуществимым из-за экспоненциального роста вычислительной сложности, в то время как генетический алгоритм продолжал находить приемлемые решения за разумное время (10-15 минут).

Литература

1. Ямалов И.У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / И.У. Ямалов. – М.: Лаборатория знаний, 2020. – 291 с.
2. Математическое моделирование действий органов внутренних дел в чрезвычайных обстоятельствах / В.В. Меньших, А.Ф. Самороковский, В.В. Горлов [и др.]. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2016. – 187 с.
3. Lihobabina, A. Model and Numerical Method of Optimization of Selection of Training Programs for Specialists / A. Lihobabina, V. Menshikh // IEEE Proceedings of 5th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, 08–10 ноября 2023 года. – Lipetsk: Lipetsk State Technical University, 2023. – P. 447-450.
4. Меньших, В.В. Моделирование процессов оптимизации выбора программ подготовки и переподготовки специалистов с использованием генетического алгоритма / В.В. Меньших, А.В. Лихобабаина // Автоматизация и моделирование в проектировании и управлении. – 2024. – № 1(23). – С. 42-48.
5. Меньших, В.В. Модель определения состава курсов обучения по нескольким направлениям / В.В. Меньших, А.В. Лихобабаина // Информатика: проблемы, методы, технологии: сборник материалов XXIV международной научно-практической конференции / под редакцией Д.Н. Борисова; Воронеж,

Воронежский государственный университет, 14-15 февраля 2024 г. – Воронеж, ВГУ, 2024. – С. 1116-1122.

6. Моделирование коллективных действий сотрудников органов внутренних дел / В.В. Меньших, А.Ф. Самороковский, Е. Н. Середа, В.В. Горлов. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2017. – 236 с.

7. Меньших, В.В. Математическая модель оптимизации траектории обучения сотрудников органов внутренних дел действиям при чрезвычайных обстоятельствах / В.В. Меньших, Е.Н. Середа // Вестник Воронежского института МВД России. – 2015. – № 3. – С. 36-44.

8. Лихобабаина, А.В. Обоснование выбора генетического алгоритма для оптимизации распределения программ подготовки специалистов / А.В. Лихобабаина // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы: сборник материалов Всероссийской научно-практической конференции, Воронеж, 19 октября 2023 года. – Воронеж: Издательско-полиграфический центр «Научная книга», ФКОУ ВО Воронежский институт ФСИН России., 2023. – С. 356-359.

9. Гладков Л.А. Генетические алгоритмы / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик / Под ред. В.М. Курейчика. - 2-е изд. М., 2010. - 368 с.

10. Карпенко А.П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой: учебное пособие / А.П. Карпенко. - 2-е изд. - Москва: Издательство МГТУ им. Н.Э.Баумана, 2017. - 446 с.

11. Men'shikh, V.V. Selecting methods of optimizing sequences in executing requests to computing systems / V. V. Men'shikh // Automatic Control and Computer Sciences. – 1996. – Vol. 30, No. 1. – P. 51-54.

Сведения об авторе

Лихобабаина Анна Викторовна, адъюнкт Воронежского института МВД России.

**Матвеев Семен Николаевич,
Нуждина Олеся Евгеньевна**

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННЫХ СРЕДСТВ «ЖИВАЯ МАТЕМАТИКА», «МАТЕМАТИЧЕСКИЙ КОНСТРУКТОР» И «GEOGEBRA»

Согласно рекомендациям Министерства просвещения и Министерства науки и высшего образования Российской Федерации для развития познавательной и творческой деятельности обучающихся в настоящее время разрабатываются и применяются специальные программы и информационные ресурсы, выступающие как интерактивные творческие предметные среды [1]. Многие из них свободно распространяемые и могут быть использованы пользователями, интересующимися математикой и проблемами преподавания математики.

Современные образовательные программы позволяют осуществить индивидуальный подход к каждому обучающемуся, учитывая при этом как содержание изучаемого материала, так и уровень знаний и навыков пользователя. Отметим, что многие свободно распространяемые программы не требуют от пользователя специальных знаний информатики, однако они эффективны в обучении, например, в геометрии в силу их наглядности. В основе таких программ в общем лежит принцип динамической геометрии, который наделяет объекты динамическими свойствами. Программные обеспечения, работающие по такому принципу, соотносятся к интерактивно геометрическим системам. Они разработаны для образовательных целей, а именно, для выполнения геометрических построений и трансформаций построенных объектов.

Сейчас для начинающих пользователей существует несколько геометрических сред, каждая из которых имеет свои преимущества и недостатки. Здесь приведем описание трёх наиболее распространенных обучающих программ: «Математический конструктор», «Живая математика» и «Geogebra».

Как показывает практика, часто в процессе обучения геометрии преподаватель задается вопросом, какую же лучше интерактивную и динамическую среду выбрать. Ведь выбранная программа должна создавать компьютерные чертежи, а также модели, при этом корректировка данных не должна повлечь за собой изменение всего процесса построения. Также стоит добавить, что выбранная среда должна давать возможность просматривать и выполнять работу с авторскими объектами, созданными лично.

Поэтому на первый выбор предлагаются такие программы, как «Живая математика», «Математический конструктор» и «Geogebra», они являются весьма популярными и широко применяются на практике в качестве программ динамической геометрии. Начнем сравнительный краткий анализ с программы «Живая математика», выделим основные ее преимущества и недостатки.

Данной среде присуще моделирование и динамическое преобразование чертежей, графиков, а также других объектов. Пользователи могут решить широкий спектр задач при изучении таких разделов, как геометрия, алгебра, математический анализ и тригонометрия. «Живая математика» создана на основе программы «Geometry Sketchpad» и переведена на русский язык Институтом новых технологий. Рассматриваемая динамическая среда доступна для таких операционных систем, как Windows и macOS.

Отметим, что все отмеченные программы дают возможность обучающимся и преподавателям создавать и работать с динамическими математическими объектами, но у каждой есть свои особенности и преимущества. Выбор среды зависит от индивидуальных потребностей и предпочтений учителя и учащихся.

Например, «Живая математика» позволяет выполнять различные построения на плоскости, такие как точки, прямые, лучи, отрезки, а также создавать модели сложных фигур. Программа почти полностью охватывает материал планиметрии. В связи с этим учащиеся седьмых, восьмых и девярых

классов могут использовать все возможности для демонстрирования и доказательства теорем геометрии [2, 3].

Но, к сожалению, в «Живой математике» имеются и некоторые недостатки, например, это проявляется в работе с 3D чертежами. Отсутствие 3D-полотна не позволяет прямое построение трехмерных фигур.

Тем не менее, можно найти выход из этой ситуации, если сделать дополнительные вспомогательные построения. Следовательно, объемные тела, тела вращения, могут быть реализованы в «Живой математике», однако подобные построения в этой среде трудоемки. В качестве иллюстрации приведем пример реализации комбинации сферы и пирамиды: в правильную треугольную пирамиду вписан шар. Секущая плоскость перпендикулярна высоте пирамиды и проходит через её середину.

В начале построения создаются числовые параметры, соответствующие координатам той или иной точки. После этого используется инструмент «Точка» по координатам. Следует отметить, что такой подход, как привязка к системе координат и выполнение построения фигуры по координатам, не всегда является удобным и точным. Поэтому предлагается использовать альтернативные методы, а также инструменты для работы с объемными телами в данной программе. (рис.1) [4].

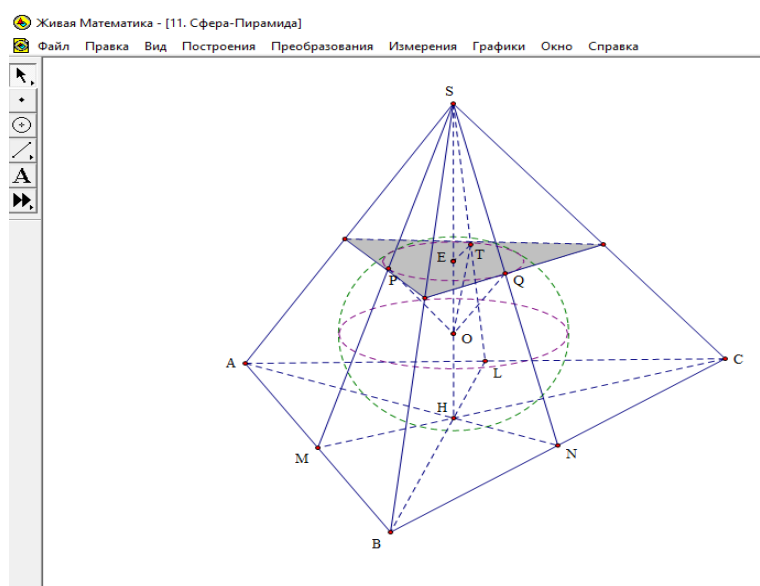


Рис.1. Сфера, вписанная в пирамиду (реализация в «Живой математике»)

Следующая программа, на которую следует обратить внимание – это «Математический конструктор». Это российская разработка, применяемая в процессе обучения в качестве интерактивного динамического инструмента. Разработчик данного конструктора, компания «1С», начиная с 1996 года создает образовательные мультимедийные продукты.

Функционал данной программы состоит в следующем: создание интерактивных моделей, объединяющие конструирование, динамические изменения и эксперименты. «Математический конструктор» работает на такие операционные системы, как Windows, Linux, MacOS, iOS и Android. Есть возможность работы в онлайн-версии, но с некоторыми ограничениями.

В сравнении с прежней версией данной программы, возможности работы с плоскими объектами довольно велики. Например, динамическое построение геометрических объектов, произведение расчетов и измерений, построение графиков функций, создание задач с возможностью автопроверки и так далее.

Сам интерфейс программы прост и удобен в использовании. Есть все необходимые инструменты для построения. Основную часть программы занимает рабочая область, а элементы дизайна находятся с правой стороны. Здесь приведен пример работы с параметром (рис.2): найдите все значения параметра a , при каждом из которых система уравнений имеет ровно два различных решения:

$$\frac{xy^2 - 5xy - 5y + 25}{\sqrt{x+5}} = 0, \quad y = ax$$

Эта программа может быть успешно использована в проектной деятельности обучающихся при работе над созданием интерактивных чертежей и моделей.

Также, как и в «Живой математике», отсутствие интерактивного 3D-холста, ограничивает возможности работы с пространственными объектами и фигурами.

Для сравнения рассмотрим следующее распространенное динамическое программное обеспечение «Geogebra», часто используемое начинающими

пользователями и в обучении математике. В сравнении с предыдущими заметно то, что «Geogebra» визуализирует связь между такими разделами, как алгебра и геометрия, калькулятором вероятности и элементами математического анализа. Начиная с 2002 года, с момента создания австрийским математиком и профессором университета Йоханнеса Кеплера (JKU) в Линце Маркусом Хоэнвартером, предлагаемая программа ежегодно завоевывает множество образовательных наград в Европе и США.

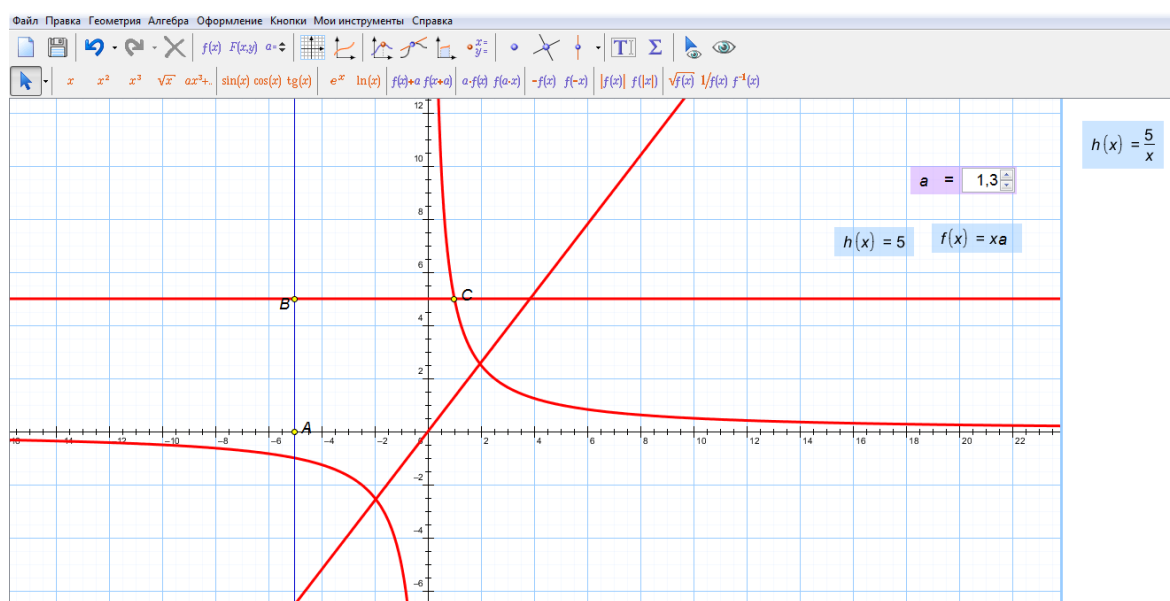


Рис. 2. Решение задачи в программе «Математический конструктор»

«Geogebra» является наиболее удобной программой для работы учителя математики по нескольким причинам, отметим их.

Во-первых, она обладает широкими возможностями для построения и визуализации математических объектов и моделей. Дает возможность создавать точки, отрезки, векторы, прямые, функции, многоугольники и другие геометрические объекты. Кроме этого поддерживает работу с переменными числами, векторами и точками, расчет производных и интегралов функций.

Во-вторых, «Geogebra» имеет удобный и интуитивно понятный интерфейс, что делает ее доступной даже для учителей, которые не имеют особых компьютерных навыков. Она переведена на множество языков, что позволяет использовать ее в разных странах. Кроме того, она поддерживает различные операционные системы, включая Windows, Linux, MacOS, iOS и Android.

В-третьих, «Geogebra» бесплатно распространяется, что позволяет устанавливать ее на школьных компьютерах и домашних ПК без дополнительных затрат. Она также может быть установлена на смартфоны и планшеты, что позволяет работать с ней в любом месте.

Наконец, «Geogebra» является мощным инструментом для различных этапов математического образования. Данная программа может быть использована для демонстрации математических концепций, проведения интерактивных уроков, создания задач и тестов с автоматической проверкой, а также для самостоятельного исследования и эксперимента.

Для того, чтобы убедиться во всех перечисленных фактах, был реализован динамический чертеж в программе «Geogebra» (рис.3).

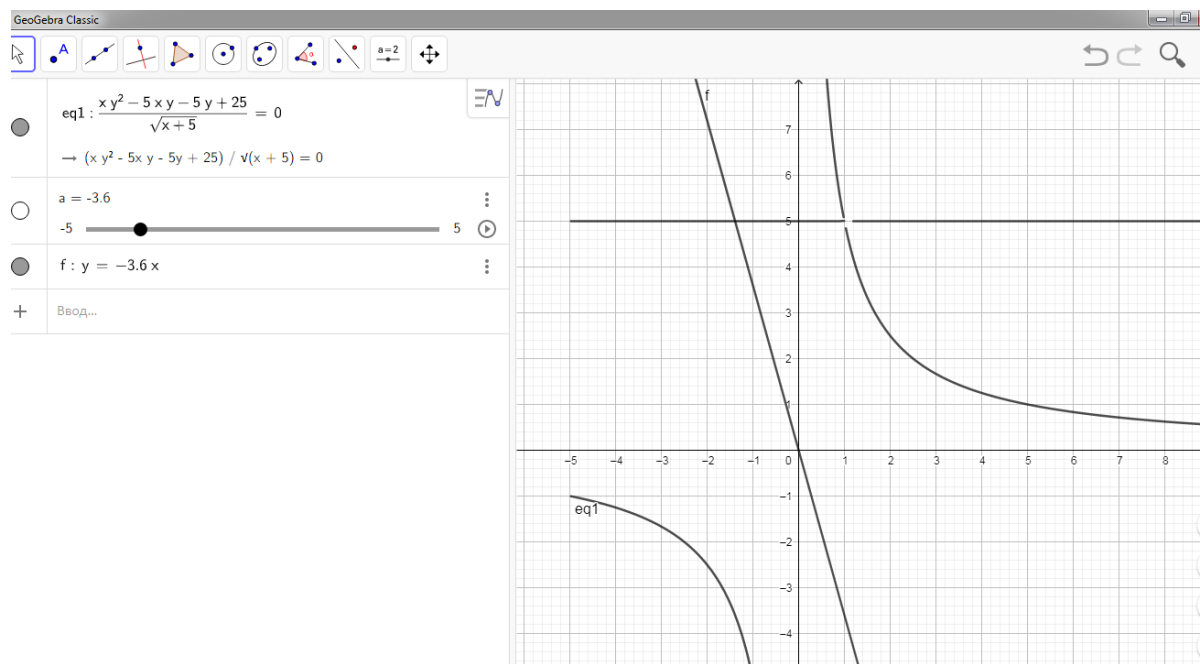


Рис. 3. Решение задачи в программе «GeoGebra»

В целом, «Geogebra» в сравнении с другими представляет собой комплексное эффективное элементарное средство для математического моделирования, которое может значительно облегчить и улучшить процесс обучения и понимания математики [5-7].

Таким образом, здесь приведен краткий анализ интерактивных динамических программ, которые работают по принципу динамической геометрии: «Живая математика», «Математический конструктор», «Geogebra».

Сравнивая каждую из трех сред, можно отметить, что для математического моделирования наиболее удобной для работы учителя представляется среда «Geogebra».

Безусловно, с каждым годом количество других программных обеспечений, используемых на современных технических средствах, обновляется, становится все больше. И использование в учебном процессе таких ресурсов, позволит пользователям лучше сориентироваться в изучаемой ими математике.

Литература

1. Матвеев, С.Н. Методические основы проектирования цифрового симулятора педагогической деятельности / А. А. Галиакберова, Э. Х. Галямова, С. Н. Матвеев // Вестник Мининского университета. – 2020. – Т. 8, № 3(32). – С. 2. – DOI 10.26795/2307-1281-2020-8-3-2. – EDN EUCXLZ.

2. Матвеев, С. Н. О некоторых методических возможностях применения компьютерной системы моделирования «ЖИВАЯ ГЕОМЕТРИЯ» / С.Н. Матвеев, Г.Р. Антропова // Проблемы современного педагогического образования. – 2018. – № 61-1. – С. 174-177. – EDN VPJPYW.

3. Матвеев, С.Н. О некоторых приложениях компьютерной системы моделирования «Live geometry» / С.Н. Матвеев, Ф.И. Хайбуллина // Информационные технологии. Автоматизация. Актуализация и решение проблем подготовки высококвалифицированных кадров (ИТАП-2018): Сборник материалов VIII международной научно-практической конференции, Набережные Челны, 19 октября 2018 года. – Набережные Челны: Издательство Набережночелнинского института (филиала) ФГАОУ ВО «Казанский (Приволжский) федеральный университет», 2018. – С. 219-229. – EDN AGVPBD.

4. Халикова, И.И. Реализация 3-D моделирования в УМК «Живая математика» / И. И. Халикова, С.Н. Матвеев // Вызовы XXI века: Материалы всероссийской студенческой научно-практической конференции, Набережные Челны, 17–21 апреля 2023 года. – Набережные Челны: Набережночелнинский

государственный педагогический университет, 2023. – С. 450-452. – EDN KJCSRG.

5. Антропова, Г.Р. Компьютерная поддержка решения вероятностных задач из истории математики / Г. Р. Антропова, С. Н. Матвеев, Р. Г. Шакиров // Высшее образование сегодня. – 2022. – № 5-6. – С. 67-73. – DOI 10.18137/RNU.HET.22.05-06.P.067. – EDN NJMNEC.

6. Антропова, Г.Р. Использование математических редакторов в подготовке учителей математики / Г.Р. Антропова, С.Н. Матвеев, Б.В. Киселев // Высшее образование сегодня. – 2023. – № 4. – С. 22-29. – DOI 10.18137/RNU.HET.23.04.P.022. – EDN IPKETS.

7. Антропова, Г.Р. Приложение Wingeom в реализации преобразований плоскости Лобачевского / Г.Р. Антропова, С. Н. Матвеев // Научно-технический вестник Поволжья. – 2023. – № 11. – С. 411-413. – EDN HRAUCQ.

Сведения об авторах

Матвеев Семен Николаевич, кандидат физико-математических наук, доцент Набережночелнинского института Казанского федерального университета.

Нуждина Олеся Евгеньевна, магистрант Набережночелнинского государственного педагогического университета.

**Мельник Вячеслав Александрович,
Фомичева Маргарита Юрьевна**

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В КИБЕРБЕЗОПАСНОСТИ

Во все времена информация была самым ценным ресурсом. Постоянно разрабатываются методы, которые обеспечивают всестороннюю защиту данных от различных видов угроз (утечка, повреждение, доступ).

Развитие и повсеместное распространение цифровизации способствовали формированию понятия кибербезопасности. Это более узкий вид информационной безопасности, связанный с онлайн-средой и цифровыми технологиями. Кибербезопасность фокусируется на защите компьютерных систем, сетей и данных именно от киберугроз, хакерских атак и вредоносного программного обеспечения [1].

Для обеспечения кибербезопасности специалистами разрабатываются и используются различные методы, разделенные на две группы: физические и математические. На рисунке 1 представлены виды физических методов, реализующих фундаментальную защиту данных от утечек в онлайн-среде [2].

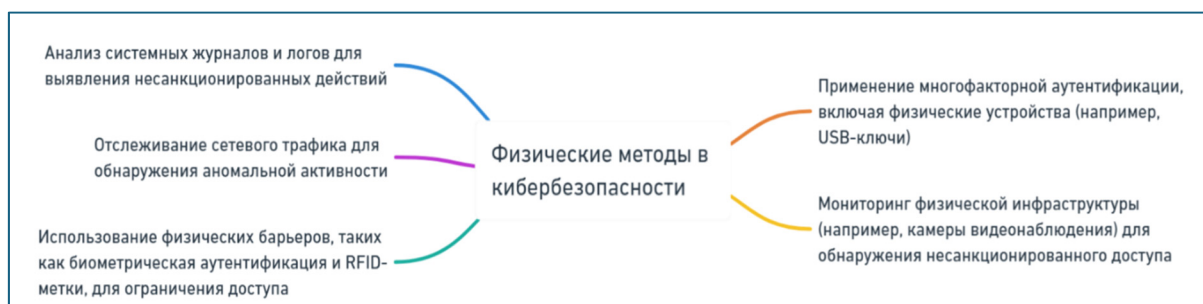


Рис.1. Примеры физических методов, используемых в кибербезопасности

Рассмотрим более детально математические методы. Их использование в кибербезопасности играет одну из ключевых ролей, обеспечивая безопасность информации и защиту компьютерных систем. Эти методы позволяют анализировать и предсказывать уязвимости систем, разрабатывать эффективные алгоритмы шифрования и аутентификации, а также обнаруживать и предотвращать атаки.

Криптография, математическая логика и статистические методы являются основными инструментами, используемыми в этой области. Благодаря математическому анализу и моделированию возможных угроз, специалисты по кибербезопасности могут эффективно защищать информацию от несанкционированного доступа и манипуляций. На рисунке 2 представлена классификация описанных выше математических методов.

Математические методы криптографии имеют большое значение в обеспечении безопасности информации в киберпространстве. Они используются для защиты данных посредством шифрования и подписывания информации, чтобы предотвратить несанкционированный доступ и изменение данных.

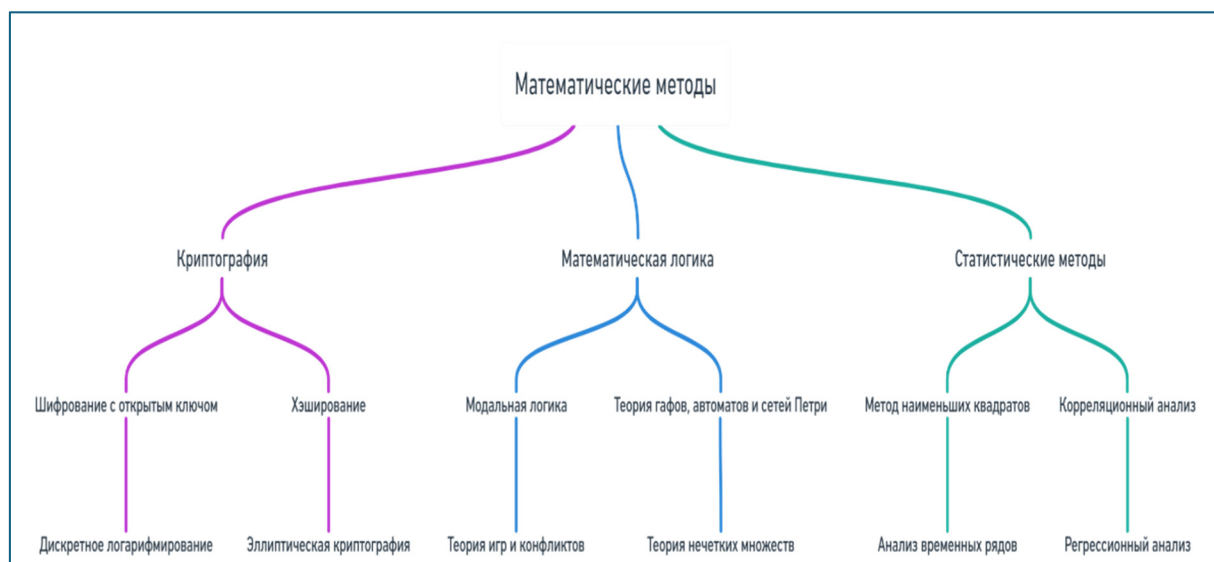


Рис.2. Классификация математических методов

Например, алгоритм RSA (Rivest, Shamir и Adleman – фамилии разработчиков алгоритма с открытым ключом) основан на сложности факторизации больших чисел и используется для шифрования данных во многих системах. Симметричные алгоритмы, такие как AES (Advanced Encryption Standard – расширенный стандарт шифрования), обеспечивают более быструю и надежную защиту данных. На рисунках 3 и 4 представлена последовательность выполнения алгоритма шифрования с открытым ключом и алгоритма стандарта шифрования соответственно.

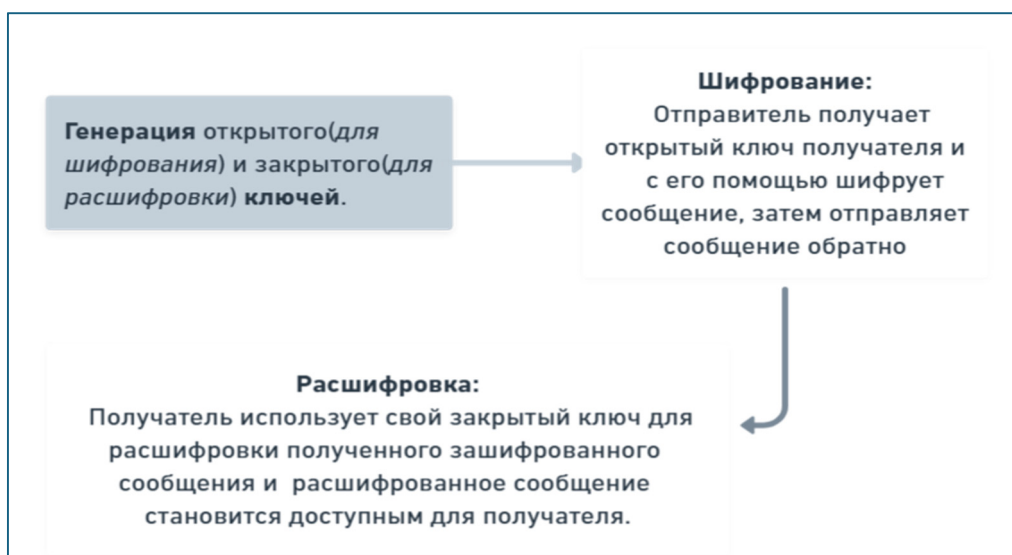


Рис. 3. Алгоритм RSA

Переходя к математической логике как методу, используемому в защите данные от кибератак, следует более детально остановиться на теории игр, теории графов и теории нечетких множеств. Они чаще всего используются разработчиками программ, обеспечивающих сохранность данных в цифровой среде от утечек и атак, совершаемых злоумышленниками с целью получения доступа к личным или корпоративным конфиденциальным данным.

Рассматривая суть каждой из этих теорий в отдельности, следует начать с теории графов. Она, как наиболее популярная используется чаще всего. В теории граф – набор из вершин и ребер. В кибербезопасности, в одних случаях, за вершины можно принять объекты, представляющие интерес для различных категорий злоумышленников, а в других – самих злоумышленников. Ребра – каналы связи между объектами, пути по которым хакеры могут «добраться» до защищаемой информации. Выделяют два вида каналов передачи информации – односторонние и двусторонние. Для отражения этого факта в теории графов были введены понятия «дуг» и «ребер» соответственно. Теория графов позволяет визуализировать часть процесса обеспечения кибербезопасности.

Теория игр является интересным пространством для изучения поиска новых решений. В этих играх участвуют различные типы игроков (все зависит от области применения), чьи решения (сделанные ходы) отражаются на всех

остальных игроках. Так, игроки разрабатывают стратегии и, придерживаясь их, ведут свою команду к той цели, ради которой и начиналась «игра». В кибербезопасности игроками могут являться сотрудники отделов по обеспечению информационной безопасности и группы потенциальных нарушителей (спецслужбы иностранных государств, хакеры, конкурирующие организации), а целями для этих двух групп игроков будут соответственно обеспечение информационной безопасности и ее нарушение. Теория игр использует термин «равновесие Нэша», что означает ситуацию, при которой игроки, сделав ход, приходят к консенсусу и не сожалеют о том, что будет за этим шагом (их устраивает сложившееся состояние). При использовании теории в рассматриваемой области, можно сказать, что равновесие по Нэшу достигается не единожды.



Рис. 4. Алгоритм AES

Теория нечетких множеств отсылает нас к тем ситуациям, когда информации мало, а решение принять нужно быстро. Здесь описывается заданное множество и в него входящие элементы. Но входят ли они в него с точностью до 100% мы утверждать не можем. Одним из примеров применения теории нечетких множеств может служить возможность оценки киберустойчивости системы оперативно-диспетчерского управления при кибератаках на системы сбора, обработки и передачи информации [3].

Математическая статистика позволяет анализировать атаки и угрозы по факту их совершения. Главное в таких методах — точность описываемых

событий. Один из статистических методов является корреляционный анализ, показывающий связь между двумя элементами так, что изменение одного ведет к модификации другого. Существует несколько видов корреляции: парная (при которой с обоими компонентами происходят изменения/отсутствуют изменения), частная (один из двух компонент меняется, другой – фиксирован) и, более сложная – множественная (изменения возникают относительно каждого элемента). Указанный метод позволяет проследивать связи и прогнозировать развитие ситуации [4]. Математическое представление этого метода можно выразить коэффициентом корреляции

$$r_{xy} = \frac{\sum(x_i - \bar{x}) \cdot (y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \cdot \sum(y_i - \bar{y})^2}},$$

где x – значение показателя-фактора (например, количество обнаруженных уязвимостей в системе), y – значение результативного показателя (количество инцидентов за определенный период времени). Результат выражения может принимать значения от -1 до 1 и чем ближе он крайним, тем сильнее корреляция между переменными. В случае если значение ближе к 0 – корреляция слабая.

Математические методы часто используются специалистами из разных областей науки и техники, с помощью описанных выше теорий можно задавать различные ситуации и искать пути выхода из них. Возможность «подстроить» математических теории под нужные специалистам значения облегчает работу по поиску уязвимостей и отражению атак. Благодаря математике специалисты по кибербезопасности могут создавать надежные системы защиты данных, обнаруживать инциденты безопасности и реагировать на них.

Однако развитие киберугроз и новейшие технологии требуют постоянного совершенствования математических методов в области кибербезопасности. В перспективе важно углублять исследования в области квантовой криптографии, машинного обучения и искусственного интеллекта для более точного анализа и прогнозирования угроз, а также для разработки новых методов защиты информации.

Таким образом, математические методы остаются фундаментальным инструментом в борьбе с киберугрозами, и их дальнейшее развитие и применение в новых направлениях исследований играют решающую роль в обеспечении кибербезопасности в будущем.

Литература

1. Основы информационной безопасности [Электронный ресурс] URL: <https://djvu.online/file/18wT6cPzoeHwX>.
2. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности [Электронный ресурс] URL: <https://files.stroyinf.ru/Data1/57/57256/index.htm>.
3. Сергеев С.С. Методика построения графа атак для объектов критической информационной инфраструктуры / С.С. Сергеев, И.И. Баранкова // Вестник УрФО. Безопасность в информационной сфере № 3(45). – 2022, с. 47–53.
4. Пять лучших инструментов для значительного повышения уровня информационной безопасности [Электронный ресурс] URL: <https://pdf.wondershare.com.ru/business/information-security.html>.

Сведения об авторах

Мельник Вячеслав Александрович, кандидат физико-математических наук, доцент кафедры информационной безопасности телекоммуникационных систем Воронежского института Федеральной службы исполнения наказаний.

Фомичева Маргарита Юрьевна, курсант Воронежского института Федеральной службы исполнения наказаний.

**Меньших Татьяна Валерьевна,
Ворончихин Максим Михайлович**

ПРИМЕНЕНИЕ ТЕОРИИ ГРАФОВ В ОПТИМИЗАЦИИ СЕТЕЙ СВЯЗИ

Сеть связи – это система среды распространения линий связи и технических средств, которые обеспечивают передачу данных от множества источников к множеству потребителей [1].

С увеличением количества пользователей данного способа коммуникации и ростом поступающих запросов появилась необходимость в расширении области покрытия связи и создании альтернативных маршрутов. Поэтому одной из важнейших задач является выбор оптимальных вариантов модернизации сети связи на основе прокладки новых маршрутов передачи данных.

Для решения данной задачи предлагается использовать методы математического моделирования [2], и, в частности, экстремальные задачи теории графов [3].

Это связано с тем, что сеть связи как объект представляет собой совокупность узлов (в число которых могут быть включены вышки проводной связи) и линий связи [1]. Поэтому графы являются естественной моделью сетей связи – вершины графа соответствуют узлам, рёбра – двусторонним, а дуги – односторонним линиям связи.

Вес рёбер или дуг могут соответствовать различным характеристикам сети, например, времени передачи сообщения или, как в рассматриваемом случае, стоимости модернизации сети.

Далее будем рассматривать только ориентированные графы, т.е. содержащие только вершины и дуги, считая, что каждое ребро заменено двумя противоположно направленными дугами с тем же весом, что и у порождающего их ребра.

Суть модели состоит в последовательном наращивании дерева кратчайших маршрутов от заданной начальной вершины до всех остальных. На первом шаге

отмечается начальная вершина; на каждом последующем шаге находится одна отмеченная вершина.

Опишем один шаг построения этого дерева. От последней отмеченной вершины определяются последующие (непосредственно достижимые) неотмеченные вершины, и вычисляется длина кратчайшего маршрута (сумма весов дуг, входящих в маршрут) от начальной вершины до каждой из них. Та вершина, до которой длина маршрута была минимальной, объявляется отмеченной.

Построение дерева заканчивается, когда помечены все вершины, минимальные маршруты до которых требуется найти.

Сам кратчайший маршрут находится на основе продвижения от конечной вершины к начальной по построенному дереву.

Достоинство данного алгоритма, предложенного нидерландским учёным Э. Дейкстрой, заключается в высокой эффективности (линейной вычислительной сложности), что позволяет использовать его при решении многих прикладных задач.

Приведём пример использования этого алгоритма для оптимизации выбора маршрута расширения сети проводной связи на основе модели фрагмента сети связи, изображённой на рисунке 1.

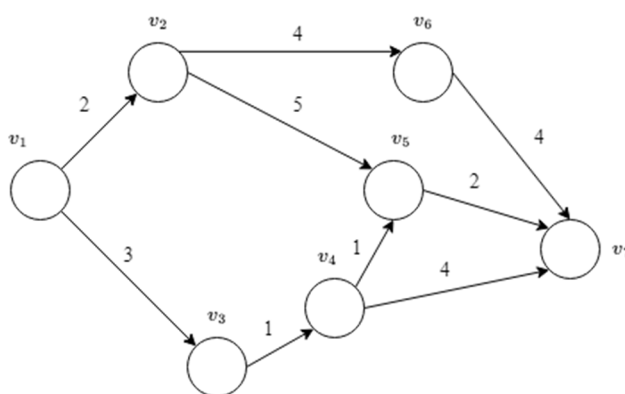


Рис. 1. Модель сети связи, представленная в виде ориентированного взвешенного графа

В качестве вершин определим вышки, а дуг с весами – потенциальные маршруты прокладки новых линий связи с затратами на установку новой вышки

в условных единицах и соединения с предыдущей. Будем считать, что требуется определить маршрут из вышки, заданной вершиной v_1 до вышки, заданной вершиной v_7 .

В таблице 1 представлены результаты присвоения меток, означающих кратчайший путь от вершины v_1 до других вершин.

Таблица 1. Этапы реализации алгоритма Дейкстры

	v_1	v_2	v_3	v_4	v_5	v_6	v_7
0	0	∞	∞	∞	∞	∞	∞
1	-	$\min(\infty; 2(v_1, v_2))$	$\min(\infty; 3(v_1, v_3))$	$\min(\infty; \infty(v_1, v_4))$	$\min(\infty; \infty(v_1, v_5))$	$\min(\infty; \infty(v_1, v_6))$	$\min(\infty; \infty(v_1, v_7))$
	-	2 v_1, v_2	3 v_1, v_3	∞	∞	∞	∞
2	-	-	$\min(3; 2 + \infty(v_2, v_3))$	$\min(\infty; 2 + \infty(v_2, v_4))$	$\min(\infty; 2 + \infty(v_2, v_5))$	$\min(\infty; 2 + \infty(v_2, v_6))$	$\min(\infty; 2 + \infty(v_2, v_7))$
	-	-	3 v_1, v_3	∞	7 v_1, v_2, v_5	6 v_1, v_2, v_6	∞
3		-	-	$\min(\infty; 3 + \infty(v_3, v_4))$	$\min(7; 3 + \infty(v_3, v_5))$	$\min(6; 3 + \infty(v_3, v_6))$	$\min(\infty; 3 + \infty(v_3, v_7))$
	-	-	-	4 v_1, v_3, v_4	7 v_1, v_2, v_5	6 v_1, v_2, v_6	∞
4		-	-	-	$\min(7; 4 + \infty(v_4, v_5))$	$\min(6; 4 + \infty(v_4, v_6))$	$\min(\infty; 4 + \infty(v_4, v_7))$
	-	-	-	-	5 v_1, v_3, v_4, v_5	6 v_1, v_2, v_6	8 v_1, v_7
5		-	-	-	-	$\min(6; 5 + \infty(v_5, v_6))$	$\min(8; 5 + \infty(v_5, v_7))$
	-	-	-	-	-	6 v_1, v_2, v_6	7 v_1, v_3, v_4, v_5, v_7
6		-	-	-	-	-	$\min(7; 6 + \infty(v_6, v_7))$
	-	-	-	-	-	-	7 v_1, v_3, v_4, v_5, v_7

Таким образом, анализируя представленные данные, можно увидеть, что наиболее выгодным вариантом является прокладывание линии связи через вышки v_3 , v_4 , v_5 с экономической составляющей в 7 у. е. Данный алгоритм является отличным способом для решения аналогичных задач, так как позволяет находить оптимальное расстояние и максимальную выгоду с учетом каких-либо условий.

Литература

1. Гольдштейн, Б.С. Системы коммутации: Учебник для вузов / Б.С. Гольдштейн. – 2-е издание, исправленное и дополненное. – Санкт-Петербург: БХВ-Санкт-Петербург, 2004. – 314 с. – ISBN 5-8206-0128-9. – EDN QMNMGZ.

2. Моделирование систем: практикум / Р.В. Кузьменко, Н.А. Андреева, Е.В. Корчагина, А.В. Папонов, Т.В. Меньших – Воронеж: Воронежский институт ФСИН России, 2021. – 99 с.

3. Меньших, В.В. Дискретная математика / В.В. Меньших. – Воронеж: Воронежский институт МВД России, 2013. – 153 с.

Сведения об авторах

Меньших Татьяна Валерьевна, кандидат технических наук, старший преподаватель кафедры математики и естественно-научных дисциплин, Воронежского института Федеральной службы исполнения наказаний.

Ворончихин Максим Михайлович, курсант Воронежского института Федеральной службы исполнения наказаний.

**Меняйло Дмитрий Васильевич,
Барсова Екатерина Руслановна**

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ЕГО ПРИМЕНЕНИЕ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИКОВ

Незаконный оборот наркотических средств на протяжении многих лет остаётся одним из самых серьёзных вызовов международному сообществу. Особую опасность на сегодняшний день представляет сращивание наркопреступности с терроризмом и трансграничной организованной преступностью.

Примечательно, что наркопреступность в современное время неотъемлемо связана с информационно-телекоммуникационной средой Интернет, формируется глобальный наркорынок, что непосредственно влияет на высокую латентность таких преступлений. Технологическая база наркоторговли развивается, нередко преступниками являются опытные программисты, совершенствующие механизм совершения наркопреступлений [4, 5].

Безусловно, вышеуказанные факторы не могли не повлиять на наркоситуацию в Российской Федерации, а также на уровне мирового сообщества. Согласно докладу ООН о наркотиках за 2022 год, в мире насчитывается около 284 млн. человек в возрасте от 15 до 64 лет, которые употребляли наркотические вещества. Данный показатель на 26% превышает показатели прошлого десятилетия [2]. При этом по данным проекта «Трезвая Россия», наркоситуация в нашей стране также не может не вызывать опасений – в 2023 году около 6 млн. человек имеют пристрастие к наркотическим веществам, что составляет 3,5% от численности населения страны [6].

Большая часть преступлений в области незаконного оборота наркотических средств осуществляется посредством использования Интернет-пространства. Бесконтактный и анонимный наркорынок обеспечивают различные нелегальные Интернет-площадки, к которым можно отнести, к примеру, Hydra, LegalRC и другие, так и современные программы мгновенного обмена сообщениями (Telegram, WickrMe, Jabber, Signal, I MO и прочие), а также коммуникационные технологии (VPN, системы прокси-серверов для

обеспечения анонимного сетевого соединения, мессенджеры, фотохостинги, онлайн-сервисы обмена цифровых валют и «биткойн-миксеры», программы определения географических координат).

Кроме того, наряду с вышеперечисленными онлайн-площадками существует так называемая сеть тёмного Интернета DarkNet, в которую можно попасть при помощи особого прокси-сервиса (к примеру, посредством сети Тор и Тор Браузер). Данная сеть обеспечивает конфиденциальность своих пользователей, что безусловно, привлекает продавцов и покупателей запрещённых веществ.

Наконец, скрыть факт купли-продажи наркотических веществ преступникам помогает система электронной оплаты, благодаря которой действия покупателей и продавцов достаточно тяжело отследить.

Таким образом, правоохранительные органы в современное время столкнулись с тяжёлой задачей, ведь, как уже было отмечено, выявить наркопреступность в сети Интернет – трудновыполнимая задача. Тем не менее, технологический прогресс сотрудников правоохранительных органов находится в постоянном развитии. На сегодняшний день в распоряжении сотрудников находятся различные онлайн-платформы, благодаря которым правоохранители предупреждают и выявляют наркопреступления. Перечислим наиболее распространённые платформы, находящиеся в арсенале у сотрудников ОВД и способствующие эффективному раскрытию преступлений в сфере незаконного оборота наркотиков.

Программное обеспечение «*Крибрум*» – платформа, предназначенная для сбора, обработки и анализа информации, поступающей в сеть Интернет. Название программного обеспечения означает «решето» не случайно, ведь с помощью данной программы сотрудникам полиции удастся использовать закрытые алгоритмы для сбора и анализа соответствующих лингвистических моделей, тем самым «фильтруя» информацию в социальных сетях в целях обнаружения запрещенного контента и других полезных данных.



Рис. 1. Схема действия программного обеспечения «Крибрум»

Сеть прошла необходимые испытания и уже стала частью работы правоохранительных органов. В 2022 году создатели Крибрума получили грант на сумму более 82 млн. рублей (общая стоимость проекта превышает 162 млн. рублей). В 2024 году предполагается завершение испытаний усовершенствованной системы «Крибрум. OSINT», которая будет использовать различного рода информацию – почтовые адреса, денежные переводы, номера телефонов, наименования организаций и многое другое. Причём представленная информация может быть использована в слабоструктурированном виде (в форме архива или массива фотографий и т.д.) [1].

Похожие функции на сегодняшний день осуществляет онлайн-платформа «Демон Лапласа», которая позволяет реализовать поиск запрещённой информации в открытых источниках социальных сетей, СМИ, выявлять подозрительные аккаунты и контент, который ими распространяется.

Смежные функции узконаправленного действия осуществляет программа «Insider Telegram», благодаря которой оперативные и иные уполномоченные подразделения ОВД выявляют запрещённые для распространения сведения в Телеграмме. Актуальность и эффективность системы на сегодняшний день не

имеет однозначного подтверждения и нуждается в совершенствовании, однако при должном уровне развития позволит оптимизировать работу по выявлению фактов купли-продажи наркотиков в закрытых сообществах [3].

Система «Шерлок», являющаяся информационно-поисковой платформой, необходимой для мониторинга и анализа социальных сетей.

Наконец, к системам, предназначенным для противодействия преступлениям, совершаемым в онлайн-пространстве (в частности, в области незаконного оборота наркотиков) можно отнести ЦИСМ – Центр изучения и сетевого мониторинга молодёжной среды – ИТ-программы, созданной в 2018 году по инициативе Президента Российской Федерации [7]. Сущность данной системы заключается в использовании в работе правоохранительных органов, иных специализированных органов и служб современных ИТ-решений для выявления информации в Интернет-пространстве, негативно влияющей на молодёжь. К примеру, в область мониторинга попадает информация, способствующая вовлечению детей и подростков в совершение противоправных деяний; информация суицидальной направленности, а также иной контент деструктивной направленности.

Таким образом, сотрудники правоохранительных органов осуществляют активную деятельность по выявлению преступлений в сфере незаконного оборота наркотических средств в сети Интернет посредством специализированного программного обеспечения. Дальнейшее развитие технологического потенциала сотрудников ОВД станет важным шагом к предупреждению и пресечению наркопреступлений, которые на протяжении многих лет являются острой проблемой международного сообщества.

Литература

1. АО «Крибрум» [Электронный ресурс] // Режим доступа: URL: <https://www.kribrum.ru/> (дата обращения: 08.12.2023).
2. ВЦИОМ. Наркотическая зависимость: мониторинг [Электронный ресурс] // Режим доступа: URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/narkoticheskaja-zavisimost-monitoring> (дата обращения: 04.12.2023).

3. Кубасов И.А., Лекарь Л.А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. №3 (67). URL: <https://cyberleninka.ru/article/n/vnedrenie-perspektivnyh-sistem-monitoringa-i-analiza-bolshih-dannyh-poluchennyh-v-seti-internet-dlya-obespecheniya-deyatelnosti> (дата обращения: 06.12.2023).

4. Меняйло, Д.В. Использование информационных технологий при профилактике наркомании / Д.В. Меняйло, А.Ф. Семенюк // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 5-й Международной научно-практической конференции, Белгород, 12 октября 2018 г. – Белгород, 2019. – С. 153-156.

5. Меняйло, Д.В. Противодействие органов внутренних дел наркотизации в России / Д.В. Меняйло, Л.Н. Меняйло, К.В. Никитина // Уголовно-исполнительная система: реалии и перспективы развития: Материалы III Международной научно-практической конференции, Псков, 15 июня 2021 г. – Псков, 2021. – С. 299-303.

6. Наркомания в России 2023 [Электронный ресурс] // Режим доступа: URL: <https://kas.clinic/blog/narkomaniya-v-rossii/#:~:text=> (дата обращения: 04.12.2023).

7. О компании «ЦИСМ» [Электронный ресурс] // Режим доступа: URL: <https://kribrum.ru/company/> (дата обращения: 10.12.2023).

Сведения об авторах

Меняйло Дмитрий Васильевич, кандидат юридических наук, доцент, начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина.

Барсова Екатерина Руслановна, слушатель Белгородского юридического института МВД России имени И.Д. Путилина.

Михайленко Евгений Владимирович

**МЕТОДЫ И ТЕХНОЛОГИИ РАЗРАБОТКИ ПРОГРАММНЫХ
ПРОДУКТОВ ДЛЯ ИСПОЛЬЗОВАНИЯ В УЧЕБНОМ ПРОЦЕССЕ ПО
МАТЕМАТИЧЕСКИМ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИМ
ДИСЦИПЛИНАМ**

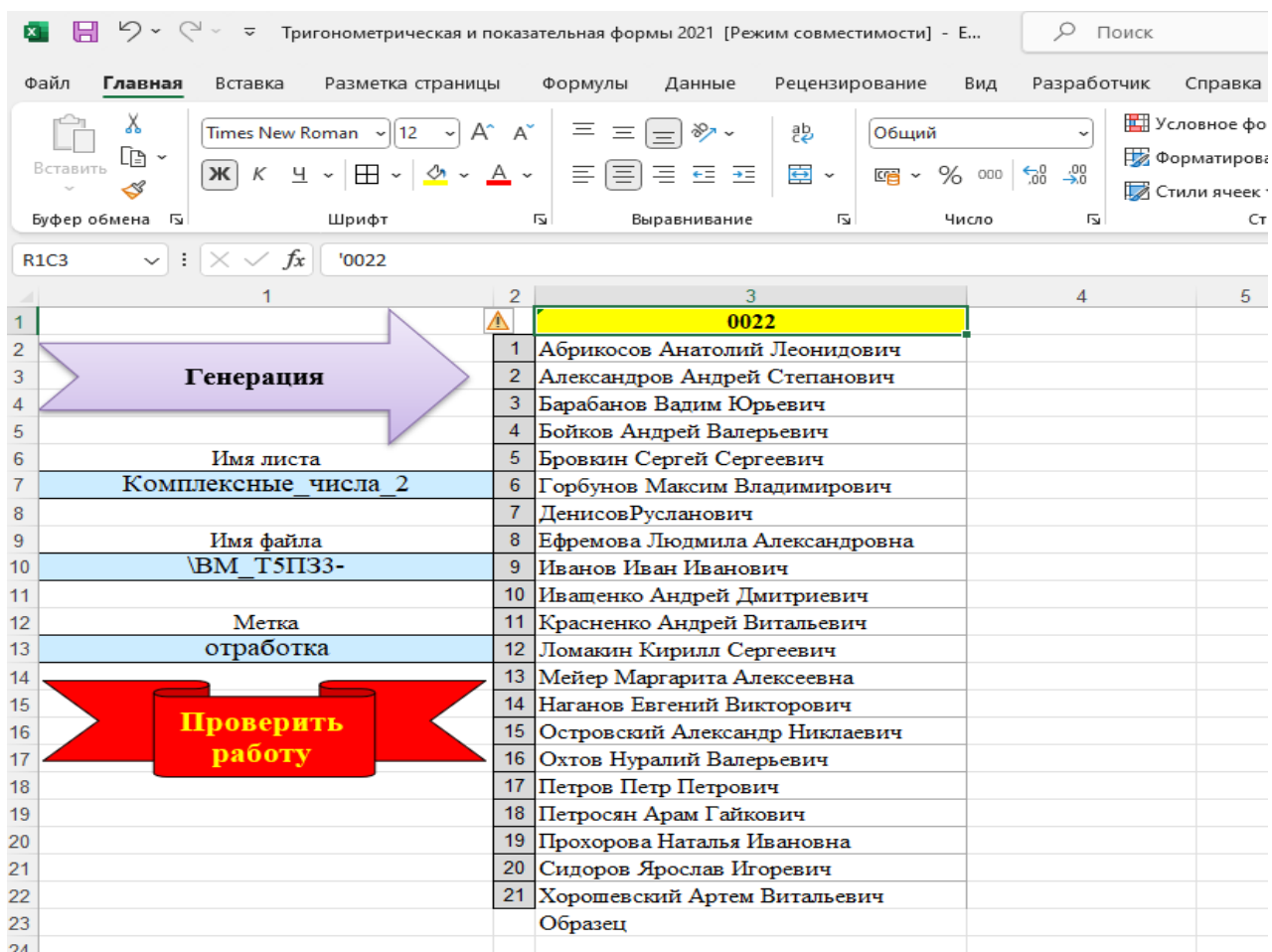
Статья посвящена технологиям разработки программных продуктов для использования в учебном процессе по математическим и информационно-техническим дисциплинам, а также методам верификации выполненных работ. Указанные дисциплины включают такие разделы математики, как линейная алгебра и аналитическая геометрия, общая алгебра, математический анализ, теория вероятностей и математическая статистика, дискретная математика, методы оптимизации. По темам дисциплин предусмотрены расчетные задания, которые выполняются курсантами на практических занятиях и в часы самостоятельной подготовки. Описываемые программные продукты предназначены для избавления преподавателей от трудоемкой работы по подбору типовых задач и проверки их решений на бумажных носителях, кроме того, каждый обучающийся получает свой уникальный вариант заданий, сгенерированных по разработанным алгоритмам, что исключает списывание готовых уже рассчитанных решений курсантов друг у друга [5].

Представляемые комплексы программных продуктов реализованы в среде Microsoft Office, но также при необходимости могут использоваться в офисных приложениях OpenOffice и LibreOffice. Так, при переходе компьютерного центра университета на операционную систему Astra Linux преподаватели продолжали работать на Windows в MS Office, а одновременно с этим обучаемые использовали LibreOffice [3].

Суть описываемого метода заключается в создании шаблонов типовых расчетных заданий, размещенных на листах книг MS Excel, в которые после выполнения макросов будут добавлены сгенерированные числовые, строковые или графические компоненты заданий [1]. Преподаватель может сгенерировать условия

заданий как для одного курсанта, так и одновременно для всей учебной группы. Подготовленные файлы со сгенерированными заданиями помещаются в доступное для обучаемых облачное пространство или папку на сервере, имена файлов содержат номера тем и практических занятий, а также фамилии курсантов. Обучающиеся, выполняя задания, помещают свои решения в поля для ввода числовых или текстовых ответов и предоставляют решенные задания с ответами для проверки. Теперь, получив файлы с решениями, преподавателю достаточно будет обработать их соответствующими макросами, которые автоматически откроют выполненные работы, проверят промежуточные и окончательные решения, а также, согласно установленным критериям, выставят оценки [6, 7].

Рассмотрим структуру описываемых программных продуктов на примере комплекса программ «Тригонометрическая и показательная формы комплексного числа» по теме 5 «Теория множеств».



	1	2	3	4	5
1			0022		
2		1	Абрикосов Анатолий Леонидович		
3		2	Александров Андрей Степанович		
4		3	Барabanов Вадим Юрьевич		
5		4	Бойков Андрей Валерьевич		
6		5	Бровкин Сергей Сергеевич		
7		6	Горбунов Максим Владимирович		
8		7	Денисов Русланович		
9		8	Ефремова Людмила Александровна		
10		9	Иванов Иван Иванович		
11		10	Ивашенко Андрей Дмитриевич		
12		11	Красненко Андрей Витальевич		
13		12	Ломакин Кирилл Сергеевич		
14		13	Мейер Маргарита Алексеевна		
15		14	Наганов Евгений Викторович		
16		15	Островский Александр Николаевич		
17		16	Охтов Нуралий Валерьевич		
18		17	Петров Петр Петрович		
19		18	Петросян Арам Гайкович		
20		19	Прохорова Наталья Ивановна		
21		20	Сидоров Ярослав Игоревич		
22		21	Хорошевский Артем Витальевич		
23			Образец		
24					

Рис. 1. Лист генерации и проверки работ

Каждый программный комплекс состоит из двух листов рабочей книги и комплекта макросов, позволяющих генерировать и проверять практические работы [2]. Первый лист содержит списки курсантов, выполняющих данную работу, описание основных параметров заданий и элементы управления для генерирования и проверки работ (рис. 1). На лист можно поместить одну или несколько учебных групп, здесь преподаватели могут вызывать макросы генерации и проверки работ, указать наименование листа шаблона или изменить имена файлов с заданиями.

Второй лист является шаблоном практического задания (рис. 2). Лист шаблона размечен так, чтобы на нем компактно размещались задания и поля для ответов. Шаблон может быть пустым и не содержать условий предлагаемых задач. В процессе обработки листа все задания будут вновь сгенерированы и помещены в нужные места.

 Комплексные числа Практическое задание Тригонометрическая и показательная формы комплексного числа Вариант 	Дата _____ Время _____ (Фамилия И.О.) _____	
1. Найти значения модулей и аргументов комплексных чисел. $32 - 24i =$ $26i =$ $-14 + 26i =$ $\text{Arg}(10 - 10i) =$ $\text{Arg}(22) =$ $\text{Arg}(-17i) =$		Во всех заданиях в ответах дроби сокращаем ! Аргумент рассчитывается в радианах с использованием
2. Представить комплексные числа в тригонометрической форме. $5 + 12i =$ $13e^{i7\pi/12} =$		тригонометрическая форма 5(cos(arctg4/3) + isin(arctg4/3))
3. Представить комплексные числа в показательной форме. $36 + 27i =$ $10(\cos 7\pi/5 + i \sin 7\pi/5) =$		показательная форма 5e^{i \arctg 4/3} или
4. Представить комплексные числа в алгебраической форме. $20(\cos \pi/2 + i \sin \pi/2) =$ $12e^{i3\pi/2} =$		
5. Найти произведение комплексных чисел. а) $z_1 = 11(\cos 270^\circ + i \sin 270^\circ)$, $z_2 = 4(\cos 180^\circ + i \sin 180^\circ)$ $z_1 z_2 =$ б) $z_1 = 11(\cos 7\pi/4 + i \sin 7\pi/4)$, $z_2 = 9(\cos 3\pi/2 + i \sin 3\pi/2)$ $z_1 z_2 =$ в) $z_1 = 12e^{i5\pi/4}$, $z_2 = 6e^{i11\pi/6}$ $z_1 z_2 =$		Аргумент комплексного числа должен находиться в инт Знак градуса "°" определяется надстрочной латинской б
6. Найти частное комплексных чисел. а) $z_1 = 7(\cos 260^\circ + i \sin 260^\circ)$, $z_2 = 3(\cos 300^\circ + i \sin 300^\circ)$ $z_1/z_2 =$ б) $z_1 = 3(\cos 5\pi/4 + i \sin 5\pi/4)$, $z_2 = 9(\cos 7\pi/4 + i \sin 7\pi/4)$ $z_1/z_2 =$ в) $z_1 = 5e^{i3\pi/8}$, $z_2 = 10e^{i7\pi/8}$ $z_1/z_2 =$		Аргумент комплексного числа должен находиться в инт
7. Возвести комплексное число в указанную степень. а) $z = 2 - 9i$ $z^3 =$ б) $z = 2 + 4i$ $z^4 =$ в) $z = 5(\cos 80^\circ + i \sin 80^\circ)$ $z^6 =$ г) $z = 2(\cos 7\pi/8 + i \sin 7\pi/8)$ $z^7 =$ д) $z = 5e^{i2\pi/5}$ $z^5 =$		Аргумент комплексного числа должен находиться в инт
8. Извлечь квадратные корни из комплексного числа. а) $z = -361$ $z_1 =$ $z_2 =$ б) $z = 529i$ $z_1 =$ $z_2 =$		Решение записать в алгебраической форме Решение записать в тригонометрической форме
9. Извлечь корни 3-ой степени из комплексного числа.		

Рис. 2. Шаблон практического задания

Стандартный программный комплекс содержит также четыре программных модуля для генерирования заданий и проверки выполненных работ.

Модуль процедур и функций разработчика (рис. 3) включает процедуры и функции, использующиеся во всех выполняемых макросах. Состав этого модуля пересекается с аналогичными модулями других программных комплексов, однако здесь находятся и специфические подпрограммы, разработанные специально для изучаемой темы.

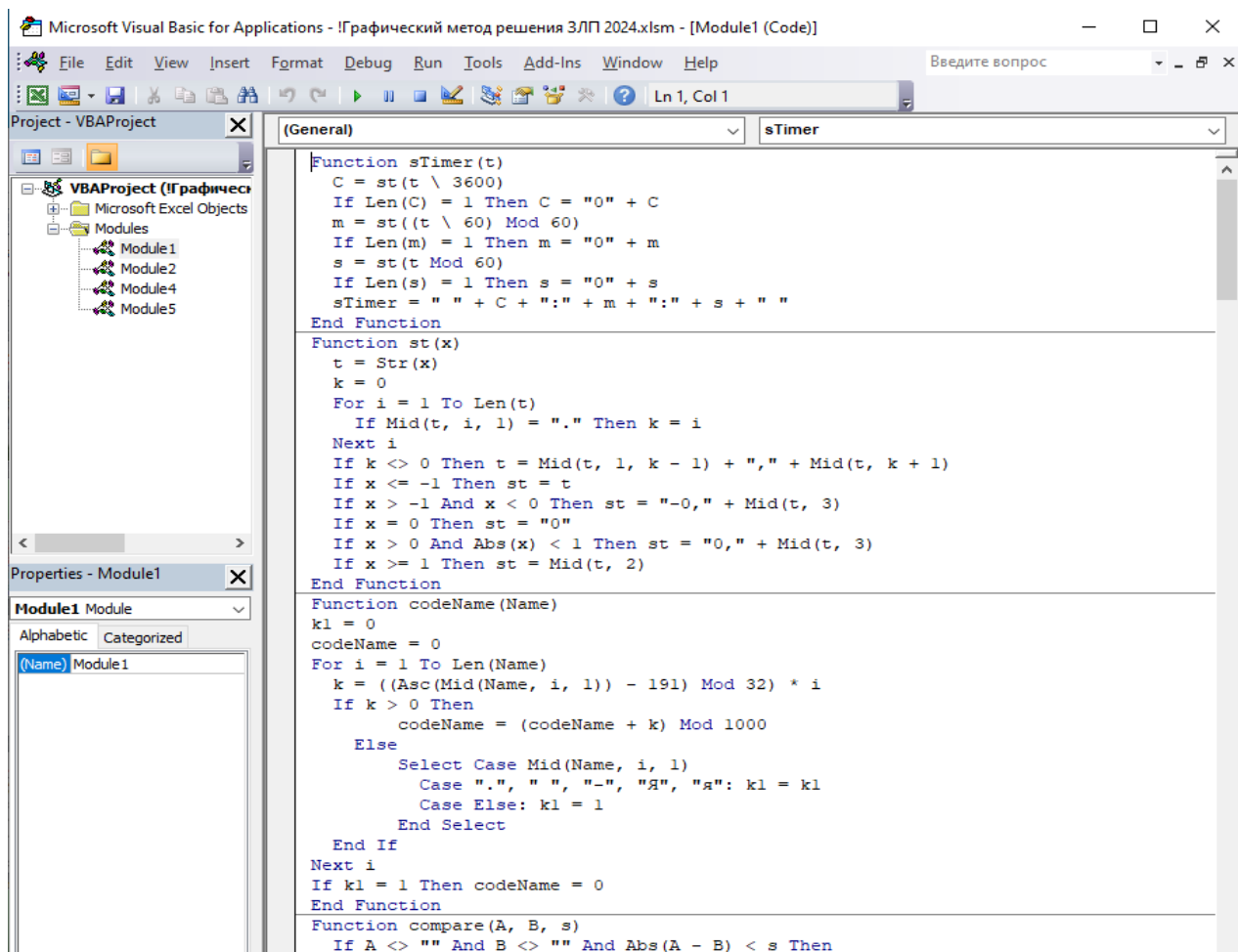


Рис. 3. Модуль процедур и функций разработчика

Модуль запуска предназначен для копирования файлов с формой для размещения на нем заданий. В зависимости от положения активной ячейки листа «Генерация» создается один или группа новых файлов для размещения в них шаблона и заполнения формы сгенерированными данными. На рисунке 4

представлен фрагмент макроса Запуск, реализующий создание новых листов, помещения на них формы, вызов модуля генерации, определения имен файлов, сохранение файлов.

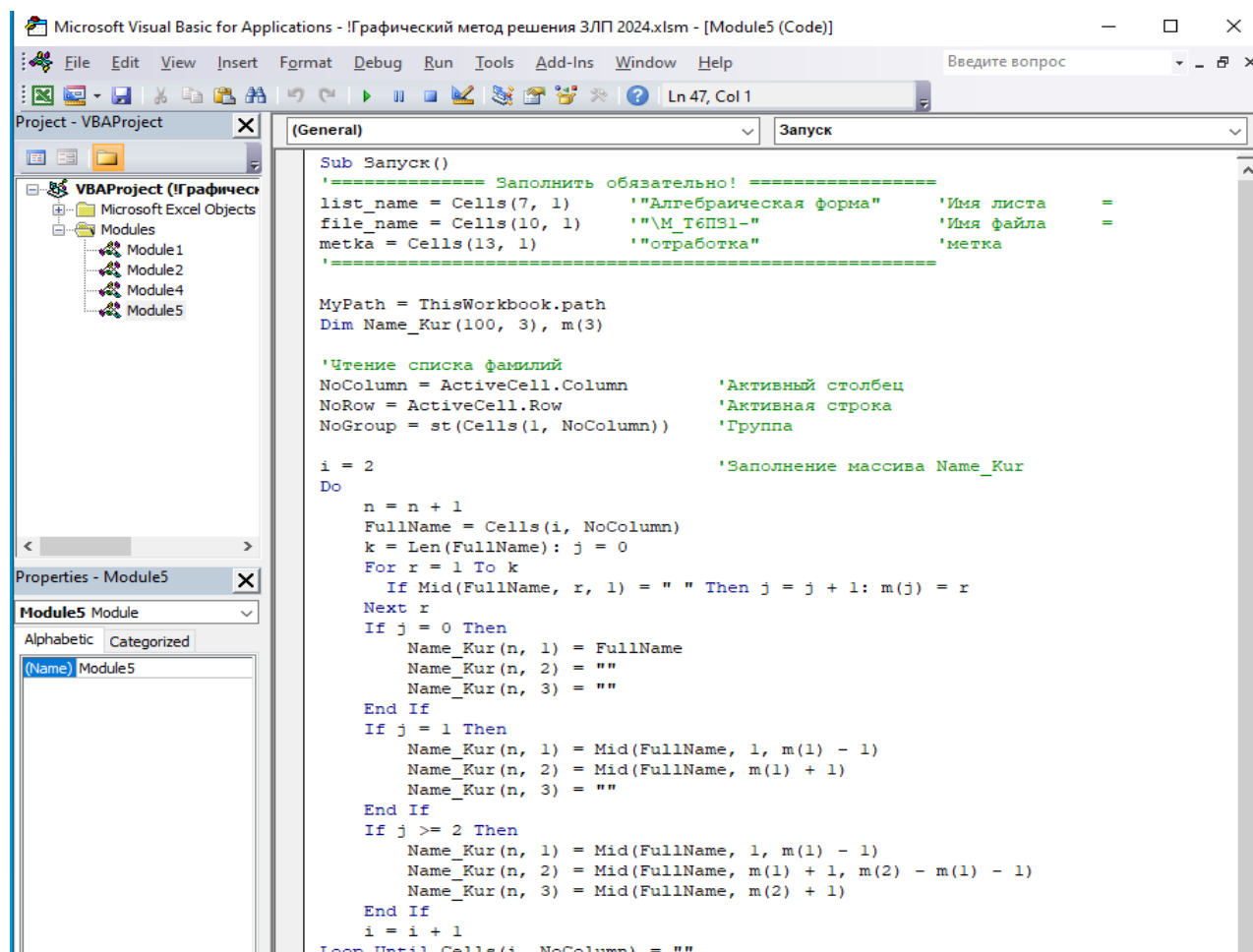


Рис. 4. Модуль запуска

Модуль генерирования заданий содержит макросы, генерирующие условия практических заданий и заполнения скопированных шаблонов полученными данными. В макросе Формы_комплексного_числа с использованием системного времени и имени обучаемого рассчитывается вариант работы и осуществляется инициализация генератора псевдослучайных чисел (рис. 5). Всем заданиям работы соответствуют отдельные процедуры, вызываемые из макроса поочередно.

Модуль проверки выполненных работ включает ряд программ для поиска файлов с выполненными заданиями, повторной генерации заданий, проверки

ответов и выставления оценок. Основной программой четвертого модуля является макрос Найти_файл (рис. 6).

Выбор и открытие проверяемого файла с решениями организовано с помощью метода GetOpenFilename, затем вызывается организационный макрос проверки, файл сохраняется под новым именем, к имени добавляется полученная оценка, а проверяемый старый файл удаляется.

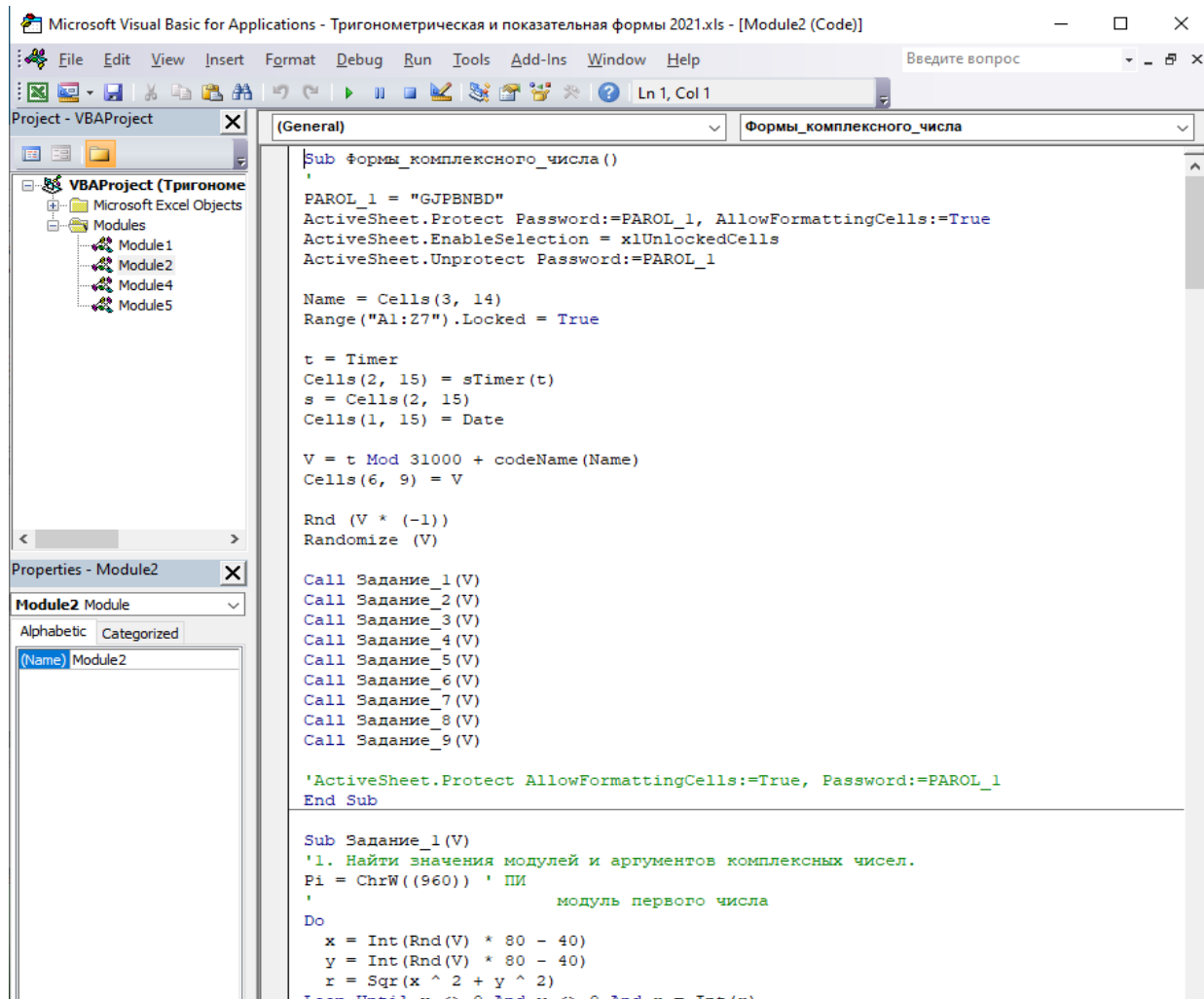


Рис. 5. Модуль генерирования заданий

Макрос проверки PR_Complex_Number_Forms предназначен для вызова процедур проверки. Здесь производится верификация работы: проверяются на соответствие номер варианта, дата и время генерации работы и идентификатора пользователя. Использование функции Randomize обязательно для получения такой же, как и при генерации, последовательности параметров заданий. Здесь, как и в макросе Формы_комплексного_числа, в том же порядке поочередно

используются алгоритмы генерации параметров заданий, далее по ним рассчитываются решения задач для сравнения с введенными ответами курсантов. В завершении проверки рассчитывается оценка.

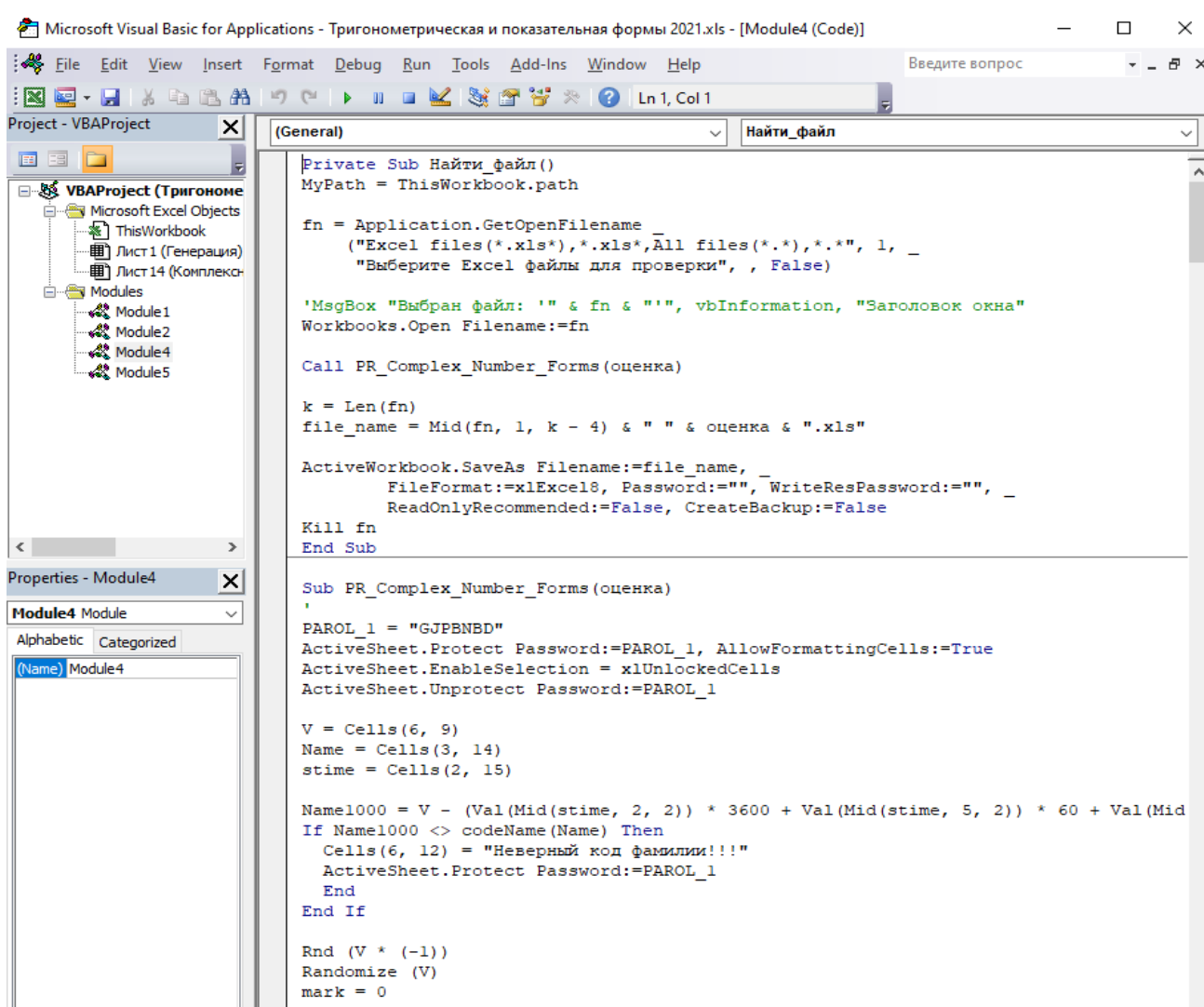


Рис. 6. Модули проверки выполненных работ

Рассмотрим технологии генерации и проверки работ на примере задания «9. Извлечь корни 3-ой степени из комплексного числа» рассматриваемого программного комплекса (рис. 7).

В задании 9.а с помощью генератора псевдослучайных чисел генерируется только одно целочисленное значение x . Затем формируется значение строковой переменной t , в которое входит x уже в третьей степени. И, наконец, ячейке, находящейся на пересечении 50-й строки и первого столбца присваивается значение сгенерированного выражения.

Properties - Module2

Module2 Module

Alphabetic Categorized

(Name) Module2

```

Sub Задание_9 (V)
'9. Извлечь корни 3-ей степени из комплексного числа.
Pi = ChrW((960)) ' ПИ

'a
x = Int(Rnd(V) * 6 + 4)
t = "a) z = " + st(x ^ 3)
Cells(50, 1) = t

'б
Do
r = (Int(Rnd(V) * 4 + 2)) ^ 3
f1 = Int(Rnd(V) * 7 + 2)
f2 = Int(Rnd(V) * 4 + 2): If f2 = 5 Then f2 = 6
Loop Until НОД(f1, f2) = 1 And f1 / f2 < 2 And НОД(f1, 3) = 1
t = "б) z = " + st(r) + "(cos" + st(f1) + Pi + "/" + st(f2) + " + i"
k = Len(t)
t = t + "sin" + st(f1) + Pi + "/" + st(f2) + ")"

Cells(54, 1) = t
Cells(54, 1).Font.FontStyle = "обычный"
Cells(54, 1).Characters(Start:=k, Length:=1).Font.FontStyle = "курсив"

End Sub

```

49 **9. Извлечь корни 3-ей степени из комплексного числа.**

50 а) $z = 216$ $z_1 =$ **Решение :**

52 $z_2 =$ $z_3 =$

54 б) $z = 8(\cos 5\pi/4 + i \sin 5\pi/4)$ $z_1 =$ **Решение :**

56 $z_2 =$ $z_3 =$

58 **Критерий оценки:**

59 31-33 баллов - "отлично"

60 24-31 баллов - "хорошо"

61 18-23 баллов - "удовлетворительно"

62 менее 18 баллов - "неудовлетворительно"

Количество набранных баллов: _____

Оценка за работу: _____

Рис. 7. Задание «9. Извлечь корни 3-ей степени из комплексного числа»

Особенность задания 9.б состоит в том, что генерируемое число представляется в тригонометрической форме и для его вывода потребуется рассчитать модуль r , а также параметры аргумента f_1 и f_2 . Кроме того, число i выделяется курсивом.

При проверке задания не нужно анализировать находящееся на листе задание, это может быть ненадежно и трудоемко. Для получения значений переменных x , r , f_1 и f_2 достаточно еще раз использовать алгоритмы, используемые при генерации задания (рис. 8) [4]. Решения рассматриваемых заданий можно найти при помощи формулы Муавра, а затем сравнить их с ответами на листе, предварительно убрав из них пробелы. Если решение курсанта совпало с расчетным, то количество набранных баллов увеличивается на единицу, в противном случае проверяемая область перечеркивается.

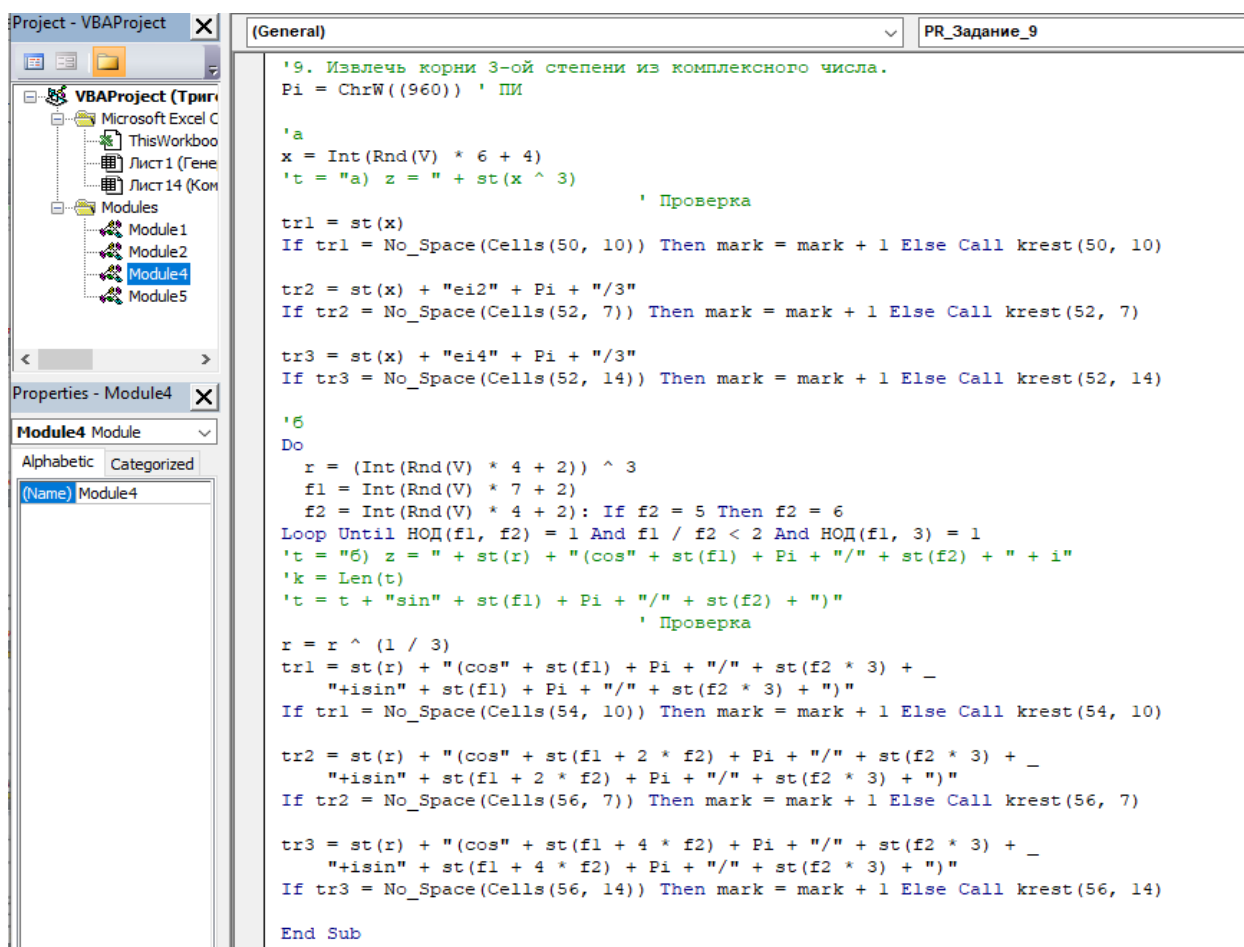


Рис. 8. Фрагмент программного кода задания «9. Извлечь корни 3-ой степени из комплексного числа»

На рисунке 9 показан результат проверки задания. Пять заданий выполнены верно, за них обучаемый получил 5 баллов, неверное выполненное задание перечеркнуто.

Сейчас мы рассмотрели достаточно простой пример генерирования и проверки заданий. На практике часто бывает недостаточно производить операции с отдельными переменными, в этом случае все действия выполняются с использованием массивов различной размерности, созданных графических объектов.

В заключении отметим, что в настоящее время на кафедре информатики и математики Краснодарского университета МВД России разработаны свыше ста приложений по разделам изучаемых дисциплин: математики, высшей математики, численных методов, информационно-технических дисциплин и

программирования. Все они внедрены в образовательный процесс на практических занятиях и в часы самостоятельной подготовки.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	Комплексные числа												Дата 08.11.2023													
2	Практическое задание												Время 13:38:20													
3	Тригонометрическая и показательная												Яковенко Д.С.													
4	формы комплексного числа												(Фамилия И.О.)													
6	Вариант												18756													
28	6. Найти частное комплексных чисел.																									
29	а) $z_1 = 11(\cos 160^\circ + i \sin 160^\circ)$, $z_2 = 5(\cos 320^\circ + i \sin 320^\circ)$												$z_1/z_2 = \frac{11}{5}(\cos 200^\circ + i \sin 200^\circ)$													
31	б) $z_1 = 2(\cos 5\pi/8 + i \sin 5\pi/8)$, $z_2 = 5(\cos 7\pi/4 + i \sin 7\pi/4)$												$z_1/z_2 = \frac{2}{5}(\cos 7\pi/8 + i \sin 7\pi/8)$													
33	в) $z_1 = 10e^{i5\pi/8}$, $z_2 = 9e^{i7\pi/6}$												~~$z_1/z_2 = \frac{10}{9}e^{i70\pi/4}$~~													
35	7. Возвести комплексное число в указанную степень.																									
36	а) $z = 6 - 3i$												~~$z^3 = -54 - 360i$~~													
38	б) $z = 5 + 3i$												$z^4 = -644 + 960i$													
40	в) $z = 2(\cos 70^\circ + i \sin 70^\circ)$												$z^5 = 32(\cos 350^\circ + i \sin 350^\circ)$													
42	г) $z = 2(\cos 5\pi/3 + i \sin 5\pi/3)$												$z^6 = 64(\cos 0 + i \sin 0)$													
44	д) $z = 5e^{i7\pi/4}$												$z^7 = 78125e^{i49\pi/4}$													
44	8. Извлечь квадратные корни из комплексного числа.																									
45	а) $z = -196$												$z_1 = -14i$, $z_2 = 14i$													
47	б) $z = 729i$												$z_1 = 27(\cos \pi/4 + i \sin \pi/4)$, $z_2 = 27(\cos 5\pi/4 + i \sin 5\pi/4)$													
49	9. Извлечь корни 3-ой степени из комплексного числа.																									
50	а) $z = 216$												$z_1 = 6$													
52													$z_2 = 6e^{i2\pi/3}$, $z_3 = 6e^{i4\pi/3}$													
54	б) $z = 8(\cos 5\pi/4 + i \sin 5\pi/4)$												$z_1 = 2(\cos 5\pi/12 + i \sin 5\pi/12)$													
56													~~$z_2 = 2(\cos 13\pi/12 + i \sin 13\pi/12)$~~ , $z_3 = 2(\cos 21\pi/12 + i \sin 21\pi/12)$													
58	Критерий оценки:												Количество набранных баллов: 25													
59	31-33 баллов - "отлично"												Оценка за работу: хорошо													
60	24-31 баллов - "хорошо"																									
61	18-23 баллов - "удовлетворительно"																									
62	менее 18 баллов - "неудовлетворительно"																									
63																										

Рис. 9. Результат проверки задания «9. Извлечь корни 3-ой степени из комплексного числа».

Эффективное внедрение описываемых программных комплексов плодотворно влияет на скорость и качество подготовки учебного материала, активизирует процессы мышления, восприятия и усвоения знаний у обучаемых, формирует устойчивые навыки стандартных математических расчетов, побуждает курсантов и слушателей к самостоятельной, творческой работе.

Литература

1. Аршинов, Г.А. О методах и технологиях разработки компьютерных программ для генерации и проверки заданий по математическим дисциплинам / Г.А. Аршинов, В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар:

КубГАУ, 2023. – №09(193). С. 50 – 81. – IDA [article ID]: 1932309008. – Режим доступа: <http://ej.kubagro.ru/2023/09/pdf/08.pdf>, 2 у.п.л.

2. Епифанцева, В.А. Создание электронной библиотечной системы средствами объектно-ориентированного программирования Python / В.А. Епифанцева, С.К. Ефремов, И.С. Нестеренко // Computational Nanotechnology. – 2023. – Т. 10, № 4. – С. 84 – 90.

3. Лаптев, В.Н. О разработке программного комплекса «Графы. Формы и операции» / В.Н. Лаптев, Е.В. Михайленко, А.Н. Прокопенко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2022. – №01(175). С. 119 – 135. – IDA [article ID]: 1752201010. – Режим доступа: <http://ej.kubagro.ru/2022/01/pdf/10.pdf>, 1,062 у.п.л.

4. Михайленко, Е.В. О проблемах автоматической генерации, верификации и защиты электронных заданий по разделам математики / Е.В. Михайленко // Информационная безопасность как элемент национальной безопасности: электронный сборник научных статей по итогам всероссийской научно-практической конференции. Нижний Новгород, 31 марта 2023 года / сост.: Крыгин С.В., Н. Новгород: НА МВД России, 2023. – С 153 – 161.

5. Старостенко, И.Н. К вопросу о формировании у обучающихся навыков работы с прикладным программным обеспечением в процессе изучения дисциплин математического цикла / И.Н. Старостенко, А.А. Хромых // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции, Белгород, 17 мая 2019 года. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2019. – С. 73-78.

6. Старостенко, И.Н. Технологии искусственного интеллекта в образовании (на примере персонализированного обучения) / И.Н. Старостенко,

А.А. Хромых // Гуманитарные, социально-экономические и общественные науки. – 2023. – № 7. – С. 94-98.

7. Хромых, А.А. Особенности методики преподавания дисциплины «Эконометрика» в Краснодарском университете МВД России / А.А. Хромых, В.А. Епифанцева // Математика и ее приложение в науке и образовании: Материалы Межвузовского научно-методического семинара с международным участием, Санкт-Петербург, 24 мая 2024 года. – Санкт-Петербург: Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева, 2024. – С. 306-310.

Сведения об авторе

Михайленко Евгений Владимирович, кандидат физико-математических наук, заместитель начальника кафедры информатики и математики Краснодарского университета МВД России.

Назаров Артур Карапетович

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ВСТРАИВАЕМЫХ СИСТЕМ

Встраиваемые системы охватывают различные отрасли: финансовый сектор, транспорт и туризм, розничная торговля, ресторанный и гостиничный бизнес, здравоохранение, государственный и некоммерческий сектор, развлечения. На сегодняшний день существует множество встраиваемых систем в виде таких устройств, как банкоматы, билетные автоматы, бензоколонки, кассы, POS-терминалы, медицинское оборудование, игровые автоматы и др.

Несмотря на то, что встраиваемые системы имеют много общего с обычными персональными компьютерами, есть у них и значительные отличия. Особенность таких систем заключается в том, что они, как правило, выполняют однотипные задачи для большого количества пользователей, в отличие от персональных компьютеров, у которых обычно один или несколько пользователей и широкий круг выполняемых задач. Другой отличительной особенностью можно назвать наличие у встраиваемой системы подключение к вычислительной сети. Эти отличия во многом определяют средства и методы защиты встраиваемых систем от имеющихся угроз. Как правило встраиваемые системы хорошо физически защищены от взлома (например, банкоматы), но могут иметь слабую защиту на программном уровне. Достаточно, например, вспомнить ограбление XXI века, когда хакерам из группировки Carbanak удалось похитить в общей сложности порядка миллиарда долларов у десятков банков по всему миру.

Среди основных векторов атак на встраиваемые системы можно выделить следующие:

1. Атаки на физическом уровне. Например, атаки методом «черного ящика», замены панели для ввода ПИН-кода (например, с помощью скиммеров), скрытые камеры, взрывы.

2. Атаки на уровне сети. К примеру, могут быть использованы уязвимости VPN-подключения, АРТ-атаки, удаленная установка.

3. Атаки на уровне программного обеспечения. К этой категории можно отнести локальную и удаленную установку программного обеспечения, атаки на операционные системы, анализаторы памяти (снифферы), заражение или изменение программного обеспечения.

При этом, согласно статистике, более 50% успешных атак на встраиваемые системы проходят при участии сотрудников компаний или сторонних поставщиков услуг.

В качестве примера угроз для встраиваемых систем отметим наличие в современных банкоматах средства считывания QR-кодов. Это средство позволяет преступникам, используя уязвимость в программном обеспечении, вызвать сервисное меню и вывести банкомат из режима киоска. Далее с помощью других QR-кодов преступники, выполняя другие команды, получают более широкие права доступа, а затем выполняют команду для выдачи денег из банкомата.

Другой пример – это атака с «черным ящиком». При такой атаке устанавливается в разрыв одноплатный компьютер размером с банковскую карту (Raspberry Pi). Далее анализируется протокол управления диспенсером и так же, как и выше, подается команда на выдачу денежных средств. Raspberry Pi с эмуляцией клавиатурного ввода может также использоваться для БРУТФОРС-атаки на пароль, что в свою очередь может привести к деактивации защиты.

Особо хочется отметить ошибки системных администраторов, например, наличие ненужных привилегий аккаунта пользователя, наличие незаблокированных сочетаний клавиш, незаблокированной экранной клавиатуры, незаблокированных функций и т.д.

Встраиваемые системы как правило используют устаревшее программное обеспечение. Многие встраиваемые системы работают на базе устаревших, уязвимых операционных систем, несовместимых с большинством современных защитных решений. Они имеют слабое аппаратное обеспечение. При этом невозможно защитить маломощные устройства с помощью обычных

инструментов для защиты рабочих мест без существенного снижения их производительности. Встраиваемые системы как правило оснащены слабым каналом связи. Низкая скорость передачи данных или нестабильное подключение к сети ограничивают возможности защиты и управления. Встраиваемые системы обычно размещаются в общественных местах. Многие встраиваемые системы расположены в удаленных районах и общественных местах, что повышает риск физической атаки и ограничивает возможности обслуживания. Все это приводит, в частности, к тому, что использование традиционных средств защиты для них не подходит.

Проводя анализ современных угроз встраиваемых систем важно также отметить тенденцию перехода с операционной системы Windows на операционную систему Linux. В Российской Федерации это особенно актуально. При этом продуктов для защиты новых систем на базе Linux совсем немного.

Таким образом, необходимо учитывать все особенности встраиваемых систем при разработке защитной стратегии, в противном случае существует риск столкнуться с определенными существенными, а иногда и непреодолимыми проблемами.

Литература

1. <https://www.kaspersky.ru>.
2. <https://www.securitylab.ru>.

Сведения об авторе

Назаров Артур Карапетович, кандидат физико-математических наук, старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России.

**Наумова Наталья Александровна,
Иващенко Никита Витальевич,
Орлов Роман Владимирович**

ПРИЛОЖЕНИЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНОВ НА МНОЖИТЕЛИ В ТЕОРИИ КОДИРОВАНИЯ

В последние десятилетия огромное значение на ряд прикладных проблем оказывает высшая алгебра, в частности, теория конечных полей. Особенно значимое приложение алгебраические объекты над конечными полями нашли в теории кодирования. Актуальная проблема в теории кодирования – построение кодов, позволяющих обнаруживать и исправлять искажения, возникающие при передаче данных. А вопрос надежного обмена информацией как никогда актуален в настоящее время.

При построении линейных и циклических кодов, а также в линейных регистрах сдвига нашли свое применение многочлены над конечными полями. Свойства многочленов над конечными полями позволяют максимизировать эффективность компьютерной реализации арифметики в конечных полях. Их криптографические приложения основаны на следующих теоретических проблемах [3]:

- 1) поиск неприводимых многочленов над заданным конечным полем;
- 2) нахождение корней неприводимых многочленов в заданном поле;
- 3) разложение многочлена на неприводимые множители.

Все три задачи взаимосвязаны. Остановимся подробно на каждой из них.

1. Поиск неприводимых многочленов над заданным конечным полем. Неприводимые многочлены малых степеней над конечными полями достаточно легко найти в явном виде опираясь на факториальность евклидовых колец. Например, следуя приведенному ниже алгоритму:

- 1) выписываем множество S_1 всех возможных многочленов данной степени n над данным конечным полем;

2) выписываем множество S_2 всех возможных разложений на множители многочленов данной степени n над данным конечным полем;

3) множество $S_1 \setminus S_2$ – множество всех неприводимых многочленов данной степени n над данным конечным полем.

Например, найдем неприводимые многочлены третьей степени над полем $\mathbb{F}_2$. Исключая делимость на x , получим общий вид; $x^3 + a \cdot x^2 + b \cdot x + 1$.

Теперь исключим наличие корня $x = 1$, то есть делимость на $x + 1$, получаем условие: $a + b = 1$. Отсюда следует, что либо $a = 0$ и $b = 1$, либо $a = 1$ и $b = 0$. Итак, получаем неприводимые многочлены над полем $\mathbb{F}_2$: $x^3 + x^2 + 1$ и $x^3 + x + 1$.

Другой способ синтеза неприводимых многочленов основан на свойствах конечных полей и проводится с помощью примитивных элементов поля.

Разработан ряд алгоритмов проверки данного многочлена на неприводимость. Отметим один, основанный на следующем ключевом утверждении: каждый неприводимый над $GF(p)$ многочлен степени r является делителем двучлена $x^{p^r} - x$.

Кроме того, очевидно, что если многочлен приводим, то один из его неприводимых делителей имеет степень $r \leq [n/2]$.

Отсюда получаем простой тест (не)приводимости: многочлен f приводим, если он не взаимно прост с одним из двучленов $x^{p^r} - x$ при $1 \leq r \leq [n/2]$. В противном случае f неприводим.

2. Нахождение корней неприводимых многочленов в заданном поле. Актуальной задачей является также поиск корней многочленов в заданном расширении некоторого конечного поля. Теоретически это возможно путём построения аффинного кратного [2].

Линеаризованным (q -многочленом) над полем $\mathbb{F}_{q^m}$ называется многочлен следующего вида:

$$L(x) = \sum_{i=0}^n \alpha_i x^{q^i}$$

где α_i - коэффициенты из расширения F_{q^m} простого поля F_q .

Для многочлена такого вида поиск корней сводится к решению однородной системы линейных уравнений, так как данный многочлен можно рассматривать как линейный оператор.

Аффинным q -многочленом над полем F_{q^m} называется многочлен следующего вида:

$$A(x) = L(x) - \alpha = \sum_{i=0}^n \alpha_i x^{q^i} - \alpha$$

где α_i - коэффициенты из расширения F_{q^m} простого поля F_q .

Задача нахождения корней аффинного q -многочлена в некотором расширении F_{q^s} поля его коэффициентов F_{q^m} ($s : m$) сводится к решению неоднородной системы линейных алгебраических уравнений над простым полем F_q .

Можно составить алгоритм (рис.1) нахождения корней произвольного многочлена $f(x) \in F_{q^m}$ степени $n \geq 1$ в заданном поле F_{q^s} .

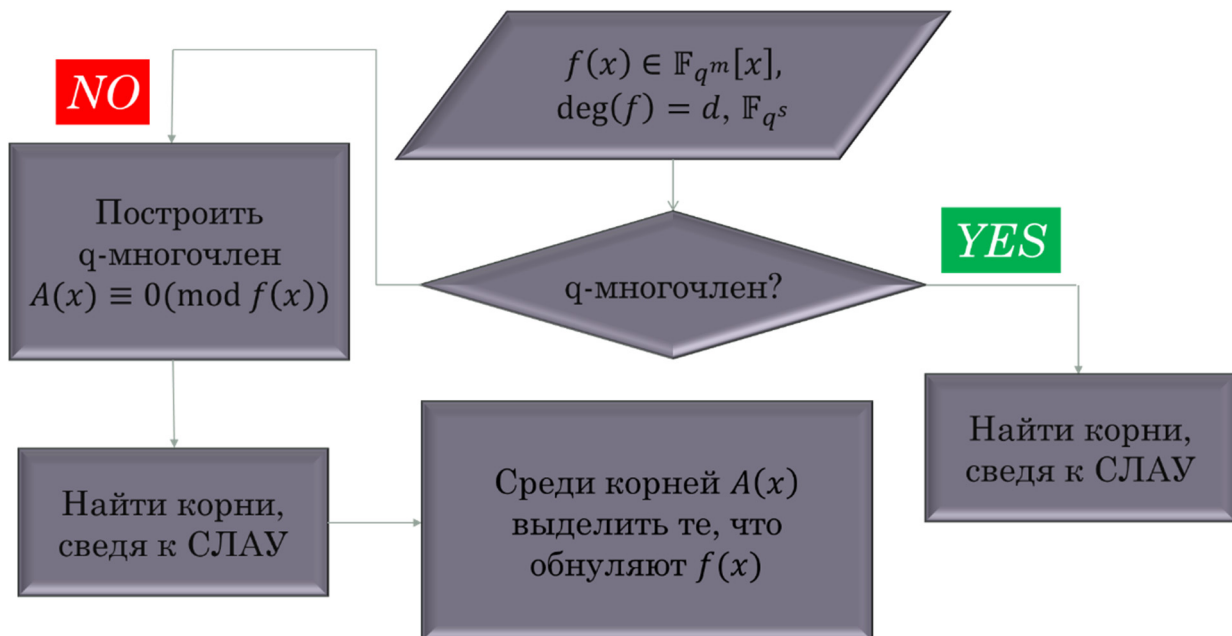


Рис. 1. Алгоритм нахождения корней произвольного многочлена

3. Разложение многочлена на неприводимые множители.

Наиболее эффективен в этом вопросе в настоящий момент алгоритм Берлекемпа. В основе этого метода лежит китайская теорема об остатках для кольца многочленов. На вход алгоритма поступает многочлен $f(x)$, свободный от квадратов:

1) находим матрицу остатков $R = R(f)$;

2) находим базис $B = \{e_1, e_2, \dots, e_k\}$ ортогонального пространства матрицы $R = R(f)$;

3) используя базис, раскладываем $f(x)$ на множители вычислением НОД($f; e_s - a$), где a – элементы поля F_q .

Усовершенствование алгоритма Берлекемпа – это метод Кантора – Цассенхауза. Он позволяет для заданного числа d найти произведение всех неприводимых делителей многочлена $f(x)$ степени d .

4. Приложения в кодировании.

В основу помехоустойчивого кодирования положена следующая идея: перед передачей сообщения к нему добавляют полученную с помощью некоторого алгоритма избыточную информацию, которая позволяет принимающей стороне обнаружить и устранить возникшие искажения [3]. С помощью многочленов проводится построение, например, циклических кодов. В качестве порождающего код многочлена берется любой делитель $g(x)$ бинома $x^n - 1$. Многочлен $g(x)$ полностью задаёт циклический код, его называют также генератором; $\deg g(x) = m < n$.

Несистематическое кодирование осуществляется путём умножения кодируемого полинома на порождающий: $u(x) \mapsto g(x) \cdot u(x) \in C$.

Систематическое кодирование осуществляется приписыванием к кодовому слову слева (в младшие разряды) остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$. Умножение $u(x)$ на x^m поместит сообщение в старшие разряды n -битового слова.

Коды Бауза – Чоудхури – Хоквингема (БЧХ) – подкласс циклических кодов, исправляющих не менее заранее заданного числа ошибок. Алгоритм построения двоичного кода БЧХ, использующего не менее r ошибок [1]:

- 1) выбираем величину t , определяющую длину кода $n = 2^t - 1 > 2r + 1$;
- 2) выбираем неприводимый полином $\alpha(x)$ степени t и строим расширение поля $\mathbb{F}_2$ как фактор-кольцо $\mathbb{F}_2^t = \mathbb{F}_2[x]/(\alpha(x))$ с примитивным элементом α ;
- 3) находим циклотомические классы поля $\mathbb{F}_2^t$ над $\mathbb{F}_2$, в которые попадают $2r$ нулей кода $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2r}$;
- 4) находим минимальные многочлены $g_1(x), g_2(x), \dots, g_h(x)$ каждого циклотомического класса;
- 5) вычисляем порождающий полином кода $g(x) = g_1(x) \cdot g_2(x) \cdot \dots \cdot g_h(x)$.

Многочлены над конечными полями и, в частности, проблема их разложения на множители, имеют большое прикладное значение в области шифрования и криптографии в настоящий момент. Но несмотря на огромное количество исследований в этой области, для задачи факторизации многочленов большой степени над конечными полями не найдено еще универсального решения.

Литература

1. Гуров С.И. Конечные поля и группы перестановок: приложение в теории кодирования и комбинаторике: учебное пособие. – Изд-во:КДУ, Владос-Пр., 2018. – 190 с.
2. Лиддл Р., Нидеррайтер Г. Конечные поля: в 2-х т. – М.: Книга по требованию, 2013. – 812 с.
3. Применко Э.А. Алгебраические основы криптографии: учебное пособие. – М.: Книжный дом. «Либроком», 2014. – 288 с.

Сведения об авторах

Наумова Наталья Александровна, доктор технических наук, доцент, заведующая кафедрой вычислительной математики и информатики Кубанского государственного университета.

Иващенко Никита Витальевич, студент Кубанского государственного университета.

Орлов Роман Владимирович, студент Кубанского государственного университета.

**Нестеренко Иван Сергеевич,
Арипов Анвар Лутфиллович,
Бровченко Сергей Юрьевич**

TELEGRAM-ПЛАТФОРМА КАК ИНСТРУМЕНТ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПЛЕНИЙ В РАМКАХ ПРАВОВОГО ПРОСВЕЩЕНИЯ НАСЕЛЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ СОВРЕМЕННОГО РОССИЙСКОГО ОБЩЕСТВА

Социальные сети и мессенджеры уже давно вошли обиход в современном обществе. Помимо возможности общения данные платформы позволяют оперативно обмениваться различным объемом информации в разных форматах. Стоит отметить, что социальные сети сильно изменились с момента их создания, активное внедрение новых технологий позволяет превратить рассматриваемы платформы в отдельные информационные пространства, на которых появляется возможность осуществлять денежные транзакции, покупать товары и различные услуги, заниматься бизнесом, играть в компьютерные и мобильные игры, обучаться, а некоторые сервисы даже позволяют следить за здоровьем.

Однако активное развитие возможностей и распространенности социальных сетей и мессенджеров привлекает внимание кибермошенников, которые видят в этом благоприятную среду для осуществления преступной деятельности. Интерес злоумышленников привлекает большое количество пользователей, что обуславливает широкий выбор жертвы, также большую роль играют особенности осуществления преступлений в киберпространстве.

Поэтому использование потенциала социальных сетей и мессенджеров для правового просвещения населения на данный момент имеет важное значение, так как появляется возможность осуществлять цели правового просвещения и одновременно предупреждать преступления, совершаемые в киберпространстве.

Для реализации целей правового просвещения населения хорошо подходит платформа Telegram. На данный момент это приложение позиционируется как кроссплатформенная система мгновенного обмена сообщениями, иначе говоря мессенджер, с возможностью предоставления информации в текстовой,

графической, звуковой форме. Функционал данного мессенджера позволяет пользователю обмениваться, помимо привычных текстовых сообщений, голосовыми и видеосообщениями, стикерами и фотографиями, а также файлами многих форматов.

Определяющим значение использования в процессе правового просвещения рассматриваемого мессенджера является одна из форм коммуникации, которую предоставляет Telegram. Речь идет о telegram-каналах, позволяющие:

- делиться информацией с неограниченным или ограниченным кругом лиц, используя для этого публичные или частные каналы;
- оставаться их создателям и абонентам анонимными, информация о участниках канала будет доступна только его администратору;
- ограничить обратную связь, посредством отсутствия возможности у пользователей возможности делиться своим мнением непосредственно в ленте канала, для этого им может быть предоставлен отдельный канал для обсуждений или возможность обсуждать только конкретно определенный пост.

Эти характеристики telegram-каналов позволяют эффективно использовать данный мессенджер как инструмент правового просвещения.

Важно отметить, для успешного правового просвещения населения необходимо использовать современные виды предоставления профилактической информации, так как это вызывает большую заинтересованность у людей, за счет предоставления информации в формах, с которыми они постоянно встречаются, являющиеся для них уже привычными. Также стоит обратить внимание на статистические показатели киберпреступности в нашей стране. По данным МВД России темп роста зарегистрированных преступлений, совершаемых с использованием в информационно-телекоммуникационных технологи, замедлился за последние несколько лет. Так 2021 году их количество выросло незначительно на 1,4% и в последующие годы наблюдается данная тенденция небольшого прироста. На наш взгляд именно своевременное информирование

населения посредством платформы Telegram могло привести к положительным результатам профилактики преступлений, совершаемых с использованием в информационно-телекоммуникационных технологий.

Из выше сказанного можно сделать вывод, что в вопросе правового просвещения населения по вопросам профилактики кибермошенничества Telegram выступает как качественный и эффективный инструмент, использование которого определяет актуальность использования данного мессенджера и функционал, который он может предоставить.

Практической частью данной работы является разработка примера telegram-канала с профилактической информацией, направленной на правовое просвещение населения в вопросе профилактики кибермошенничества.

Выбор данного мессенджера, как уже отмечалось выше, обуславливается:

- 1) широкой востребованностью использования данного мессенджера среди пользователей;
- 2) разнообразным функционалом платформы, позволяющим предоставлять профилактическую информацию в различных формах;
- 3) возможностью создателям канала оставаться анонимными;
- 4) распространением информации на неограниченный или ограниченный круг лиц.

Канал создан для того, чтобы показать, каким образом можно осуществлять правовое воспитание населения посредством мессенджера Telegram, профилактическую информацию, которая может быть донесена до сведения пользователей.

Канал называется: «! Осторожно! Мошенники в сети!». Тип канала; частный. Возможность обсуждать посты и оставлять реакции ограничена для подписчиков канала, также имя администратора канала не отображается в подписях к постам.

В шапке канала закреплён текст: «Данный канал создан с целью профилактики одной из актуальных проблем современной России —

кибермошенничество». Также имеется ссылка-приглашение для присоединения к каналу: <https://t.me/+NJAjNjKDYSUyZmM6>.

В канале предоставляется контент в форме предупредительных изображений, памяток в виде изображений, пост с ссылкой для перехода на сайт с профилактической информацией, пост с ссылкой на публикацию другого канала, содержащей информацию профилактического характера, пост с ссылкой на видеоролик, размещенный в социальной сети, пост с ссылкой на статью.

На канале представлены две памятки, содержащие профилактическую информацию. На первой из них указывается 6 правил информационной безопасности, соблюдение которых позволит не стать жертвой киберпреступников. Памятка разделяется на 6 блоков: надежные пароли, безопасный WI-FI, проверенные браузеры и сайты, безопасность электронной почты, использование приложений, соцсетей и мессенджеров, защита данных банковских карт. К каждому блоку прилагаются соответствующие рекомендации, а также то, что не рекомендуется делать.

Кроме того, на нашем канале показан пост с ссылкой на сайт с профилактической информацией MYFIN.by, где мы сможем ознакомиться со статьей «Под кого чаще всего маскируются кибермошенники», в которой авторы дают рекомендации по поводу того, на что стоит обращать внимание при проведении сделок. Также предупреждают, что, покупая или продавая что-то в интернете, стоит проявлять разумную осторожность и осмотрительность. Также на канале представлен пост с ссылкой на опубликованную статью другим telegram-каналом. В данной статье пользователя предупреждают о том, что необходимо всегда ознакомиться с пользовательским соглашением в интернете прежде, чем его принять. Далее можно ознакомиться с ссылкой на видеоролик, который размещен в социальной сети «ВКонтакте». В данном видеоролике доводится профилактическая информация по безопасности в интернете, при этом форма подачи информации рассчитана на детскую аудиторию. Вся информация сопровождается анимированными зарисовками, а также

пояснениями от представителя «Национального центра помощи детям». Также представлен нами пост ссылкой на статью, в которой рассказывается про приложения, которые позволят пользователю защитить конфиденциальную информацию на своем устройстве, избежать нежелательного прослушивания разговоров, воспрепятствовать шпионским программам и вирусам получить доступ к видеокамере устройства и прочее.

Данная разработка может послужить примером того, как может быть реализовано направления правового просвещения в вопросе профилактики кибермошенничества используя потенциал мессенджера Telegram, также активное научное исследования данного вопроса позволит создавать профилактический контент для размещения в каналах, созданных непосредственно с целью информирования пользователей по вопросам правового просвещения.

Подводя итог, можно отметить, что развитие информационных технологий закономерно ведет и к развитию возможностей киберпреступников, поэтому для борьбы с ними нужно активно изучать дынные технологии, чтобы разработать эффективные методы и средства, которые способны будут дать правоохранительным органам возможность противостоять новому виду преступности на должном уровне.

Литература

1. Андреева Е.Е., Морозов Г.Б. Об эффективных формах правового просвещения граждан Российской Федерации // Педагогическое образование в России. – 2016. - № 1. -С. 75-81.

2. Аршинов Г.А. О методах и технологиях разработки компьютерных программ для генерации и проверки заданий по математическим дисциплинам / Г.А. Аршинов, В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2023. – №09(193). С. 50 – 81

3. Богданов А.В., Ильинский И.И., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. – 2020. - № 1. - С. 15-20

4. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – №. 24. - С. 45-55.

5. Мяханова А.Н. К вопросу об использовании Telegram-каналов как инструмента профилактики правонарушений / А. Н. Мяханова, Ж. П. Гунзынов // Уголовно-исполнительное право. – 2019. – Т. 14(1–4), № 4. – С. 390–393.

6. Состояние преступности в России за 2022-2024 года // МВД России, ФКУ «Главный информационно-аналитический центр». – М., 2022. – С. 67.

Сведения об авторах

Нестеренко Иван Сергеевич, кандидат педагогических наук, доцент кафедры информатики и математики Краснодарского университета МВД России.

Арипов Анвар Лутфиллоевич, кандидат юридических наук, начальник кафедры информационной безопасности и цифровых технологий факультета № 5 Академии МВД Республики Таджикистан.

Бровченко Сергей Юрьевич, курсант 5 курса факультета по подготовке специалистов для подразделений полиции Краснодарского университета МВД России.

Никифорова Лариса Владимировна

МОДЕЛИРОВАНИЕ ПЕРИОДИЧЕСКОЙ СИСТЕМЫ УПРАВЛЕНИЯ СТРУКТУРНО НЕОПРЕДЕЛЕННЫМ ОБЪЕКТОМ С ЗАПАЗДЫВАНИЯМИ

В статье предпринимается попытка решения одной из актуальных задач современной теории управления – моделирование периодической системы управления сложными динамическими объектами с запаздываниями различных типов. Такие системы широко встречаются в самых разных областях науки и техники, что делает задачу их эффективного управления крайне востребованной. Рассматриваемый в работе случай действительно является одним из наиболее сложных – структурно и параметрически априорно-неопределенный объект с запаздываниями нейтрального типа и по управлению, в котором прямым измерениям доступен только скалярный выход. Наличие запаздываний различной природы значительно усложняет синтез законов управления из-за необходимости компенсации их негативного влияния на динамику системы. Параметрическая и структурная неопределенности также вносят свои трудности. Для решения такого рода задач необходим комплексный подход, сочетающий методы теории управления, робастных и адаптивных систем, наблюдателей состояния с привлечением современного математического аппарата.

Математическая модель исследуемой системы

Рассмотрим объект с указанными типами запаздываний:

$$\frac{dx(t)}{dt} = A_0 x(t) + D x(t - \tau_1) + \Gamma_0 \frac{dx(t - \tau_2)}{dt} + B(u(t - h) + f(t)), \quad (1)$$

$$y(t) = L^T x(t),$$

$$x(0) = x_0, \quad x(\zeta) = \phi(\zeta), \quad \zeta \in [-\tau_1, 0], \quad \frac{dx(\zeta)}{d\zeta} = \frac{d\vartheta(\zeta)}{d\zeta}, \quad \zeta \in [-\tau_2, 0],$$

$$u(\zeta) = v(\zeta), \quad \zeta \in [-h, 0]$$

где $x(t) \in R^n$ – вектор состояния; A_0 – произвольная матрица состояния в форме Фробениуса размерности $n \times n$; D, Γ_0 – матрицы размерности $n \times n$, все элементы

которых нули, кроме последней строки; собственные значения матрицы Γ_0 неизвестны, но принадлежат кругу единичного радиуса; $B = [0, \dots, 0, 1]^T$ – вектор размерности n ; $u(t) \in R$ – управляющее воздействие, $\tau_1, \tau_2, h = \text{const} > 0$ – известные постоянные запаздывания; $f(t) = f(t + T) \in R$ – постоянно действующая периодическая неконтролируемая внешняя помеха, которая является ограниченной $|f(t)| \leq f_0, f_0 = \text{const} \geq 0$ – неизвестная постоянная величина, $T = \text{const}$ – период; L^T – вектор выхода размера n , компоненты вектора L могут быть нулевыми (кроме первого) и ненулевыми; $y(t) \in R$ – измеряемый выход объекта; x_0 – начальные условия, $\phi(\xi), \mathcal{A}(\xi), \mathcal{U}(\xi)$ – ограниченные непрерывные начальные соответственно вектор-функции и скалярная функция.

Объект управления (1) функционирует в условиях априорной параметрической неопределенности

$$A_0 = A_0(\xi), D = D(\xi), \Gamma_0 = \Gamma_0(\xi), L = L(\xi), f(t) = f_\xi(t), \quad (2)$$

где $\xi \in \Xi$, ξ – набор неизвестных параметров принадлежащих известному ограниченному множеству Ξ .

Следуя [1], можно заменить

$$\frac{dx(t - \tau_2)}{dt} = \tau_2^{-1} (x(t) - x(t - \tau_2)) + \phi(t). \quad (3)$$

Если $\frac{dx(t - \tau_2)}{dt}$ удовлетворяет условию Липшица с постоянной α , $0 < \tau_2 \leq \tau_1$,

$\|\phi(t)\| \leq \alpha \tau_2$, $\bar{\phi}(t) = \Gamma_0 \phi(t)$. Из ограниченности $\phi(t)$ следует ограниченность $\bar{\phi}(t)$.

Введем следующие обозначения:

$$A = A_0 + \tau_2^{-1} \Gamma, \Gamma = -\tau_2^{-1} \Gamma_0, \bar{f}(t) = f(t) + \bar{\phi}(t).$$

Тогда уравнение (1) примет вид

$$\frac{dx(t)}{dt} = Ax(t) + Dx(t - \tau_1) + \Gamma x(t - \tau_2) + B(u(t - h) + \bar{f}(t)), y(t) = L^T x(t), \quad (4)$$

Передаточная функция объекта управления (4)

$$W_{OY}(s) = L^T (sE - A - De^{-\tau_1 s} - \Gamma e^{-\tau_2 s})^{-1} B e^{-hs} = \frac{b(s)}{a(s)} e^{-hs},$$

где s – переменная Лапласа, $a(s)$, $b(s)$ – нормированные полиномы, $a(s)$ – произвольный квазиполином, $b(s)$ – гурвицевый полином; $\deg a(s) = n$; степень полинома $b(s)$ изменяется в зависимости от наличия нулевых компонент в L , число которых неизвестно, поэтому $\deg b(s) = m$, $0 \leq m \leq n - 1$.

Движение объекта управления (4) должно выполняться по заданной траектории, уравнение которой (1) задается неявной эталонной моделью

$$\frac{dx_*(t)}{dt} = A_* \cdot x_*(t) + B_* \cdot r(t), \quad y_*(t) = L^T x_*(t), \quad x_*(0) = 0, \quad (5)$$

где $x_*(t) \in \mathbb{R}^n$ – переменные состояния; A_* – гурвицева матрица $n \times n$; $B_* = B\chi_1$, $\chi_1 = \text{const} > 0$ – неизвестная постоянная; $r(t) = r(t + T) \in R$ – периодический заданный сигнал; $y_*(t) \in \mathbb{R}^n$ – выход эталона.

Для объекта управления (4) и эталонной модели (5) выполняются условия структурного согласования [2]:

$$\chi_1 = -\left(L^T A_*^{-1} B\right)^{-1}, \quad A_* = A - B\chi_2 L^T, \quad (6)$$

где $\chi_2 = \text{const} \gg 0$ – неизвестная достаточно большая постоянная.

Выполнение соотношений (6) приводит к тому, что выход эталона (5) является задающим воздействием траектории движения объекта (4)

$$y_* = L^T x_*(t) = r(t).$$

Требуется синтезировать явный вид закона управления

$$u = u(y(t), u(\zeta), t), \quad \zeta \in [t - h, t] \quad (7)$$

так, чтобы в процессе функционирования системы (1), (2), (5) выполнялась цель управления:

$$\lim_{t \rightarrow \infty} |y(t) - r(t)| \leq \Delta_0 = \text{const}, \quad (8)$$

где Δ_0 – малая величина.

Наличие в объекте (1) запаздывания по управлению, как правило, ведет к потере устойчивости системы, поэтому параллельно объекту в основной контур подключается дополнительное устройство, компенсирующее отрицательное

влияние запаздывания [3, 4]

$$\frac{dy_K(t)}{dt} = -ky_K(t) + k(u(t) - u(t-h)), \quad (9)$$

где $y_K(t) \in R$, $k = \text{const} > 0$.

Явный вид закона управления (7), обеспечивающего выполнение цели управления (8), синтезируется на основе критерия гиперустойчивости [2, 5], но прежде необходимо решить проблему неопределенности структуры объекта управления, связанную с неизвестной степенью числителя его передаточной функции. Для этого к выходу объекта управления (1) последовательно подключается фильтр-корректор [6] с передаточной функцией

$$y_{out}(s) = \left(\frac{T_1 \cdot s + 1}{T_2 \cdot s + 1} \right)^{n-m-1} \cdot y(s) \quad (10)$$

где $y_{out}(s)$ – выход фильтр-корректора; $T_1, T_2 = \text{const} > 0$ – заданы, $T_2 \ll T_1$.

Представим последовательное соединение объекта и фильтр-корректора

$$y_{out}(s) = \frac{b(s)}{a(s)} \left(\frac{T_1 \cdot s + 1}{T_2 \cdot s + 1} \right)^{n-m-1} U(s) = W_{BOY}(s) W_{BCB}(s) U(s),$$

$$W_{BOY}(s) = \frac{b(s) \cdot (T_1 \cdot s + 1)^{n-m-1}}{a(s) \cdot (T_2 \cdot s + 1)^{n-m+m-n}} = \frac{\bar{b}(s)}{\bar{a}(s)}, \quad W_{BCB}(s) = \frac{1}{(T_2 s + 1)^{n-m-1}},$$

где $U(t) = u(t-h) + \bar{f}(t)$, $\bar{a}(s)$ – квазиполином, $\deg \bar{a}(s) = n$, $\bar{b}(s)$ – гурвицевый полином, $\deg \bar{b}(s) = n - 1$; $W_{BOY}(s)$ – передаточная функция видоизмененного объекта управления с относительным порядком равным единице; $W_{BCB}(s)$ – передаточная функция блока структурных возмущений. Следуя [6], постоянная времени T_2 задается достаточно малой, поэтому допустимо $(T_2 s + 1)^{n-m-1} \cong 1$. Это позволяет исключить блок структурных возмущений из дальнейшего рассмотрения, а синтез закона управления осуществлять для видоизмененного объекта управления. Тогда цель управления (8) относительно основного контура преобразуется к виду:

$$\lim_{t \rightarrow \infty} |y_m(t) - y_{out}(t)| \leq \Delta_1 = \text{const}, \quad (11)$$

где Δ_1 – малая величина.

Поскольку имеет место периодичность внешней помехи $f(t)$ и задающего воздействия $r(t)$, рассматриваемая система является периодической. В подобных системах с целью компенсации периодических помех и более точного отслеживания периодического задания, используется генератор периодических сигналов [7, 8]

$$\mathcal{G}(t) = \mathcal{G}(t - h) + z(t), \mathcal{G}(\theta) = 0, \theta \in [-h, 0], \quad (12)$$

где $\mathcal{G}(t) \in R$ – выход генератора; $z(t) = r(t) - (y_{out}(t) + y_K(t))$.

Синтез явного вида закона управления (7) осуществлялся на основе критерия гиперустойчивости В.М. Попова [2, 5]. Следуя последовательности этапов критерия, был получен закон управления, включающий адаптивные, робастную и периодическую составляющие

$$\begin{aligned} u(t) = & \alpha_1 y_{out}(t) \int_0^t y_{out}(\xi) z(\xi) d\xi + \alpha_2 y_{вых}^2(t) z(t) + \alpha_3 y_K(t) \int_0^t y_K(\xi) z(\xi) d\xi + \\ & + \alpha_4 y_{out}(t - \tau_1) \int_0^t y_{out}(\xi - \tau_1) z(\xi) d\xi + \alpha_5 y_{out}(t - \tau_2) \int_0^t y_{out}(\xi - \tau_2) z(\xi) d\xi + \\ & + \alpha_7 u(t - h) \int_0^t u(\xi - h) z(\xi) d\xi + \alpha_8 \mathcal{G}(t) \int_0^t \mathcal{G}(\xi) z(\xi) d\xi, \end{aligned} \quad (13)$$

где $\alpha_i = \text{const} > 0$, $i = \overline{1, 8}$ – неизвестные параметры регулятора, значения которых определяются на этапе имитационного моделирования системы управления (1), (2), (5), (9), (10), (12), (13), исходя из качества функционирования системы.

Таким образом, в работе представлено моделирование системы управления (1), (2), (5), (9), (10), (12), (13) сложным динамическим объектом, обладающим следующими особенностями: наличие запаздываний нейтрального типа и по управлению, которые оказывают негативное влияние на динамику системы (для компенсации запаздывания по управлению использован упредитель-компенсатор (7)); структурная неопределенность объекта управления, заключающаяся в том, что относительный порядок передаточной функции неизвестен заранее (данная проблема решена применением фильтр-

корректора (8)); воздействие значительных периодических внешних помех (их компенсация осуществляется включением в контур генератора периодических сигналов). Синтезированный закон управления обеспечивает L-диссипативность исследуемой системы, что гарантирует ее гиперустойчивость согласно использованному критерию. Имитационное моделирование синтезированной системы проводилось в интегрированной среде разработки Matlab, его результаты полностью подтвердили работоспособность полученного регулятора. Использование в системе генератора периодических сигналов позволяет практически полностью компенсировать влияние значительных возмущений на траекторию движения объекта управления и с хорошим качеством отрабатывать требуемое задающее воздействие.

Литература

1. Репин Ю.М. О приближенной замене системы с запаздыванием обыкновенными динамическими системами // Прикладная математика и механика 1965. Т. 29, вып. 2, с. 226 – 235.
2. Еремин Е.Л. Нелинейные преобразования алгоритмов прямого адаптивного управления непрерывными объектами: автореф. дис. ...д-ра техн. наук. – Владивосток: ИАПУ ДВО РАН, 1994.
3. Еремин Е.Л., Теличенко Д.А., Чепак Л.В. Синтез адаптивных систем для скалярных объектов с запаздыванием по управлению – Благовещенск: Амурский государственный университет, 2006. – 240 с. – ISBN 5-93493-075-0.
4. Eremin E. L., Chepak L. V. Combined controller for a nonaffine plant with delay in control // Optoelectronics, Instrumentation and Data Processing. 2019. Vol. 55, № 6. P. 542-549.
5. Попов В.М. Гиперустойчивость автоматических систем. М.: Наука, 1970. 456 с.
6. Еремин Е.Л. L-диссипативность гиперустойчивой системы управления при структурном возмущении. IV // Информатика и системы управления. 2013. – № 2(36). – С.100-106.

7. Закс В.С. Об одной возможности повышения точности регулирования в следящих системах циклического действия // АиТ. – 1981. – №1. – С.170-174.

8. Еремин Е.Л. Гиперустойчивость циклических систем управления с генератором периодических сигналов // Информатика и системы управления. 2006. – № 1(11). – С. 224-234.

Сведения об авторе

Никифорова Лариса Владимировна, кандидат технических наук, доцент кафедры информационной безопасности Амурского государственного университета.

**Прокопенко Алексей Николаевич,
Жукова Полина Николаевна,
Страхов Андрей Александрович**

НЕКОТОРЫЕ ВОПРОСЫ ЛИЦЕНЗИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ НА СОВРЕМЕННОМ ЭТАПЕ

Вопросы лицензирования деятельности в области защиты информации являются одними из самых актуальных, поскольку непосредственно определяют кто может осуществлять те или иные действия при обеспечении информационной безопасности.

В соответствии со статьёй 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (далее – ФЗ «О лицензировании...») лицензированию в области защиты информации подлежат следующие виды деятельности (рис. 1):

Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств осуществляется в соответствии с Постановлением Правительства РФ от 16.04.2012 № 313.

Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, осуществляется в соответствии с Постановлением Правительства РФ от 12.04.2012 № 287.

Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического

лица или индивидуального предпринимателя) осуществляется в соответствии с Постановлением Правительства РФ от 16.04.2012 № 314.

Разработка и производство средств защиты конфиденциальной информации осуществляется в соответствии с Постановлением Правительства РФ от 03.03.2012 № 171.

Деятельность по технической защите конфиденциальной информации осуществляется в соответствии с Постановлением Правительства РФ от 03.02.2012 № 79.

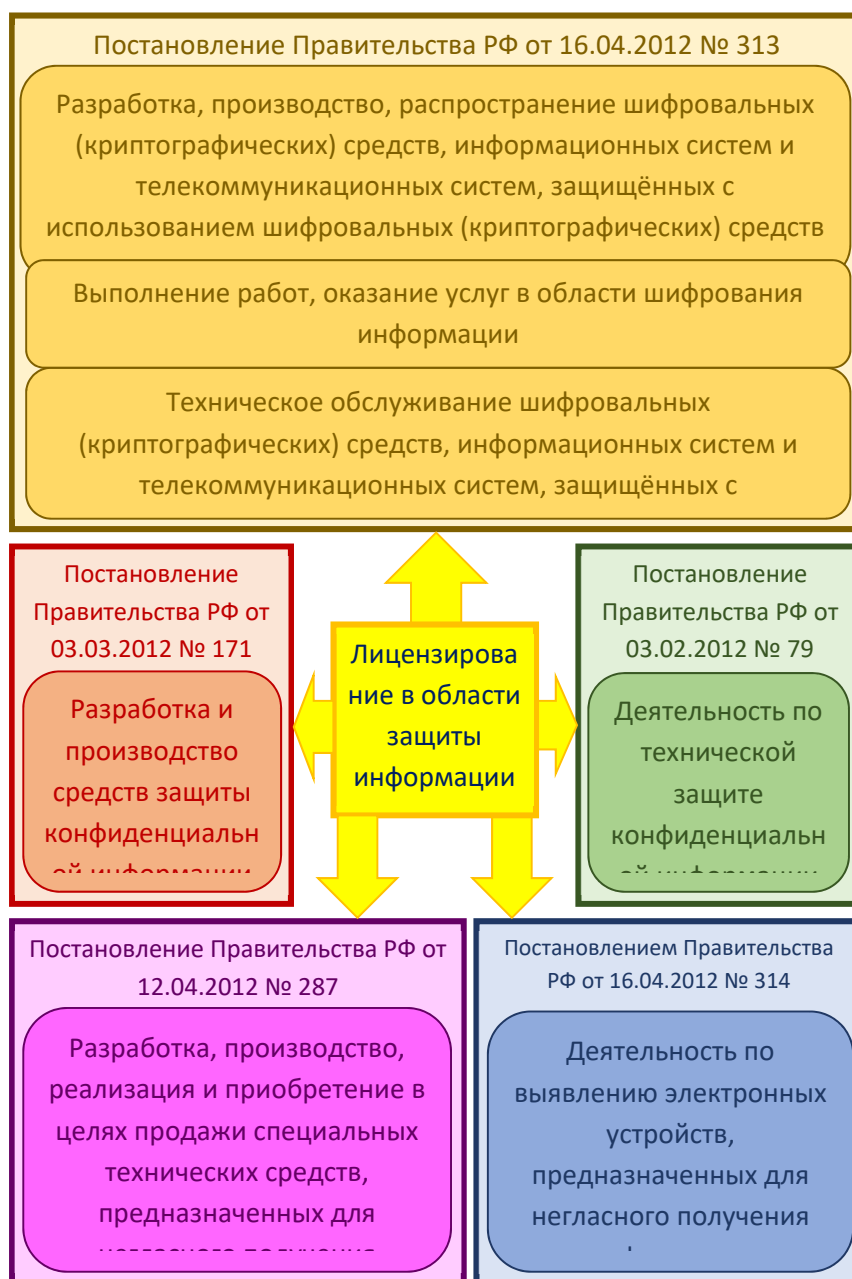


Рис. 1. Виды лицензируемой деятельности в области защиты информации

Лицензирование по первым трем видам деятельности осуществляется ФСБ России, по четвертому виду деятельности и ФСБ России и ФСТЭК России в зависимости от средства защиты информации, по пятому виду деятельности – ФСТЭК России.

Особенностью данных видов деятельности является то, что в 2021 году были внесены изменения, которые запретили осуществление лицензируемой деятельности иностранными юридическими лицами. Таким образом деятельность в области защиты информации по всем пяти направлениям может осуществляться исключительно российскими организациями или индивидуальными предпринимателями. Данное изменение является принципиально новым направлением, причем оно было принято до начала Специальной военной операции и ухода западных производителей средств защиты информации с нашего рынка.

Статья 9 ФЗ «О лицензировании...» в части 4 установила, что срок действия лицензий является бессрочным вне зависимости от вида лицензируемой деятельности. Однако, это не означает, что лицензии выдаются, что называется «навсегда». Закон в статье 18 предусматривает ряд случаев, в которых переоформление лицензии является обязательным, то есть фактически лицензия получается заново. Такие случаи делятся на две группы. С одной стороны, это преобразование лицензиата, то есть реорганизация, смена адреса деятельности, а для индивидуального предпринимателя также и смена ФИО или паспорта. С другой стороны, это изменение тех работ и услуг, которые оказывает лицензиат, соответственно возникает необходимость получения лицензии заново. Подобные требования к переоформлению лицензии представляются справедливыми, поскольку происходят или при смене деятельности или смене субъекта.

Закон в статье 20 предусматривает ряд случаев, при которых осуществляется приостановление лицензии. Такое право делегировано лицензионному органу, то есть в зависимости от вида деятельности ФСБ России

или ФСТЭК России. Основаниями для приостановления деятельности являются не устранение грубого нарушения лицензионных требований, что подтверждается фактом привлечения лицензиата к административной ответственности. Кроме того, основанием может быть не подтверждение лицензиатом своего соответствия требованиям в процессе периодического подтверждения. Это связано с тем, что у лицензиата должно быть в наличии соответствующее оборудование и программное обеспечение, а также штатные сотрудники с образованием в области информационной безопасности и соответствующим опытом. Однако оборудование и ПО могут устареть, может закончиться сертификация на используемые средства защиты информации, а люди могут уволиться и уйти в другую компанию. В результате сложится ситуация, что лицензия у компании есть, но она не соответствует установленным требованиям. В этом случае ФСТЭК России или ФСБ России приостанавливает лицензию данной компании и обращается в суд за аннулированием лицензии.

Отдельно необходимо остановиться на рассмотрении вопросов по лицензированию деятельности по технической защите конфиденциальной информации, урегулированной Постановлением Правительства РФ от 03.02.2012 № 79. Лицензирование деятельности по технической защите конфиденциальной информации (далее – ТЗКИ) осуществляет ФСТЭК России, а данная деятельность является наиболее массовой в области защиты информации и составляет более половины лицензируемых вопросов обеспечения информационной безопасности.

Деятельность по ТЗКИ включает в себя следующие виды работ (услуг) (рис. 2).

Услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в защищаемых помещениях, помещениях с информационными системами или средствах автоматизации.

Услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

Услуги по мониторингу информационной безопасности средств и систем информатизации.

Работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации всех объектов информатизации.

Работы и услуги по проектированию в защищенном исполнении всех объектов информатизации.

Услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации.

Необходимо отметить, что Постановление № 79 содержит ряд формулировок, которые подразделяют деятельность по ТЗКИ на три большие группы.

Во-первых, это обеспечение защиты информации организацией для себя, что в соответствии с пунктами 1, 2, 3 и 6 осуществляется без обязательного лицензирования. Это определено формулировкой услуги, то есть осуществление работ в собственных целях под данную формулировку не попадает. Таким образом, организация может самостоятельно сначала смонтировать, наладить и испытать систему обеспечения информационной безопасности. А затем осуществлять ее эксплуатацию, мониторить состояние ИБ, контролировать защищенность информации от утечек по техническим каналам и от несанкционированного доступа. При этом самостоятельно разрабатывать систему защиты информации и проводить ее аттестационные испытания организации не имеющие лицензии права не имеют.

Во-вторых, это компании, осуществляющие проектирование систем защиты информации и/или проводящие их аттестационные испытания. Данные компании специализируются на оказании услуг и выполнении работ

организациям, которые впоследствии самостоятельно осуществляют обеспечение ИБ. Возможно создание таких специализированных организаций в рамках министерств или ведомств для того, чтобы не привлекать организации со стороны. Например, в МЧС России лицензией на данные виды работ обладает ФКУ «Специальный центр МЧС России».



Рис. 2. Виды работ по технической защите конфиденциальной информации в соответствии с Постановлением Правительства РФ от 03.02.2012 № 79.

В-третьих, это организации, которые оказывают все виды услуг комплексно. То есть не только разрабатывают новые системы обеспечения ИБ и проводят аттестационные испытания объектов информатизации, но и осуществляют контроль проникновения, мониторинг состояния ИБ и т.д. Данные компании принято называть интеграторами, поскольку они интегрируют средства защиты информации различных производителей в рамках одной системы. Сам принцип обеспечения ИБ сторонней организацией называется аутсорсингом и предполагает комплексное оказание услуг по ТЗКИ. Причем организация, оказывающая услуги по ТЗКИ несет полную ответственность за качество защиты информации и возможные утечки. В государственных организациях такой порядок обеспечения ИБ, как правило, не применяется. В последние годы в бизнес сообществе приобретает особую популярность размещение информационных систем, баз и банков данных в облаке. При этом компания, предоставляющая услуги по облачному размещению информации, несет ответственность также и за ТЗКИ.

Особо необходимо обратить внимание на требования к лицензиату по персоналу, помещениям, средствам защиты информации и программному обеспечению которые должны быть в наличии. При этом при получении лицензии соискатель должен подтвердить их наличие соответствующей документацией. К таким требованиям относятся наличие в штате организации не менее трех специалистов, имеющих высшее образование или прошедших профессиональную переподготовку по направлению информационная безопасность. Указанные специалисты должны обладать определенным опытом, причем если для инженеров требования к опыту не менее трех лет, то для руководителей службы ИБ должен иметь опыт работы в сфере ТЗКИ не менее пяти лет. Также организация должна подтвердить, что у нее есть помещения, автоматизированные системы и средства защиты информации, необходимые для выполнения работ и оказания услуг. На помещения составляются технические паспорта и аттестаты соответствия. Наличие СЗИ и ПО подтверждается

сертификатами соответствия и другими документами. Все вышеперечисленное должно находиться у лицензиата в собственности или в аренде, что также подтверждается документацией.

Кроме того, соискатель лицензии должен иметь в своем наличии соответствующее производственное и испытательное оборудование, контрольно-измерительные приборы. Перечень такого оборудования утвержден ФСТЭК России 19.04.2017 года и по состоянию на 18.11.2023 года содержит 28 видов оборудования и программного обеспечения.

У лицензиата должны быть в наличии техническая документация, методические документы и стандарты, перечень которых утвержден ФСТЭК России 12.08.2020 года и по состоянию на 18.11.2023 года содержит 108 документов.

Процедура прохождения лицензирования утверждена Приказом ФСТЭК России от 12.01.2023 № 3, которая помимо перечней того, что должен сделать лицензиат, содержит сроки процедур по получению лицензии, ее переоформления или выдачи дубликата.

Резюмируя вышесказанное, необходимо отметить, что в последние годы система лицензирования в области защиты информации претерпела ряд существенных изменений, которые ее значительно усложнили. В целом требования стали выше, но одновременно лицензии выдаются не на какой-то срок, а являются бессрочными. Также нужно отметить, что деятельность по проектированию новых систем обеспечения ИБ и их аттестационным испытаниям по-прежнему доступна только организациям, имеющим соответствующую лицензию.

Литература

1. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» // Российская газета. № 97. 06.05.2011.

2. Постановление Правительства РФ от 28.12.2021 № 2518 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам

лицензирования отдельных видов деятельности и признании утратившим силу отдельного положения акта Правительства Российской Федерации» // Официальный интернет-портал правовой информации <http://pravo.gov.ru>, 30.12.2021.

3. Постановление Правительства РФ от 26.11.2021 № 2055 «О внесении изменений в Положение о лицензировании деятельности по технической защите конфиденциальной информации» // Собрание законодательства РФ. 06.12.2021. № 49 (Часть I). Ст. 8244.

4. Постановление Правительства РФ от 12.04.2012 № 287 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации» // Российская газета. № 85. 18.04.2012.

5. Постановление Правительства РФ от 16.04.2012 № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» // Собрание законодательства РФ. 23.04.2012. № 17. ст. 1988.

6. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если

техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» // Собрание законодательства РФ. 23.04.2012. № 17. ст. 1987.

7. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации») // Собрание законодательства РФ. 12.03.2012. № 11. Ст. 1297.

8. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации») // Собрание законодательства РФ. 13.02.2012. № 7. ст. 863.

9. Приказ ФСТЭК России от 12.01.2023 № 3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений» // Официальный интернет-портал правовой информации <http://pravo.gov.ru>, 03.02.2023.

10. Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по ТЗКИ: утвержден ФСТЭК 19.04.2017 [Электронный ресурс]. URL: <https://fstec.ru/dokumenty/vse-dokumenty/perechni/perechen-kontrolno-izmeritelnogo-i-ispytatelnogo-oborudovaniya-sredstv-kontrolya-zashchishchennosti-ot-19-aprelya-2017-g> (Дата обращения – 21.11.2023).

11. Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по ТЗКИ: утвержден ФСТЭК России 12.08.2020 [Электронный ресурс]. URL: <https://fstec.ru/dokumenty/vse-dokumenty/perechni/perechen-tekhnicheskoy-dokumentatsii-natsionalnykh-standartov-i-metodicheskikh-dokumentov-ot-12-avgusta-2020-g> (Дата обращения – 21.11.2023).

12. Основы информационной безопасности в МЧС России: учебник / Хабибулин Р.Ш., Прокопенко А.Н., Жукова П.Н. и [др.] М.: Академия ГПС МЧС России, 2023. 649 с.

Сведения об авторах

Прокопенко Алексей Николаевич, кандидат технических наук, доцент, профессор кафедры информационных технологий Академии Государственной противопожарной службы МЧС России.

Жукова Полина Николаевна, доктор физико-математических наук, доцент, заместитель начальника кафедры высшей математики и системного моделирования сложных процессов Санкт-Петербургского университета Государственной противопожарной службы МЧС России им. Героя Российской Федерации генерала-армии Е.Н. Зиничева.

Страхов Андрей Александрович, доцент кафедры информатики и математики Московского университета МВД России имени В.Я. Кикотя.

Разбегаев Павел Витальевич**ПОЛИЦЕЙСКАЯ РОБОТОТЕХНИКА: ИСТОРИЯ И
ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ**

Согласно Стратегии развития информационного общества в Российской Федерации на 2017– 2030 годы, «информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения». К основным направлениям развития отечественных информационных и коммуникационных технологий указанной Стратегией отнесена, в частности, робототехника.

Вместе с тем, необходимо отметить, что робототехнические комплексы специального назначения отнесены к приоритетным направлениям развития науки, технологий и техники в Российской Федерации [5].

Многие исследователи, например, А.Б. Смушкин [3], отмечают, что в зарубежных публикациях активно используется термин «полицейская робототехника» (police robotics) [6, 7]. Российские авторы определяют «полицейского робота» как «программируемый механизм, способный автономно выполнять задачи в интересах полиции» [1, 213]. При этом понятие полицейского робототехнического комплекса можно определить, как «комплекс, состоящий из одного или нескольких полицейских роботов, их рабочих органов и любых механизмов, оборудования, приборов или датчиков, обеспечивающих выполнение роботом функционального назначения (задания)» [1, 213], также автор указывает, что «под механизмом можно понимать не только материальные, но и виртуальные, программно-технологические решения» [1, 213].

Таким образом, полицейская робототехника представляет собой область технологии, связанной с разработкой и использованием роботов в полицейских задачах и функциях. Эта технология нацелена на повышение эффективности работы полиции, обеспечение безопасности общества и сотрудников правоохранительных органов. Полицейские роботы могут включать в себя

разнообразные устройства, от автономных патрульных роботов до беспилотных летальных аппаратов.

Целью полицейской робототехники является создание инновационных средств и технологий, способных улучшить реагирование правоохранительных органов на различные вызовы, включая преступления, аварии, чрезвычайные ситуации. Важным аспектом является также уменьшение рисков для сотрудников полиции, а также обеспечение эффективной защиты граждан и их имущества.

Полицейская робототехника включает в себя разработку и интеграцию передовых технологий, таких как: искусственный интеллект, машинное обучение, автономная навигация и датчики для создания интеллектуальных и автономных систем, способных оперативно реагировать на разнообразные ситуации.

Рассмотрим историю развития полицейских роботов. Она насчитывает несколько десятилетий и включает в себя эволюцию технологий, а также изменения в потребностях и задачах, стоящих перед полицией. Перечислим этапы развития полицейской робототехники:

1. Начальный этап (1950-1960-е годы). Он включает в себя начало экспериментов с использованием роботов в полицейских операциях. Так, примитивные устройства использовались для обнаружения и обезвреживания взрывчатых устройств.

2. Второй этап (1980-1990-е годы). Он включает в себя зарождение автономных систем. Именно в это десятилетие появились первые полицейские роботы, способные перемещаться автономно. Они использовались для разведки в опасных ситуациях и сбора информации.

3. Третий этап (2000-2010-е годы). Он характеризуется стремительным развитием технологий. Достижения в области систем искусственного интеллекта и изготовлении датчиков позволили создавать «умных» и адаптивных роботов. Роботы-патрульные стали широко использоваться для наблюдения на общественных мероприятиях.

4. Четвертый этап (2010-2020-е годы). Он отмечен интеграцией беспилотных летательных аппаратов (дронов) и роботов-спасателей. Дроны стали активно применяться в полицейской работе для воздушного наблюдения; происходит массовое использование роботов-спасателей для операций в опасных или труднодоступных местах.

5. Пятый этап (2020 годы - по настоящее время). Этап характеризуется интеграция применением технологий «будущего», в том числе таких технологий как распознавание лиц, биометрические системы и машинное обучение. Получают развитие роботы с социальными навыками для более эффективного взаимодействия с гражданами в различных сферах.

Таким образом, этапы развития полицейской робототехники показывают, что она прошла путь от первых экспериментов к использованию высокотехнологичных систем в современных полицейских операциях.

Особое развитие в последнее время получило использование беспилотных летательных аппаратов (дронов). Они могут использоваться для воздушного наблюдения и сбора информации, оснащаются камерами с высоким разрешением, тепловизорами и другими сенсорами.

В Волгоградской академии МВД России создана учебно-научная лаборатория «Научно-техническая лаборатория по обслуживанию и ремонту беспилотных и робототехнических средств». Она представляет собой оборудованный кабинет, оснащенный специализированным инструментом для восстановления работоспособности беспилотных и робототехнических средств, комплектующими и расходными материалами для проведения технического обслуживания беспилотных и робототехнических средств, предназначенных для реализации образовательного процесса.

Учебно-научная лаборатория входит в материально-техническое оснащение кафедры информатики и математики и способствует реализации практико-ориентированного подхода с целью повышения качества образовательного процесса в ВА МВД России.

Основными задачами учебно-научной лаборатории являются:

1. Своевременный ремонт и техническое обслуживание беспилотных и робототехнических средств, задействованных при реализации учебных программ.

2. Способствование формированию у обучающихся в процессе практического обучения сознательного отношения к своей профессиональной деятельности, развитие инициативы и нестандартного мышления.

3. Обеспечение формирования позитивного отношения к профессиональной деятельности сотрудников органов внутренних дел у обучающихся образовательных организаций Министерства внутренних дел Российской Федерации.

4. Совершенствование и укрепление учебно-материальной базы ВА МВД России.

Основными функциями Учебно-научной лаборатории являются:

1. Организация и проведение практических занятий с обучающимися ВА МВД России.

2. Формирование, развитие и закрепление профессиональных компетенций и практических навыков по применению основных видов беспилотных и робототехнических средств в различных оперативно-служебных ситуациях.

3. Использование учебно-научной лаборатории для проведения профориентационной работы с обучающимися иных образовательных организаций.

4. Привлечение обучающихся и профессорско-преподавательского состава к подготовке, разработке и реализации научно-исследовательских проектов.

Материально-техническое оснащение учебно-научной лаборатории включает современный набор инструментов для ремонта и доработки технических средств, комплект расходных материалов к беспилотным и робототехническим средствам стоящих на балансе ВА МВД России, комплект мультимедийного оборудования для тестирования видеосистем беспилотных и робототехнических средств, 3D принтер для восстановления и доработки узлов и механизмов беспилотных и робототехнических средств.

Таким образом, использование учебно-научной лаборатории «Научно-техническая лаборатория по обслуживанию и ремонту беспилотных и робототехнических средств» позволяет в полной мере реализовывать практико-ориентированную модель обучения. Отмечается высокая степень удовлетворенности сопровождением учебных занятий наглядными средствами [2]. К положительным сторонам применения оборудования лаборатории следует отнести повышение интереса обучающегося к предмету, получение обучающимися дополнительных знаний по дисциплине. Это, несомненно, повысит качество полученного образования.

Следует отметить, что применение данной технологии способствует не только в полной мере реализации компетентного подхода со стороны обучающихся, но имеет двойной эффект. Педагогические работники сталкиваются с необходимостью приобретения новых компетенций, в том числе и в сфере применения беспилотных и робототехнических средств в деятельности правоохранительных органов. Все это подчеркивает актуальность применения указанного подхода.

Таким образом, использование возможностей учебно-научной лаборатории «Научно-техническая лаборатория по обслуживанию и ремонту беспилотных и робототехнических средств» в образовании, в частности погружение обучающихся в учебный материал с помощью практико-ориентированного обучения, позволит персонализировать и адаптировать обучение, в полной мере включить обучаемых в познавательный процесс, активизировать их познавательный интерес по изучаемым предметам.

Литература

1. Лукашов Н. В. Организационные и правовые основы применения полицейских робототехнических комплексов в органах внутренних дел Российской Федерации // Труды Академии управления МВД России. 2020. № 3 (55). С. 210–221.
2. Разбегаев П.В. Инновационные технологии в образовательной системе МВД РФ // «Мир науки, культуры, образования», 2022, № 4 (95). С. 76-78.

3. Смушкин А. Б. Криминалистическая робототехника: основы концепции // Актуальные проблемы российского права. – 2023. – Т. 18. – № 11. – С. 146–153.

4. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы». Доступ из справ. – правовой системы «КонсультантПлюс» (дата обращения: 24.04.2024).

5. Указ Президента Российской Федерации от 7 июля 2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации». Доступ из справ. – правовой системы «КонсультантПлюс» (дата обращения: 24.04.2024).

6. Looking to the future of police robotics. The use of robotics in police work requires an integration of policy, infrastructure and common sense // policeone.com Jul 7, 2014. URL: [https:// www.police1.com/explosives-eod/articles/looking-to-the-future-of-police-robotics-9OzOWqIPn103Oaoi/](https://www.police1.com/explosives-eod/articles/looking-to-the-future-of-police-robotics-9OzOWqIPn103Oaoi/) / (дата обращения: 24.04.2024).

7. Spilsbury L., Spilsbury R. Robotics. CuttingEdge Technology. eBook. 2017. P. 38.

Сведения об авторе

Разбегаев Павел Витальевич, кандидат педагогических наук, доцент, начальник кафедры информатики и математики Волгоградской академии МВД России.

**Рыбальченко Антон Юрьевич,
Дрога Андрей Анатольевич**

**ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ,
СВЯЗАННЫМ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИЧЕСКИХ
СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ, В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ**

Современное общество в настоящий период времени проходит этап цифровизации. Проще говоря, в различные сферы жизнедеятельности человека происходит внедрение цифровых технологий: от повседневного быта до государственного управления.

Данный процесс, несомненно, облегчает многие задачи и позволяет значительно сэкономить время, являющееся наиболее ценным ресурсом в нашем мире. Однако цифровизация обладает и рядом недостатков: цифровые системы являются уязвимыми перед киберугрозами, т.е. хакерскими атаками. Кроме того, цифровые технологии дают огромное преимущество для преступного мира.

Одной из самых опасных и глобальных преступных угроз является наркотическая преступность. Во-первых, она вовлекает огромное количество людей, в том числе и малолетних. Наркотическая преступность представляет собой организованную иерархичную преступную систему, где каждый выполняет свою роль. Одни лица задействованы в подборе «клиентов», другие отвечают за «доставку» наркотика, третьи – подбирают так называемый «персонал» и т.д. При такой организованной системе, нижестоящие участники не знают вышестоящих, и в таких условиях выявить всех участников преступной группы становится невозможным. Далеко не каждый, кто задействован в преступной схеме является потребителем, однако это ничуть не преуменьшает общественную опасность преступлений, совершаемых в сфере незаконного оборота наркотиков. Во-вторых, употребление наркотиков разрушает не только физическое, но и психическое здоровье людей. Под воздействием запрещенных веществ оказывается губительное и необратимое воздействие на мозг человека,

а также его репродуктивную систему. Несмотря на такие страшные последствия, люди продолжают разрушать свое человеческое начало наркотическими средствами и веществами.

Развитие современных технологий еще больше упрощает процесс получения наркотиков. Торговля наркотиками происходит в зашифрованной части Интернета, более известной как «Даркнет» [2]. «Скрытая» или «темная» сеть является закрытой сетью, куда не проникают роботы поисковых систем, поэтому сайты, находящиеся в этой части Всемирной паутины, никак не индексируются. Анонимная сеть не связанных между собой виртуальных туннелей, представляющих передачу данных в зашифрованном виде; изначально она создавалась военными для использования в своих целях с сохранением полной конфиденциальности [1]. Наиболее развита система «закладок». Покупатель оплачивает «товар» посредством перевода средств на OIWI-кошельки, или же криптовалютой, чаще всего – биткоином. Подобные операции отследить практически невозможно, поскольку используются технологии VPN: IP-адрес пользователя постоянно изменяется. Данный способ получил название бесконтактного, поскольку не требует личного присутствия обоих участников одновременно. Специфика совершения преступлений с использованием информационных технологий также приводит к отсутствию свидетелей.

В таких условиях перед правоохранительными органами стоит нелегкая задача: с наркотической преступностью всегда нелегко было бороться, но сейчас, с использованием преступниками информационных технологий, все многократно усложнилось.

Сотрудники органов внутренних дел должны обладать специальными познаниями в сфере информационных технологий для осуществления противодействия таких преступлений. Учитывая, что наиболее обучаемым человек является в более молодом возрасте, то специализированное обучение должно осуществляться на этапе получения высшего образования будущими сотрудниками, т.е. в образовательных организациях системы МВД России.

Так, в Белгородском юридическом институте МВД России имени И.Д. Путилина реализуется профильное направление подготовки специализации «Оперативно-розыскная деятельность» узкой специализации - деятельности подразделений по контролю за оборотом наркотиков, осуществляющих выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий на базе кафедр оперативно-розыскной деятельности и информационно-компьютерных технологий в деятельности органов внутренних дел. Обучающиеся данной специализации могут не только эффективно бороться с преступлениями в сфере незаконного оборота наркотиков, совершаемыми с использованием информационных технологий, но и использовать возможности технологий в свою пользу.

Данное направление подготовки имеет очный формат обучения, где учатся главным образом лица, окончившие учреждение общего образования, т.е. школы. Однако такая специализация особенно актуальна и для действующих сотрудников. В связи с этим, необходимо разработать специализированную программу повышения квалификации. Получение сотрудниками специальных знаний позволит вывести борьбу с электронной наркокоммерцией на качественно новый уровень.

Необходимо также включить в программу обучения анализ различных подходов к контролю за криптовалютными рынками, включая тайные операции, почтовый перехват, сбор доказательств и судебное преследование внутри страны. Безусловно, интернет-торговцы наркотиками представляют более серьезную угрозу по сравнению с теми, кто осуществляет сделки лично, без использования сети Интернет. Также необходимо рассмотрение взаимосвязи между пользователями криптовалютного рынка и правоохранительными органами.

Представляется, что незаконный оборот наркотических средств и психотропных веществ из сети Интернет никуда не исчезнет. Безусловно,

незаконная торговля в Интернете не раз претерпевала всевозможные неудачи – аресты, мошенничество, потери денежных средств, имущества и др. Однако после каждой такой неудачи запускались процессы восстановления и консолидации. Заккрытие одних торговых площадок порождало создание еще нескольких. Все это свидетельствует о процессе постепенного слияния и переплетения наркотической субкультуры и сетевой.

Вместе с тем, такая ситуация подтолкнула органы государственной власти к поиску оперативных решений возникшей проблемы. С 2012 года в Интернет-пространстве функционирует Единый реестр сайтов. Соответственно, сайты, содержащие ту или иную информацию о наркотиках, незамедлительно блокировались. В 2020 году Президентом Российской Федерации было дано поручение о закрытии доступа к сайтам и страницам в социальных сетях, которые содержащих информацию пропагандистского характера о наркотиках [4]. Также было предложено ввести на всем отечественном сетевом пространстве сетевые фильтры, которые бы затруднили доступ к получению информации о наркотиках.

Подводя итог, правоохранительные органы несмотря на возникающие трудности продолжают вести упорную борьбу с незаконным оборотом наркотиков, которая на сегодняшний день перенеслась в виртуальную среду. В связи с этим необходимо дальнейшее введение специализированных программ в процесс обучения в образовательных организациях системы МВД России в целях овладения сотрудниками правопорядка необходимых знаний и навыков. Помимо противодействия, нельзя забывать и о профилактической работе, которую информационные технологии позволяют вести достаточно наглядно и массово.

Литература

1. Ростовцев, А.В., Берестенко, Е.Д. Использование информационных технологий при расследовании незаконного оборота наркотических средств бесконтактным методом // Вестник Академии права и управления. – 2020. – №3. – С. 39-45.

2. Полунина А.В., Магомедов Р.М. Даркнет: по ту сторону Интернета // Академический журнал Западной Сибири. Т. 15. № 3 (80). 2019. С. 69-70.

3. Генкин А., Михеев А. Блокчейн: как это работает и что нас ждет завтра. – Москва: Альпина Паблишер, 2018. С. 170.

4. Битов А.А. Выявление и раскрытие преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием информационных технологий // Проблемы экономики и юридической практики. 2018. № 3. С. 269-272.

Сведения об авторах

Рыбальченко Антон Юрьевич, старший преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

Дрога Андрей Анатольевич, заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

**Савин Владимир Николаевич,
Гончарова Мария Сергеевна**

АНАЛИЗ УСТОЙЧИВОСТИ ХЭШ-ФУНКЦИИ К ВЗЛОМУ РАДУЖНЫМИ ТАБЛИЦАМИ

Хэш-функции играют важную роль в современной криптографии. На сегодняшний день они имеют широкое применение, и устойчивость хэш-функций к различным видам атак приобретает первостепенное значение. Одной из наиболее значимых проблем в данной области являются атаки, осуществляемые с использованием радужных таблиц.

Криптографическая хэш-функция – это односторонняя хэш-функция [1], обеспечивающая непредсказуемое изменение битов хэш-кода при изменении входных данных и обладающая такими свойствами, как:

1. Лёгкость вычисления $H(M)$ (за полиномиальное время) для любого значения M ;
2. Для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что $H(M) = h$;
3. Для любого данного x вычислительно невозможно найти такой $y \neq x$, что $H(y) = H(x)$;
4. Вычислительно невозможно найти произвольную пару (x, y) такую, что $H(y) = H(x)$.

В современной криптографии хэш-функции объединяются с симметричными криптосистемами для обеспечения целостности сообщений и аутентификации источника данных, а в комбинации с асимметричными криптосистемами они обеспечивают работу систем электронных цифровых подписей [2, 3].

Несмотря на надёжность криптографических хэш-функций, этот способ защиты не является гарантией неприкосновенности данных. Хэш-функции подвержены различным атакам, среди которых выделяются атаки радужными таблицами.

Радужные таблицы – это метод взлома хэша, помогающий злоумышленнику обратить хэш-функцию и представляющий собой предварительно вычисленную базу данных хэш-кодов. Атаки радужными таблицами выполняются быстро, так как злоумышленнику не нужно тратить время на вычисление хэшей. Это является основным отличием между атаками радужными таблицами, brute-force атаками (атаками полным перебором) и атаками по словарю (атаками, осуществляемыми путём пересмотра самых распространённых слов, фраз и комбинаций цифр).

Полный перебор требует огромных временных ресурсов, а хранение каждого входного массива данных с хэш-кодом требует огромного объёма памяти. Радужные таблицы являются компромиссом между временем и объёмом памяти, требуемым для хранения предварительно вычисленных хэшей. В радужной таблице хранятся только начальный входной массив данных и конечный хэш-код, поэтому цепочка, содержащая миллионы хэш-кодов, может быть представлена всего лишь двумя значениями.

Рассмотрим построение хэш-функции методом умножения, выполняемого в два этапа. Сначала умножение ключа k на константу $0 < A < 1$ и получение дробной части полученного произведения ($\bmod 1$). Затем умножение полученного значения на m и округление вниз полученного числа, т.е. $h(k) = [m(kA \bmod 1)]$, где выражение « $kA \bmod 1$ » означает получение дробной части произведения kA , т.е. величину $kA - [kA]$.

Достоинство метода умножения заключается в том, что значение m перестаёт быть критичным. Обычно величина m для удобства реализации функции выбирается равной степени 2. Пусть имеется компьютер с размером слова w битов и k помещается в одно слово. Возможные значения константы A ограничиваются видом $s/2^w$, где s – целое число из диапазона $0 < a < 2^w$. Тогда k сначала умножается на w -битовое целое число $s = A \cdot 2^w$. Результат представляет собой $2w$ -битовое число $r_1 2^w + r_0$, где r_1 – старшее слово

произведения, а r_0 – младшее. Старшие p битов числа r_0 представляют собой искомый -битовый хэш-код (рис. 1).

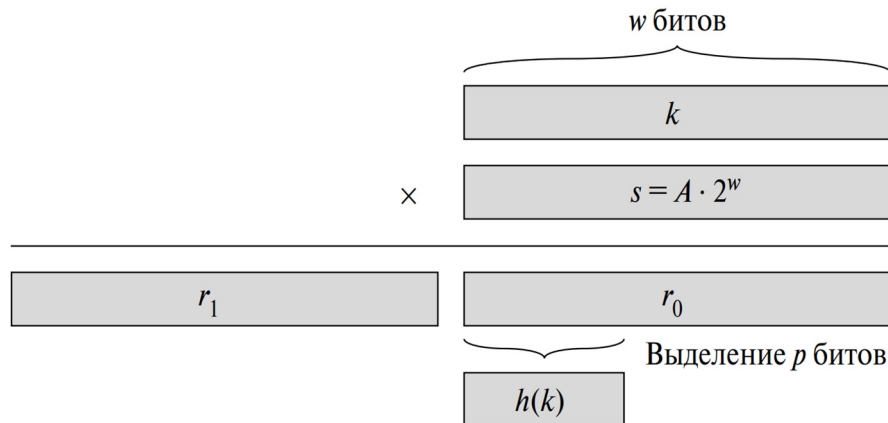


Рис. 1. Хэширование методом умножения

Хотя описанный метод работает с любыми значениями константы A , некоторые значения дают лучшие результаты по сравнению с другими. Кнут предложил использовать значение $A \approx (\sqrt{5} - 1)/2 \approx 0,6180339887 \dots$

В качестве примера, $k = 123456$, $p = 14$, $m = 2^{14} = 16384$ и $w = 32$. Выбираем значение A в виде $s/2^w$, ближайшее к величине $(\sqrt{5} - 1)/2$, так что $A = 2654435769/2^{32}$. Тогда

$$k \cdot s = 327\,706\,022\,297\,664 = (76\,300 \cdot 2^{32}) + 17\,612\,864,$$

и, соответственно, $r_1 = 76\,300$ и $r_0 = 17\,612\,864$. Старшие 14 битов числа r_0 дают хэш-код $h(k) = 67$ [4].

Рассмотрим набор двузначных значений, которые зашифрованы в четырёхзначных хэш-кодах. При использовании построения хэш-функции методом умножения хэш-код числа 10 равен 0823. Простая функция редукции может захватить последние две цифры четырёхзначного числа. Хэш-код 0823 возвращает входной массив данных 23.

Одним из способов уменьшения воздействия коллизий на радужные таблицы является использование нескольких функций редукции.

Рассмотрим таблицу поиска, построенную в Excel (рис. 2). Для иллюстрации задачи вычисления хэш-кодов будут использованы числа от 0 до 99. Алгоритм хэширования принимает входной массив данных в виде числа от 0

до 99 и хэширует его в четырёхзначное число. Функции редукции R_1 и R_2 захватывают две последние цифры и две первые цифры соответственно.

M1	h3
3	3708
10	5850
25	4202
68	5520
91	5109

Рис. 2. Таблица поиска

Таблица поиска (рис. 2) демонстрирует свойство радужной таблицы, которое позволяет сократить требуемое количество места для данных, ограничиваясь хранением только начального входного массива данных и конечного хэш-кода. Пусть требуется найти входной массив данных хэш-кода 5520. В таблице данное значение конечного хэш-кода соответствует начальному входному массиву данных 68. Хэш-код числа 68 равен 3131. Для любого заданного допустимого хэш-кода функция сокращения должна генерировать допустимое значение входного массива данных. К хэш-коду применяется функция редукции R_1 , после чего хэшируется число 31. Хэш-код числа 31 равен 3790 и не соответствует значению 5520. Далее к хэш-коду 3790 применяется функция редукции R_2 , после чего хэшируется число 37. Хэш-код числа 37 равен 5520. Соответственно, входной массив данных равен 37 (рис. 3).

M1	h1=H(M1)	M2=R1(h1)	h2=H(M2)	M3=R2(h2)	h3=H(M3)
68	3131	31	3790	37	5520

Рис. 3. Пример цепочки в радужной таблице

Радужная таблица создаётся построением цепочек хэшей, начиная с возможных паролей. Создание полноценных радужных таблиц требует больше времени, чем нужно для создания обычных таблиц поиска, но также требует значительно меньше памяти. При этом радужные таблицы более реализуемы на практике, хоть они и требуют больше времени на восстановление входного массива данных (для построения обычной таблицы для 6-символьного пароля с байтовыми символами потребуется $256^6 = 2,81 \cdot 10^{14}$ блоков памяти, в то время как для радужной – всего $256^{6-2/3} = 4,29 \cdot 10^9$ блоков).

Но несмотря на все преимущества радужных таблиц, включая возможность отказаться от обработки сотен тысяч потенциальных паролей и сопоставления их хэш-кодов, использование огромного набора предварительно вычисленных хэш-значений и сокращения времени, необходимого для взлома, есть способы, позволяющие предотвратить атаки радужными таблицами.

Соль (Salt) – это данные, передающиеся хэш-функции вместе с входным массивом данных. Эти данные могут быть добавлены в начале, в середине или в конце выходного массива данных. Для того чтобы сделать Salting более эффективным с точки зрения предотвращения взлома хэша, используются уникальные значения соли для паролей разных пользователей. В этом случае, если злоумышленник взломает хэш-код одного пользователя, он не сможет взломать хэш-код пользователя, использующего идентичный пароль. Значение соли и входной массив данных воспринимаются хэш-функцией как обычный входной массив. Злоумышленник не сможет взломать хэш, используя стандартную атаку радужными таблицами, так как он получит обратное значение хэша в виде обычного текста без значения соли. Для создания надёжных солей рекомендуется использовать криптографически стойкие генераторы псевдослучайных чисел, что делает каждую попытку взлома более трудной и затратной, а также предотвращает использование радужных таблиц.

Ещё один способ избежать взлома радужными таблицами – это не использовать уязвимые алгоритмы хэширования, такие как MD5 или SHA-1. Вместо этого рекомендуется применять современные и более устойчивые к атакам функции хэширования, которые разработаны специально для повышения безопасности и усложнения процесса взлома, используя методы, такие как соль, итерации и повышенные требования к памяти.

Таким образом можно сделать следующие выводы:

- Для защиты информации с использованием хэш-функций важно выбирать алгоритмы, усложняющие процесс подбора паролей.
- Применение таких методов, как использование соли и итераций, позволяет снизить риски взлома после атаки радужными таблицами.

- Для обеспечения безопасности нужно отказываться от использования небезопасных алгоритмов хэширования, таких как MD5 и SHA-1, и отдавать предпочтение более современным алгоритмам, таким как Кескак, scrypt и другим.

Литература

1. Игнатъев, Е. Б. Защита информации: криптоалгоритмы хэширования / Е. Б. Игнатъев. – 2-е изд., испр. – Санкт-Петербург: Лань, 2024. – 264 с. – ISBN 978-5-507-47433-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/370928> (дата обращения: 04.05.2024). – Режим доступа: для авториз, пользователей.
2. Ahmad Neyaz Khan, Ming Yu Fan, Asad Malik, Mohammed Aslam Husain, Cryptanalyzing Merkle-Hellman Public Key Cryptosystem with Artificial Neural Networks, 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 10.1109/I2CT45611.2019.9033917, (1-7), 2019.
3. ГОСТ 34.11-2018 Информационная технология. Криптографическая защита информации. Функция хэширования
4. Кормен, Томас Х., Лейзерсон, Чарльз И., Ривест, Рональд Л., Штайн, Клиффорд. Алгоритмы: построение и анализ, 2-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2011. – 1296 с.: ил. – Парал. тит. англ. ISBN 978-5-8459-0857- (рус.)

Сведения об авторах

Савин Владимир Николаевич, кандидат технических наук, доцент кафедры Кубанского государственного технологического университета.

Гончарова Мария Сергеевна, студент Кубанского государственного технологического университета.

**Савотченко Сергей Евгеньевич,
Акапьев Виктор Львович,
Чеканов Александр Николаевич**

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОИСКА ПОТЕНЦИАЛЬНОГО ПОДОЗРЕВАЕМОГО ПО ПРИЗНАКАМ СОВЕРШЕННОГО ПРЕСТУПЛЕНИЯ

В настоящее время в арсенале сотрудников правоохранительных органов, осуществляющих оперативно-розыскные мероприятия, имеются различные информационно-поисковые системы (ИПС), автоматизированные банки данных (АБД), информационно-поисковые карты (ИПК), автоматизированные дактилоскопические идентификационные системы (АДИС) и другие средства хранения и накопления информации о правонарушениях. Все эти современные информационно-технические средства и технологии направлены на более успешное расследование преступления и установления лица или круга лиц, его совершивших.

Одним направлением поиска подозреваемых преступников является система использования всех имеющихся в банке данных признаков способов совершения преступления конкретным лицом. Способы совершения преступления (почерк) являются устойчивым поисковым признаком и, в большинстве случаев, определяются характером, навыками и привычками преступника, что давно замечено на практике. Повторяемость способов совершения преступления в определенной мере позволяет выделить подозреваемых. Однако при повторном совершении одним и тем же субъектом аналогичного преступления точного (детального) повторения всех признаков способов совершения может и не быть, хотя, тем не менее, наблюдается определенное сходство по совокупности признаков.

В историческом плане истоки возникновения и современное состояние проблемы поиска преступников по признакам способов совершения преступлений изложено в статье [3], в которой на примере квартирных краж

(краж из жилищ) также предложены определенные конкретные меры оптимизации поиска.

Основная цель нашей работы – обратить внимание специалистов по криминалистике на имеющиеся методы теории линейного программирования [4], предназначенные для обработки больших объемов данных с использованием современных быстродействующих компьютеров. Нами сделана попытка поиска одного или нескольких потенциальных (возможных) преступника по признакам, как самого преступника, так и связанных непосредственно с ним признаков совершенного преступления на основе математической модели с применением венгерского метода из теории линейного программирования [5]. К примеру, в известной компьютерной системе MAPLE [6] в пакете SIMPLEX имеются встроенные функции *minimize* и *maximize*, которые предназначены для решения задач линейного программирования [7].

Модель формулируется следующим образом. Пусть имеется n возможных пронумерованных преступников $i = 1, 2, 3, \dots, n$, для которых субъективно назначены по какой-либо шкале оценки по каждому из n признаков ($j = 1, 2, 3, \dots, n$) по ранее совершенным подобным преступлениям. В результате имеем следующую таблицу «эффективности» расследуемого преступления:

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & \cdot & c_{1j} & \cdot & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdot & c_{2j} & \cdot & c_{2n} \\ c_{31} & c_{32} & c_{33} & \cdot & c_{3j} & \cdot & c_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{i1} & c_{i2} & c_{i3} & \cdot & c_{ij} & \cdot & c_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{n1} & c_{n2} & c_{n3} & \cdot & c_{nj} & \cdot & c_{nn} \end{pmatrix}. \quad (1)$$

Наиболее подходящая потенциальная кандидатура по признакам (всего цикла преступления, т.е. от подготовки, совершения и сокрытия) как совершенного преступления, так и самого подозреваемого находится из решения

стандартной задачи линейного программирования. Задача формулируется так: найти максимальное значение так называемой целевой функции

$$F = \sum_{i=1}^{i=n} \sum_{j=1}^{j=n} c_{ij} x_{ij}, \quad (2)$$

при ограничениях

$$\sum_{i=1}^{i=n} x_{ij} = 1, \quad \sum_{j=1}^{j=n} x_{ij} = 1, \quad (3)$$

где $x_{ij} = 0$ или $1, i = 1, 2, 3, \dots, n, j = 1, 2, 3, \dots, n$.

В теории линейного программирования строго математически доказано, что задача (2), (3) имеет решение. В частности, вектор-матрица X может быть представлена в виде

$$X = \begin{pmatrix} 0 & 0 & 1 & . & 0 & . & 0 \\ 0 & 1 & 0 & . & 0 & . & 0 \\ 0 & 0 & 0 & . & 1 & . & 0 \\ . & . & . & . & . & . & . \\ 1 & 0 & 0 & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & 0 & 0 & 1 \end{pmatrix}, \quad (4)$$

из чего следует, что по третьему признаку для расследуемого совершенного преступления более всего подходит 1-й преступник, по второму признаку – 2-й преступник, по первому признаку – i -й преступник и так далее.

Венгерский метод решения задачи (1)-(3) является частным случаем так называемой транспортной задачи. Специфический характер системы ограничений позволяет существенно упростить алгоритм такой решения задачи. Эта задача впервые была поставлена, в первую очередь перед математиками, экономистом Т. Купмансом, который в годы Второй мировой войны занимался вопросами оптимального распределения военных грузов из Америки в Европу, в Советский Союз. Рассматриваемый метод получил широкое распространение из-

за упрощенного алгоритма, который был разработанный венгерским математиком Я. Эгервари, и был в последствие назван «венгерским».

Отметим, что имеется достаточно простая возможность компьютерной реализации предложенной модели без использования прикладных математических пакетов. В этом случае необходимо (специалисту-программисту) разработать приложение с удобным пользовательским интерфейсом, что позволит сотрудникам правоохранительных органов, осуществляющих оперативно-розыскные мероприятия без специальных знаний, использовать рассматриваемый метод поиска. Кроме того, современные реалии потребуют учета в постановке задачи поиска такого фактора как «цифровой след» преступника.

В заключение следует отметить, что любые средства и методы оптимизации поиска в информационно-поисковых системах могут дополняться узкоспециализированными приложениями, которые позволяют проводить поиск в разы эффективнее, призваны служить цели борьбы с преступностью в бурно развивающемся цифровом обществе.

Литература

1. Криминалистика: учебник / Под. ред. Е.П. Ищенко. – М.: ИНФРА-М, 2010. 780 с.
2. Зуйков Г.Г. Поиск преступников по признакам способов совершения преступлений. – НИиРИО ВШ МВД СССР, 1970. 191 с.
3. Свистильников А.Б., Свистильникова Е.А. Противодействие кражам из жилищ с помощью автоматизированной информационно-поисковой системы оперативно-розыскного назначения. Вестник калининградского юридического института МВД России. 2011, №4, с.20-25.
4. Банди Б. Основы линейного программирования. Пер. с англ. М.: Радио и связь, 1989. 176 с.
5. Халимон В.И., Проститенко О.В., Рогов А.Ю. Модели принятия решений (транспортная задача). – СПб.: СПбГТИ(ТУ), 2017. 56 с.

6. Савотченко С.Е., Кузьмичева Т.Г. Методы решения математических задач в Maple. – Белгород: Изд-во «Белаудит», 2001. 116 с.

7. Баков А.А. Решение задач линейного программирования в учебном курсе «Компьютерное моделирование» посредством системы Maple // Вестник МГПУ. Серия: Информатика и информатизация образования. 2007. №10. С. 61-65.

Сведения об авторах

Савотченко Сергей Евгеньевич, доктор физико-математических наук, доцент, профессор кафедры математики Российского государственного геологоразведочного университета имени Серго Орджоникидзе.

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина.

Чеканов Александр Николаевич, старший преподаватель кафедры обеспечения безопасности на объектах транспорта Белгородского юридического института МВД России имени И.Д. Путилина.

**Самойлова Юлия Михайловна,
Некрасова Анастасия Александровна**

СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Современный мир находится в бурно развивающемся потоке технических инноваций, обусловленных стремительным развитием научно-технического прогресса и разносторонней модернизацией общественных отношений и всех сфер жизни общества. Это привело к появлению различных технических средств, призванных упрощать жизнь человека и повышать эффективность тех или иных сфер профессиональной служебной деятельности.

Деятельность правоохранительных органов так же находится в непрерывной модернизации и стремится использовать новейшие технические разработки для достижения максимальной эффективности защиты прав, свобод и законных интересов граждан.

На современном этапе развития аппаратно-программных средств прогресс в преобладающей степени определяется степенью их интеллектуализации. Возникновение элементов искусственного интеллекта в автоматизированных информационных системах и технологиях многие публицисты воспринимают как появление «летающих машин» и называют 21 век веком будущего.

В октябре 2019 г. Президент России В.В. Путин утвердил Национальную стратегию развития искусственного интеллекта до 2030 года. В документе указаны приоритетные научные задачи: обеспечение ускоренного развития искусственного интеллекта в Российской Федерации, проведение научных исследований в области искусственного интеллекта, повышение доступности информации и вычислительных ресурсов для пользователей, совершенствование системы подготовки кадров в этой области [2].

Данная стратегия ставит одной из целей национальной политики - совершенствование разработок систем искусственного интеллекта, что теоретически способно принести огромную пользу в различных сферах и

существенно упростить достижение задач внутренней политики, в том числе в вопросах правоохранительной деятельности, которая по своей сущности является достаточно сложной и многозадачной. Для рассмотрения вопроса применения интеллектуальных информационных систем в правоохранительной деятельности необходимо определить само понятие и сущность систем искусственного интеллекта в целом и искусственного интеллекта в частности [1].

Искусственный интеллект является создаваемым с помощью смежных технологий программным обеспечением, способным к выполнению задач интеллектуального характера. Особенностью аппаратно-программного средства с элементом искусственного интеллекта является его способность к самообучению, глубокому анализу получаемой им информации и способностью самостоятельно принимать экспертные решения на основе имеющегося у него данных и опыта. Во многом принцип работы систем искусственного интеллекта схож с когнитивной работой человеческого мозга, откуда и произошло название данного программного обеспечения.

Системы искусственного интеллекта, используемые в правоохранительной деятельности, позволяют органам внутренних дел более эффективно выполнять задачи, связанные с противодействием преступности [3]. Данные технологии представлены разными классами автоматизированных информационных систем, оказывающих помощь подразделениям полиции по выявлению, пресечению, раскрытию и расследованию преступлений, а также поиску разыскиваемых лиц и обнаружению подозрительной активности отдельных индивидов.

Одной из наиболее популярных систем искусственного интеллекта в деятельности правоохранительных органов является биометрическая система. Она представляет собой программное обеспечение, выявляющее особенности внешности сканируемых людей и сопоставляющая их с внешностью лиц, находящихся в ее базе данных с последующим уведомлением сотрудников правоохранительных органов о нахождении сходства. Современные биометрические системы применяются при выявлении преступной активности и

для облегчения расследования и раскрытия уже совершенных преступлений, а сам процесс работы данных систем состоит из следующих стадий:

- 1) захват фотоизображения с фотоаппарата или в виде кадра из видеопотока;
- 2) выявление лица – определение наличия лица (лиц) на фотографии в виде прямоугольных областей;
- 3) выделение существенных признаков;
- 4) нормализация или выпрямление лица;
- 5) распознавание или кодирование лица, заключающееся в анализе программным обеспечением полученных в ходе наблюдения данных;
- 6) сравнение лиц, заключающееся в сопоставлении полученной в ходе анализа информации с информацией, находящейся в базе для получения сходств.

Еще одним видом систем с искусственным интеллектом, используемых в правоохранительной деятельности, являются автоматизированные информационные системы управления дорожным движением. Особенностью такого аппаратно-программного комплекса является то, что он представляет собой целую систему различных технических средств и систем с общим доступом управления из единого центра. Центр представляет собой совокупность видеокамер, оснащенных искусственным интеллектом, многочисленных электронных табло, информирующих водителей о тех или иных событиях на разных участках дорог, детекторов транспорта, дорожных контролеров, метеостанций и прочей технической аппаратуры, позволяющей объективно оценить ситуацию на определенном участке дорог федерального и регионального значения. Данные системы способны анализировать состояние дорожного полотна, наличие на них посторонних предметов или влияние на них погодных условий и прочих факторов и самостоятельно принимать экспертное решение о наличии опасности и даже классифицировать эту опасность по уровням.

Автоматизированный комплекс, представляющий собой беспилотный летательный аппарат (гибридный седан), является разработкой в сфере искусственного интеллекта, позволяющий оценивать оперативную ситуацию на земле и в небе и принимать решение о наличии тех или иных криминогенных или общественно опасных факторов с дальнейшим уведомлением об этом различных органов внутренних дел. Данная система способна самостоятельно строить маршрут своего передвижения, выделять предметы по фактору их предполагаемого интереса для правоохранительных органов и фокусироваться на них, передавая изображение сотрудникам полиции и самостоятельно анализируя его. Для повышения эффективности данной системы, стоящей на страже правопорядка и законности, она оборудована следующими приборами:

- системой спутниковой и инерционной навигации;
- системой круглосуточного наблюдения;
- камерой видимого диапазона;
- тепловизионной камерой;
- системой радиовидения;
- радиоканалом для передачи цифровых изображений;
- функционалом обнаружения, классификации и сопровождения объекта интереса [5].

Данная аппаратура позволяет вышеуказанной интеллектуальной информационной системе сопровождать интересующий ее объект оставаясь незамеченной и существенно усложнять совершение преступления, обеспечивая своевременное оповещение сотрудников правоохранительных органов.

Таким образом, автоматизированные системы искусственного интеллекта являются сложным аппаратно-программным средством, способным самостоятельно анализировать получаемые им данные, сопоставлять их с уже имеющейся информацией из базы данных и принимать те или иные решения самостоятельно, без помощи человека. Указанные системы ввиду значительного

количества полезных функций востребованы при решении тех или иных задач правоохранительной деятельности и принятия управленческих решений.

В подразделениях органов внутренних дел информационные системы с элементом искусственного интеллекта показывают высокую эффективность своей работы. Данное направление в информационно-компьютерных технологиях необходимо продолжать модернизировать с целью дальнейшего развития технологий, позволяющих даже молодому специалисту с недостаточным уровнем профессиональных знаний в правоохранительной деятельности ставить и решать служебные задачи.

Литература

1. Финн, В.К. Искусственный интеллект: методология, применения, философия. М: КРАСАНД, 2018. 448 с.

2. Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (доступ получен: 08.05.2024).

3. Степаненко, Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Д.В. Бахтеев, Ю.А. Евстратова // Всероссийский криминологический журнал. – 2020. – № 2. – Т. 14. – С. 206–214.

4. Булгаков, Д.Ю. Современные подходы к тестированию систем биометрической идентификации по изображению лица / Д.Ю. Булгаков // Искусственный интеллект (большие данные) на службе полиции. Сборник статей международной научно-практической конференции. М.: Академия управления МВД России, 2020. С. 45 – 51.

5. Гаврилов, Д.А. Возможности применения автоматизированной оптико-электронной системы наземно-воздушного мониторинга в деятельности ОВД /

Д.А. Гаврилов, Н.Н. Щелкунов // Искусственный интеллект (большие данные) на службе полиции. Сборник статей международной научно-практической конференции. М.: Академия управления МВД России, 2020. С. 59 – 64.

Сведения об авторах

Самойлова Юлия Михайловна, кандидат технических наук, старший преподаватель кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России им. И.Д. Путилина.

Некрасова Анастасия Александровна, курсант Белгородского юридического института МВД России им. И.Д. Путилина.

**Селеменова Татьяна Александровна,
Ермакова Софья Андреевна**

К ПРИЛОЖЕНИЮ ТЕОРИИ СТАТИСТИЧЕСКИХ РЕШЕНИЙ

Систематическое и разностороннее применение математических методов, прежде всего математического моделирования, является прочной основой для повышения эффективности деятельности специалистов территориальных органов, структурных подразделений, управленческого аппарата, научных и образовательных организаций МВД и МЧС России [6]. Поскольку подавляющее большинство актуальных практических проблем связано с ситуациями, представляющими собой случайные события, особую роль при реализации потенциала математического моделирования играют вероятностно-статистические модели [2].

В такого вида моделях реальных явлений и процессов для выражения объективных соотношений используются термины и научные идеи теории вероятностей, что позволяет отразить заложенную в ситуации неопределенность. Использование статистического аналога понятия «вероятность» дает возможность по одним относительным частотам произвести расчет других частот, получив новую важную информацию об исследуемом явлении или процессе. Таким образом, чисто теоретическая, базовая (вероятностная) модель надстраивается в соответствии с понятийным аппаратом и методологией математической статистики [1].

Интеграция идей теории вероятностей с положительными и отрицательными аспектами выборочного метода, являющегося фундаментальным в математической статистике, приводит к построению адекватной вероятностно-статистической модели. Для построения моделей, которые могут быть использованы для получения достоверных выводов о закономерностях, присущих генеральной совокупности, по ограниченным выборочным данным, необходимо:

- 1) сформировать репрезентативную выборку;

- 2) исходить из априорной гипотезы о связи выборочных и генеральных (теоретических) числовых характеристик;
- 3) корректно применять теорию оценивания выборочных характеристик;
- 4) последовательно реализовывать этапы статистической проверки параметрических (непараметрических) гипотез.

Покажем особенности построения вероятностно-статистической модели в процессе применения теории статистических решений.

Постановка задачи. На основе теории статистических решений требуется установить наличие статистически значимых различий между двумя выборочными совокупностями, объемы которых не совпадают. Статистические различия следует выявить по некоторому общему признаку X , используя подходящий для этой цели статистический критерий Манна-Уитни [3].

Таблица 1. Ранжирование значений признака по суммарной выборке

№ п/п	Показатели в баллах	Ранги	№ п/п	Показатели в баллах	Ранги
1	31	1	14	40	12,5
2	33	2	15	41	16
3	34	3	16	41	16
4	35	4	17	41	16
5	36	5,5	18	42	19
6	36	5,5	19	42	19
7	37	7	20	42	19
8	38	8,5	21	44	21
9	38	8,5	22	46	22
10	39	10	23	47	23
11	40	12,5	24	48	25
12	40	12,5	25	48	25
13	40	12,5	26	48	25

При проведении эксперимента формировались выборки из слушателей заочной формы обучения, служебная деятельность которых связана с мегаполисом Санкт-Петербургом (выборка А) и Ленинградской областью (выборка В). В качестве признака X рассматривался показатель «вовлеченности» в деятельность [4]. По двум репрезентативным выборкам получены статистические данные, измеренные в баллах, которые затем были переведены в

ранги [5]. В таблице 1 представлены результаты выполнения ранжирования значений признака по суммарной выборке.

Результат перехода от баллов к рангам по выборочной совокупности А ($n = 14$) представлен в таблице 2.

Таблица 2. Перевод баллов в ранги по выборке А

Баллы	36	37	38	38	39	41	42	42	44	46	47	48	48	48
Ранги	5,5	7	8,5	8,5	10	16	19	19	21	22	23	25	25	25

В таблице 3 отражено соответствие между баллами и рангами, полученное для данных выборки В ($n = 12$).

Таблица 3. Перевод баллов в ранги по выборке В

Баллы	31	33	34	35	39	40	40	40	40	41	41	42
Ранги	1	2	3	4	5,5	12,5	12,5	12,5	12,5	16	16	19

Для вычисления наблюдаемого (выборочного) значения по критерию Манна-Уитни применяется формула:

$$U_{\text{набл}} = n_a n_b + \frac{n_{\max}(n_{\max}+1)}{2} - T_{\max} \quad . \quad (1)$$

Подставив в формулу (1) объемы выборок (n_a , n_b), объем максимальной выборки ($n_{\max}$), наибольшую из двух ранговых сумм ($T_{\max}$), получим наблюдаемое значение критерия: $U_{\text{набл}} = 38,5$.

По таблице критических значений для критерия Манна-Уитни, учитывая объемы выборок и задав уровень значимости 0,05, найдем критическую точку: $U_{\text{кр}}(0,05) = 45$.

Так как используемые эмпирические данные приводят к получению соотношения $U_{\text{кр}} > U_{\text{эмп}}$, то критерию Манна-Уитни гипотезу H_0 об отсутствии различий между двумя выборками следует отклонить. Это означает, что имеются статистические основания, позволяющие на уровне значимости 0,05 принять альтернативную гипотезу H_1 . Имеющиеся различия в выборочных данных можно считать статистически значимыми.

Таким образом, построение вероятностно-статистической модели в соответствии с поставленной задачей привело к важному выводу: показатели

уровня вовлеченности в группе сотрудников МЧС, осуществляющих профессиональную деятельность в Ленинградской области выше, чем в группе сотрудников, служба которых проходит в Санкт-Петербурге.

В заключение отметим, что в целях дальнейшего повышения эффективности теории и практики прогнозирования, постановки и решения организационно-управленческих задач, стоящих перед министерствами и ведомствами Российской Федерации, необходимо интенсивное привлечение всего спектра разработанных классических и современных научных методов и информационно-технологических средств [7].

Литература

1. Кремер, Н.Ш. Теория вероятностей и математическая статистика: Учебник для вузов. М.: ЮНИТИ ДАНА, 2017. 551 с.
2. Никонов О.И. Математическое моделирование и методы принятия решений: учеб. пособие / О. И. Никонов, С. В. Кругликов, М. А. Медведева. Екатеринбург: Изд-во Урал. ун-та, 2015. 100 с.
3. Осипова, С.И. Математические методы в педагогических исследованиях: Учебное пособие / С.И. Осипова, С.М. Бутакова, Т.Г. Дулинец, Т.Б. Шаипова. Красноярск: Сиб. Федер. Ун-т, 2012. 264 с.
4. Самонов, А.П. Психология для пожарных. Психологические основы подготовки пожарных к деятельности в экстремальных условиях / А.П. Самонов. – Пермь: Звезда, 2004. – 594 с.
5. Селеменева Т.А., Фомичева Т.М. Применение статистических гипотез для работы с личным составом формирований МЧС России // ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МЕТОДОВ К РЕШЕНИЮ ЗАДАЧ МЧС РОССИИ: Сборник трудов секции №14 XXXIII Международной научно-практической конференции. Химки, 2023. С. 167-172.
6. Трофимец, Е. Н. Теоретико-вероятностные методы и модели в системе управления информационно-аналитической подготовкой специалистов МЧС России / Е.Н. Трофимец. Текст: непосредственный // Современная наука:

актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2021. №8. С. 128-134.

7. Selemeneva T.A. Application of mathematical methods in study of scientific and mathematical education efficiency in the higher education institutions of emergency situations Ministry of Russia // Int. J. Learning and Change, 2018. Vol. 10. No. 4. P. 346-358.

Сведения об авторах

Селеменова Татьяна Александровна, кандидат педагогических наук, доцент кафедры высшей математики и системного моделирования сложных процессов Санкт-Петербургского университета Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева.

Ермакова Софья Андреевна, курсант Санкт-Петербургского университета Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева.

Старостенко Игорь Николаевич

УГРОЗЫ И УЯЗВИМОСТИ, СВЯЗАННЫЕ С СЕТЕВЫМ ПРОТОКОЛОМ IP

Протокол IP (Internet Protocol) представляет собой ключевой сетевой протокол, применяемый в современных компьютерных сетях, включая Интернет. Его основная функция заключается в маршрутизации и передаче данных между сетевыми устройствами, что обеспечивает их взаимодействие независимо от используемого аппаратного обеспечения и операционных систем. Главная задача протокола IP – доставка пакетов данных от отправителя к получателю по наиболее эффективному маршруту. Для достижения этой цели каждому устройству в сети назначается уникальный IP-адрес, который служит для идентификации как отправителя, так и получателя. Протокол IP функционирует на сетевом уровне модели OSI и взаимодействует с протоколами более высоких уровней: TCP и UDP. Существует две основные версии протокола IP: IPv4 (Internet Protocol version 4) и IPv6 (Internet Protocol version 6). На сегодняшний день наиболее распространенной продолжает оставаться версия IPv4. Однако, в связи с ограниченным количеством доступных IPv4-адресов, активно внедряется IPv6, который предлагает значительно большее количество адресов и улучшенные функциональные возможности.

IP был разработан как протокол без установления соединения. Он не предназначен для мониторинга потока пакетов и управления им. При необходимости эти функции выполняются в основном протоколом TCP на транспортном уровне.

IP не предпринимает никаких действий, чтобы проверить, действительно ли указанный в пакете IP-адрес источника поступил из этого источника. Поэтому злоумышленники могут отправлять пакеты, используя поддельный IP-адрес источника. Кроме того, при выполнении своих атак злоумышленники могут изменять и другие поля в заголовке IP.

Существуют различные типы атак, связанные с IP. Одной из наиболее распространенных угроз является атака, основанная на ICMP (Internet Control

Message Protocol). Злоумышленники используют пакеты эхозапросов (ping) для сканирования подсетей и хостов в защищенных сетях, что позволяет им осуществлять лавинные атаки типа DoS (Denial of Service) и манипулировать таблицами маршрутизации на целевых устройствах. Эти атаки могут быть направлены на сбор информации, что позволяет злоумышленникам определить топологию сети, выявить активные хосты, распознать операционные системы (создавая цифровые отпечатки ОС) и оценить состояние межсетевых экранов. Для реализации таких атак злоумышленники используют различные сообщения ICMP:

- Эхозапрос и эхоответ ICMP – применяются для проверки доступности хостов и осуществления DoS-атак.
- Сообщения о недостижимости ICMP – используются для разведывательных атак и сканирования сети.
- Ответ ICMP с маской – помогает в создании карты внутренней структуры IP-сети.
- Перенаправления ICMP – могут быть использованы для того, чтобы заставить целевой хост отправлять весь трафик через взломанное устройство, что открывает возможности для атак через посредника.
- Обнаружение маршрутизатора ICMP – позволяет злоумышленникам вставлять ложные записи в таблицу маршрутизации целевого устройства.

Для защиты сетей необходимо применять строгую фильтрацию ICMP на границах сети с использованием списков контроля доступа (ACL), чтобы предотвратить зондирование из Интернета. Специалисты по безопасности должны уметь выявлять ICMP-атаки, анализируя захваченный трафик и журналы событий. В крупных сетях устройства безопасности, такие как межсетевые экраны и системы обнаружения вторжений (IDS), должны быть настроены на обнаружение подобных атак и выдачу предупреждений.

Межсетевые экраны и IDS часто развертываются для частичной автоматизации задач мониторинга трафика. Они сравнивают входящий трафик с административными правилами. Межсетевые экраны обычно проверяют на

соответствие правилам заголовков пакета, а IDS часто сравнивают с набором правил полезные данные пакета. Поскольку межсетевые экраны и IDS применяют предварительно определенные правила к различным частям IP-пакета, то правила IDS и правила межсетевого экрана имеют различные структуры.

Несмотря на различия в структуре правил, остаются некоторые сходства между компонентами правил. Например, правила межсетевого экрана и IDS содержат компоненты соответствия и действия. Действия предпринимаются после обнаружения соответствия.

Компонент соответствия определяет интересующие элементы пакета, такие как источник пакета, назначение пакета, протоколы транспортного уровня и порты, а также данные, включенные в полезную нагрузку пакета.

Компонент действия определяет, что следует сделать с пакетом, у которого компонент соответствует условиям, например, принять и переслать пакет, пропустить пакет или отправить пакет на дополнительный набор правил для дальнейшей проверки.

Стандартно межсетевой экран предназначен для отбрасывания всех пакетов по умолчанию при определении вручную, какой трафик должен быть разрешен. Известное под названием «отбрасывание по умолчанию», такое устройство экрана имеет преимущество при защите сети от неизвестных атак и протоколов. В рамках этой структуры обычно события отбрасывания пакетов записываются в журнал, поскольку они соответствуют пакетам, которые не были явно разрешены и таким образом нарушали политику организации. Такие события должны быть записаны для последующего анализа.

Еще одним распространенным типом атак является атака «отказ в обслуживании» (DoS). Основная цель таких атак – лишить законных пользователей доступа к веб-сайтам, электронной почте, учетным записям и другим онлайн-сервисам. Существует два основных источника DoS-атак:

1.Пакеты с неправильным форматированием. Злоумышленники создают пакеты с ошибками и отправляют их на уязвимые хосты, что может привести к сбоям или значительному замедлению работы.

2.Перегрузка трафиком. Злоумышленники направляют большой объем трафика на целевую сеть, хост или приложение, что также может вызвать сбой или замедление работы.

Эти угрозы подчеркивают важность эффективных мер безопасности для защиты сетевой инфраструктуры.

DDoS-атаки (Distributed Denial of Service,) аналогичны DoS-атакам, направлены на отказ в обслуживании, но отличаются по своей природе и масштабу. Основное различие между DoS и DDoS атаками заключается в количестве источников, используемых для атаки. DoS-атака осуществляется с одного компьютера или устройства. В этом случае злоумышленник отправляет множество запросов к целевому серверу, перегружая его и лишая легитимных пользователей доступа. Такие атаки легче обнаружить и остановить, так как они исходят только из одного IP-адреса, что делает их менее эффективными. DDoS-атака, напротив, происходит с множества устройств, которые могут быть частью ботнета – сети зараженных компьютеров, управляемых злоумышленником. Это позволяет атакующим генерировать гораздо больший объем трафика, что значительно усложняет обнаружение и защиту от атаки. DDoS-атаки могут использовать различные методы, такие как UDP-флуд, SYN-флуд и HTTP-запросы, что делает их более разнообразными и мощными.

Атаки с подменой представляют собой одну из наиболее распространенных и опасных форм киберугроз, в которых злоумышленники подделывают свою личность или идентификационные данные, чтобы обмануть системы безопасности и получить доступ к конфиденциальной информации. Эти атаки могут происходить через различные каналы связи, включая телефонные звонки, электронные письма и веб-сайты, и могут принимать различные формы, такие как подмена IP-адресов, DNS-спуфинг и подмена электронной почты.

Атаки с подменой могут проводиться в виде открытой подмены и подмены вслепую.

Открытая подмена используется злоумышленником для изучения пакета ответа от целевой жертвы. В этом случае злоумышленник может видеть трафик, который передается между хостом и целевым объектом. Целью открытой подмены может быть определение состояния межсетевого экрана, прогнозирование порядкового номера или перехват авторизованного сеанса. В случае подмены вслепую злоумышленник не видит трафик, который передается между хостом и целевым объектом. Подмена вслепую используется в DoS-атаках.

Атаки с подменой MAC-адресов используются, когда у злоумышленника есть доступ к внутренней сети. Злоумышленники изменяют MAC-адрес своего хоста в соответствии с другим известным MAC-адресом целевого хоста. Затем атакующий хост отправляет по сети кадр с только что заданным MAC-адресом. Когда коммутатор получает кадр, он проверяет MAC-адрес источника. Коммутатор перезаписывает текущую запись в таблице CAM и назначает MAC-адрес новому порту. Затем он пересылает кадры, предназначенные для целевого хоста, на атакующий хост [4].

Еще одним примером подмены является подмена приложения или службы. Злоумышленник может подключить мошеннический сервер DHCP, чтобы сформировать состояние «человек посередине» (англ. Man-In-The-Middle attack, MITM) [1]. Данная угроза представляет собой вид кибератак, при которых злоумышленник тайно перехватывает и при необходимости модифицирует связь между двумя сторонами, считающими, что они напрямую общаются друг с другом. Атака направлена на обход взаимной аутентификации или её отсутствие и может быть успешной в случае, если стороны не используют надлежащие меры защиты. Злоумышленник для достижения поставленной цели может осуществлять отправку поддельных ARP-пакетов в локальной сети с целью сопоставления MAC-адреса злоумышленника с IP-адресом жертвы (ARP-спуфинг), подмену записей DNS, перенаправляющая жертву на поддельный

сайт, контролируемый атакующим (DNS-спуфинг), отслеживать и перехватывать сетевой трафик с помощью специального программного обеспечения или оборудования для кражи информации (сниффинг трафика). Успешная атака посредника может привести к краже конфиденциальной информации, нарушению целостности передаваемых данных, внедрению вредоносного программного обеспечения в систему жертвы.

Для предотвращения атак типа «человек посередине» рекомендуются использовать протокол HTTPS для шифрования трафика между клиентом и сервером, применять VPN для создания защищенного туннеля при работе в публичных сетях, использовать менеджер паролей для генерации и хранения надежных паролей, регулярно обновлять системное и прикладное программное обеспечение для устранения известных уязвимостей.

Литература

1. Лазутин, А.И. Программно-аппаратные средства защиты информации: курс лекций / А.И. Лазутин. – Армавир: ГБПОУ КК АЮТ, 2019.
2. Старостенко, И.Н. Информационная безопасность: курс лекций / И.Н. Старостенко, Ю.Н. Сопильняк. – Краснодар: Краснодарский университет МВД России, 2012.
3. Старостенко, И.Н. Целенаправленные атаки (АРТ) и методы защиты от них // Проблемы информационного обеспечения деятельности правоохранительных органов. Материалы 3-й Международной научно-практической конференции, 2017. С.127-131.
4. Старостенко, И.Н. К вопросу обеспечения безопасности локальной сети на канальном уровне // Математические методы и информационно-технические средства. Материалы XV Всероссийской научно-практической конференции, 2019. С.171-174.

Сведения об авторе

Старостенко Игорь Николаевич, кандидат физико-математических наук, доцент, начальник кафедры информатики и математики Краснодарского университета МВД России.

**Толстых Марина Юрьевна,
Баханов Максим Валентинович**

ПРИЛОЖЕНИЕ-ДЕТЕКТОР ДЕСТРУКТИВНОГО КОНТЕНТА В МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЯХ ARFA

В современном цифровом обществе проблема распространения деструктивного контента [1] становится всё более актуальной. Особенно остро она стоит в сфере музыки, где деструктивный контент может оказывать негативное влияние на молодёжь и подростков, взрослую аудиторию, распространяясь под прикрытием безобидных средств воплощения художественных образов. В связи с этим возникает необходимость разработки эффективных методов и инструментов для обнаружения и предотвращения распространения такого контента.

На текущий момент отечественным законодательством не закреплено определение деструктивного контента, примерный перечень подобной информации содержится в ст. 5 так называемого закона об информационной безопасности детей [2]. Предлагается следующее возможное толкование: «Деструктивный контент – это информация, независимо от формы её представления, размещённая в цифровой среде, которая отрицательно влияет на индивидуальное сознание или социальную группу, способствуя развитию негативных, агрессивных, разрушительных или антисоциальных установок и поведения.» Таким образом, определение включает в себя, но не ограничивается, следующее:

1. Пропаганда насилия: материалы, которые призывают к физическому насилию или оправдывают его применение.

2. Ненавистнические высказывания: контент, который распространяет и популяризирует ненависть или дискриминацию на основе расы, пола, возраста, национальности, религии, сексуальной ориентации или любых других характеристик.

3. Материалы сексуального характера: откровенные сексуальные изображения или тексты, которые могут быть вредными или неуместными для определенных групп населения.

4. Пропаганда экстремизма: контент, который поддерживает и популяризирует экстремистские взгляды или террористическую деятельность.

5. Фальсификация информации: сознательное распространение ложной информации, которая может ввести в заблуждение или вызвать социальный разлад.

6. Содействие вредным привычкам: материалы, которые пропагандируют употребление наркотиков, алкоголя или табака, ведение асоциального образа жизни.

7. Цифровой моббинг: контент, который включает в себя унижение, запугивание или иное агрессивное поведение в отношении индивидуумов или групп в интернете.

8. Психологические манипуляции: информация, предназначенная для манипулирования чувствами, мнениями и решениями людей.

Одной из возможных технологий защиты от описанной и проклассифицированной выше угрозы деструктивного контента является разработанное приложение «ARFA». Программа включает в себя нейронную сеть [3], которая написана на языке Python на основе открытой программной библиотеки TensorFlow. Также в основе обучения лежит библиотека Keras, которая обеспечивает преобразования массива звуковых данных в понятный для программы текстовый. Обучение происходит на основе заранее размеченного массива данных, где деструктивная часть понижает общий показатель метрики. Поиск деструктивного контента осуществляется при помощи библиотеки Keras, нейронная сеть обнаруживает связи в предложении, а не ищет ключевые слова в облачном словаре.

Для того, чтобы грамотно и корректно обучить нейронную сеть, необходимо сформировать уникальный датасет. В данной программной

реализации на разных этапах ее создания были использованы 3 датасета: тестовый (10 строк из песен); токсичные комментарии (250 000 строк токсичных комментариев); финальный (вручную обработанные данные на более 100 000 строк из музыкальных произведений).

Датасет формируется при помощи технологии NLP (обработка естественного языка) для анализа и понимания человеческого языка, например, для синтаксического и семантического анализа текстов. Она дает машинам способность понимать и интерпретировать человеческий язык так, как это делают люди.

Процесс работы включает в себя решение широкого спектра задач: распознавание речи (преобразование устной речи в текст); понимание языка (анализ смысла слов, фраз и текстов); генерация языка (автоматическое создание текста на естественном языке); машинный перевод (автоматический перевод текста с одного языка на другой); извлечение информации (извлечение конкретной информации из текстов); автоматическое реферирование (создание краткого содержания больших текстов); анализ тональности (определение эмоциональной окраски текста или речи его автора).

Разработанная программа включает в себя два поля отображения информации: `textBox` с отображением текста песни, её метрика по частям, `listBox` с песнями ранее загруженными и имеющие готовый результат.

Функционал «ARFA» предусматривает (рис. 1): загрузку файлов вручную с компьютера; поиск по ранее загруженным композициям; кнопку запуска работы программы; удаление ранее загруженных треков; кнопку отображения метрики у загруженных песен; отдельный вывод под метрику и результат программы. Также предусмотрена отдельная возможность работы с парсером, а именно: поиск по сайту «Genius».

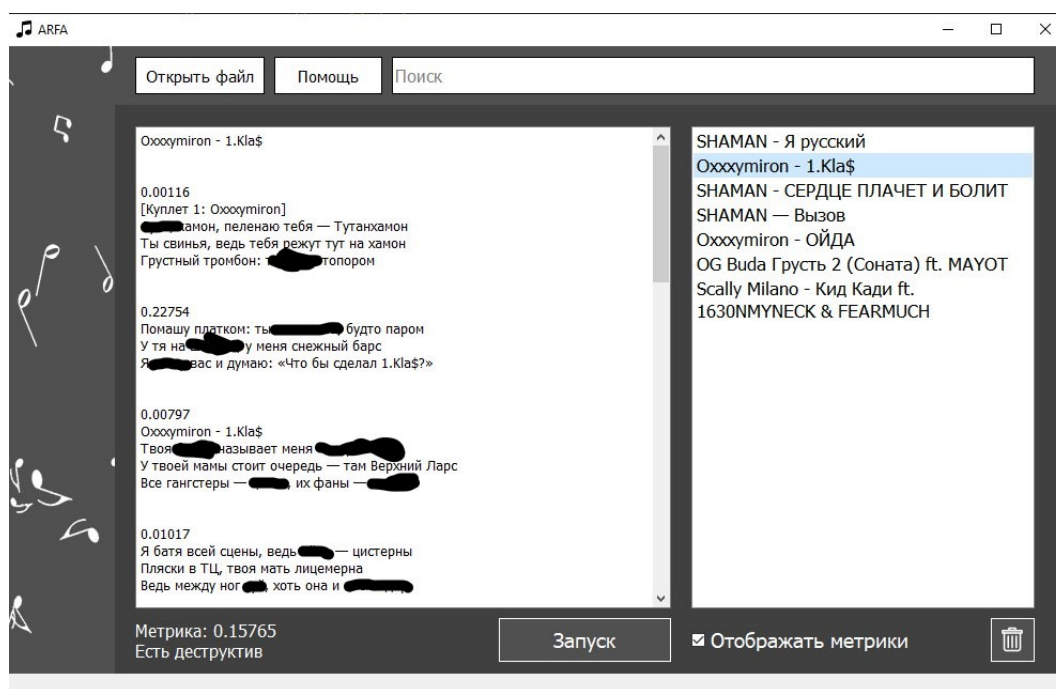


Рис.1. Интерфейс программы «ARFA», пример оценки песни «Оххуmiron- 1.Kla\$» на деструктивность

Оценка деструктивности музыкального произведения выстраивается на принципах нечеткой математики: градация от 0 (деструктивный контент) до 1 (недеструктивный контент). Однако, если в треке существуют строчки, которые содержат деструктивный контент ($<0,51$), то трек автоматически заносится в реестр недоброжелательных треков.

Разработка приложения-детектора деструктивного контента в музыкальных произведениях «ARFA», на наш взгляд, является значительным шагом в сторону повышения цифровой безопасности и защиты пользователей от потенциально деструктивного контента. Проект демонстрирует, как с помощью современных методов обработки естественного языка и машинного обучения можно эффективно анализировать текстовый и аудиовизуальный контент на предмет наличия запрещенных или опасных элементов.

В будущем исследования могут быть направлены на улучшение алгоритмов распознавания, расширение базы данных для обучения и тестирования, а также интеграцию с другими платформами и сервисами., что укрепит позиции «ARFA» как важного инструмента в борьбе с

распространением деструктивного контента и воспитании осознанного и безопасного подхода к потреблению медиапродуктов.

Литература

1. Цимбал, В.Н. Противодействие деструктивному контенту в сети Интернет / В.Н. Цимбал, М.Ю. Толстых. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – 52 с.

2. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (последняя редакция) // URL: <http://publication.pravo.gov.ru> (дата обращения: 30.05.2024).

3. Романюта, Д.Ю. Исследование алгоритма Виолы-Джонса для разработки системы распознавания лиц с помощью нейронных сетей / Д.Ю. Романюта, А. В. Коваленко, М. В. Шарпан // Инженерный вестник Дона. – 2024. – № 1(109). – С. 739-751.

Сведения об авторах

Толстых Марина Юрьевна, кандидат технических наук, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя.

Баханов Максим Валентинович, курсант Московского университета МВД России имени В.Я. Кикотя.

**Толстых Марина Юрьевна,
Быков Даниил Русланович**

ЦИФРОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИКОВ

Количество преступлений, связанных с незаконным оборотом наркотиков в России в период январь – сентябрь 2023 года выросло на 8,8 % по сравнению с аналогичным отчетным периодом, что подтверждается статистическими сведениями, представленными МВД России.

На заседании Государственного антинаркотического комитета, проводимом летом текущего года и включающим в себя среди прочих вопрос об антинаркотической пропаганде в цифровой среде, Министр правоохранительного ведомства Владимир Колокольцев подчеркнул, что ведутся активные работы в медиа среде, цифровых ресурсах и сервисах. К таковым относятся сайты и интернет-страницы, социальные сети, новостные и развлекательные телеграмм-каналы, медиаресурсы и пр.

Экспертным сообществом признается, что способы осуществления преступной деятельности активно трансформируются посредством передовых цифровых инструментов и современных информационно-технических средств и систем. Отмеченное актуально и для незаконного оборота наркотиков.

За последнее десятилетие Интернет стал рынком сбыта, онлайн площадкой для торговли наркотиками, а с учетом уровня технических знаний преступников, необходимого для сокрытия сделок от правоохранительных органов, торговля наркотиками через глобальную сеть становится все более распространенной.

К причинам распространения и увеличения данной угрозы можно отнести:

- анонимность операций (благодаря использованию технологий анонимизации, таких как шифрование, VPN и прокси-серверы, преступники уклоняются от идентификации, поскольку весьма затруднительно с технической и правовой стороны отследить и установить преступников);

- глобальный охват пользователей (Интернет позволяет охватить более широкую клиентскую базу, что на почве анонимности в коммуникации между

продавцом и покупателем, устраняет необходимость физического взаимодействия);

- ресурсы для обмена знаниями и опытом (глобальная сеть инкапсулирует колоссальное количество информации об изучаемой преступной деятельности, включая инструкции по приготовлению наркотиков, методы приобретения незаконных химических веществ-прекурсоров, сведения об услугах по распространению, по переводу оплаты, которая теперь может быть в кибервалюте, процедуры сокрытия, позволяющие избежать обнаружения правоохранительными органами).

В динамике наблюдается рост потребления наркотиков несовершеннолетними и молодежью. В подобных условиях особое значение приобретает профилактический подход в борьбе с наркопреступностью, при котором приоритетное значение в методах и средствах борьбы, на наш взгляд, должно быть отдано информации.

Цифровые данные, циркулирующие в медиа среде (интернет-сайтах, ресурсах, сервисах, мессенджерах и аналогичных репозиториях), участвуют в формировании общественного мнения по определенным проблемам, в том числе по борьбе с наркопреступностью. Указанный факт не следует игнорировать в осуществлении правоохранительной деятельности по направлению противодействия незаконному обороту наркотиков. Информация часто позиционируется как оружие, следовательно, силу пропаганды не следует умалять. Грамотное представление «полезной» информации может способствовать популяризации здорового образа жизни, расширению гражданских ценностей и достижению благополучия пользователей медиа среды. На наш взгляд, актуальным является продвижение профилактических программ, распространяемых в медиа среде и направленных на просвещение молодежи о рисках, связанных со злоупотреблением наркотическими веществами и последствиях от указанных действий.

Кроме того, перспективным видится применение технологий искусственного интеллекта для идентификации любых триггеров преступной

деятельности, связанной с наркотиками. Так, цифровые технологии возможно использовать в качестве парсера, т.е. интеллектуального поисковика и агрегатора массивов информации о названиях торговых наркоплощадок, жаргоне преступников, производстве платежей и ряде других важных сведений. Корректно настроенные нейронные сети могут обрабатывать и анализировать полученные метаданные, активно обучаясь в процессе работы, предоставлять четкие, краткие и действенные рекомендации для сотрудников правоохранительных органов практически в режиме реального времени. Выходные сведения могут быть предикатного типа: предсказание места и времени сбыта, прогноз состава наркотического вещества и психоактивного эффекта от употребления.

Поскольку влияние наркопреступности сказывается на деятельность как государства, так и общества, отдельных сферах безопасности, здравоохранения и экономики, борьба с незаконным оборотом наркотиков требует коллективного и скоординированного реагирования со стороны правительства, правоохранительных органов, специализированных организаций и гражданского общества в целом. Вместе с социально-административным и организационным аспектом следует также учитывать технический, прикладной, цифровой. Тенденция перехода на цифровые технологии влияет на каждого человека, общество, и должна применяться в целях обеспечения безопасности. В указанном процессе лидерами должны выступать правоохранительные органы, как гарант защиты общества, оснащенный всеми необходимыми современными знаниями и цифровыми компетенциями.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 12.10.2023) // СПС «Консультант Плюс» [Электронный ресурс] <https://www.consultant.ru> (дата обращения: 05.05.2024).

2. Пакляченко, М.Ю. Инструментарий цифровизации деятельности полиции / М.Ю. Пакляченко // Математические методы и информационно-технические средства: Материалы XVIII Международной научно-практической конференции, Краснодар, 17 июня 2022 года / Редколлегия: И.Н. Старостенко, Е.В. Михайленко, А.В. Еськов [и др.]. – Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2022. – С. 131-134.

3. Черняков, С. А. О роли Белгородского юридического института МВД России имени И.Д. Путилина в противодействии незаконному обороту наркотиков / С. А. Черняков // Противодействие незаконному обороту наркотиков в условиях цифровизации общества: сборник материалов Международной научно-практической конференции, Белгород, 17 ноября 2022 года. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2023. – С. 181-186.

4. Чиненов, А.В. О некоторых проблемах противодействия преступлениям, связанным с незаконным оборотом наркотиков, совершаемым с использованием ИКТ / А. В. Чиненов // Противодействие незаконному обороту наркотиков в условиях цифровизации общества: сборник материалов Международной научно-практической конференции, Белгород, 17 ноября 2022 года. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина, 2023. – С. 186-189.

Сведения об авторах

Толстых Марина Юрьевна, кандидат технических наук, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя.

Быков Даниил Русланович, курсант Московского университета МВД России имени В.Я. Кикотя.

**Халафян Алексан Альбертович,
Авраменко Александр Алексеевич,
Патрушев Руслан Сергеевич**

ПОСТРОЕНИЕ ПРОГНОСТИЧЕСКИХ МОДЕЛЕЙ МЕТОДАМИ DATA MINING ДЛЯ ПРИНЯТИЯ ОБОСНОВАННЫХ КЛИНИЧЕСКИХ РЕШЕНИЙ В СТОМАТОЛОГИИ

В современной стоматологической практике ключевую роль играют не только клинические навыки врача, но и применение передовых технологий для анализа медицинских данных и прогнозирования результатов лечения. Одной из таких технологий является Data Mining, метод, позволяющий извлекать скрытые закономерности и информацию из больших объемов данных. В данной статье мы рассмотрим применение Data Mining в стоматологии для построения прогностических моделей и принятия обоснованных клинических решений.

Статья посвящена использованию методов машинного обучения и искусственного интеллекта для выявления взаимосвязи клинических параметров с прогрессированием пародонтита/утратой зубов и разработке прогностической модели для возможности принятия обоснованных клинических решений.

Data Mining – это мощный инструмент для анализа клинических данных и выявления взаимосвязей между различными факторами заболеваний полости рта и эффективностью лечения. Путем анализа больших объемов данных, содержащих информацию о состоянии зубов, десен, а также о медицинской истории пациентов, можно выявить скрытые закономерности, которые могут быть использованы для построения прогностических моделей.

Рассмотрим регрессию и классификацию методом автоматизированных нейронных сетей на примере таблицы данных полученных из дневниковых записей пациентов, которые были пролечены в период с 2000 по 2006 годы по поводу хронического генерализованного пародонтита легкой, средней и тяжелой степени (активная пародонтальная терапия, АПЛ) и длительно наблюдавшихся в четырех стоматологических учреждениях до 2021 года. Для анализа было отобрано 109 из 236 просмотренных медицинских карт стоматологического

пациента в соответствии с критериями включения/ невключения. Важность изучения данной проблемы заключается в своевременной постановке верного диагноза и проведении необходимого лечения. Отсутствие лечения пародонтита в дальнейшем приводит к пародонтозу, при котором разрушается костная ткань и начинают выпадать зубы.

На рисунке 1 представлен фрагмент исходных данных.

1	Пол	Возраст	Курение	ОСЗ	АПЛ	Диагноз	ИН	ЧЗЗ	ГЗ 1	ГЗ 2	ГЗ 3	%Кр(зубы)	i	ГЗ 1	ГЗ 2	кр	ИН**	ЧЗЗ**	ГЗ 1**	%Кр(зубы)**	Риск
2	ж	30-54	курит	нет	рег. пар. хир.	средняя	0,4	25	20	4	4	11,18	2	2	0	0	0,42	23	23	7,14	низкий
3	м	55-70	не курит	нет	рег. пар. хир.	тяжелая	0,54	23	22	1	0	11,54	5	5	0	0	0,53	21	16	12,67	низкий
4	м	55-70	курит	нет	рег. пар. хир.	средняя	0,44	23	23	0	0	11,42	5	5	0	0	0,45	22	22	12,23	низкий
5	м	55-70	не курит	нет	рег. пар. хир.	тяжелая	0,68	20	20	4	6	7,73	7	7	0	0	0,48	20	18	8,42	высокий
6	ж	30-54	не курит	нет	рег. пар. хир.	легкая	0,48	26	26	0	0	3,84	2	2	0	0	0,42	25	25	15,12	низкий
7	м	55-70	не курит	нет	рег. пар. хир.	тяжелая	0,38	20	17	2	1	9,44	6	5	1	0	0,53	19	11	5,67	высокий
8	м	55-70	не курит	есть	рег. пар. хир.	тяжелая	0,34	20	18	2	0	7,77	6	6	0	0	0,42	19	16	8,14	высокий
9	м	30-54	не курит	нет	рег. пар. хир.	легкая	0,36	28	28	0	0	4,41	0	0	0	0	0,52	28	28	4,34	низкий
10	ж	30-54	не курит	нет	рег. пар. хир.	легкая	0,84	26	26	0	0	11,9	2	2	0	0	0,31	26	26	4,22	низкий
11	ж	55-70	не курит	есть	рег. пар. хир.	тяжелая	1,3	20	12	7	1	20,9	0	0	0	0	0,63	19	16	17,04	высокий
12	ж	55-70	не курит	есть	рег. пар. хир.	тяжелая	1,32	20	19	1	0	17,1	6	6	0	0	1,3	20	0	13,15	высокий
13	м	55-70	не курит	есть	рег. пар. хир.	тяжелая	1,11	20	5	8	7	45,05	4	4	0	0	0,33	20	11	9,8	высокий
14	м	55-70	не курит	есть	рег. пар. хир.	средняя	0,48	22	19	3	0	10,12	6	6	0	0	0,37	22	22	9,38	низкий
15	ж	30-54	не курит	нет	рег. пар. хир.	тяжелая	0,45	24	22	2	0	10,67	4	4	0	0	0,38	24	22	7,38	низкий
16	м	30-54	не курит	нет	рег. пар. хир.	легкая	0,34	26	26	0	0	7,15	2	2	0	0	0,3	26	26	7,57	низкий
17	ж	30-54	курит	есть	рег. пар. хир.	тяжелая	1,54	23	10	8	5	11,05	0	0	0	0	1,74	18	0	7,17	высокий
18	ж	30-54	не курит	есть	рег. пар. хир.	тяжелая	0,38	22	20	2	0	12,13	5	5	0	0	0,41	22	22	9,14	низкий
19	ж	30-54	курит	нет	рег. пар. хир.	тяжелая	0,57	26	26	0	0	12,05	2	2	0	0	0,34	24	24	8,25	высокий
20	м	30-54	не курит	нет	рег. пар. хир.	средняя	0,42	25	25	0	0	7,13	3	3	0	0	0,44	22	22	7,58	низкий
21	м	30-54	не курит	нет	рег. пар. хир.	легкая	0,34	28	28	0	0	11,41	0	0	0	0	0,47	28	28	4,34	низкий
22	ж	30-54	не курит	есть	рег. пар. хир.	средняя	0,7	24	20	4	0	14,05	6	6	0	0	0,53	21	21	7,13	низкий
23	ж	55-70	не курит	нет	рег. пар. хир.	тяжелая	0,35	25	24	1	0	10,13	4	4	0	0	0,75	24	24	10,21	низкий
24	ж	30-54	не курит	есть	рег. пар. хир.	средняя	0,31	24	24	0	0	11,7	5	5	0	0	0,35	23	23	6,17	низкий
25	ж	55-70	не курит	есть	рег. пар. хир.	средняя	0,41	26	23	3	0	12,13	0	0	0	0	0,37	24	23	7,18	высокий
26	ж	30-54	не курит	есть	рег. пар. хир.	легкая	0,65	27	27	0	0	8,41	2	2	0	0	0,47	26	26	4,34	низкий
27	м	30-54	не курит	нет	рег. пар. хир.	легкая	0,84	26	26	0	0	11,19	2	2	0	0	0,53	26	26	7,71	низкий
28	м	30-54	не курит	нет	рег. пар. хир.	легкая	0,44	27	26	1	0	7,15	2	2	0	0	0,3	26	26	6,57	низкий
29	ж	30-54	не курит	нет	рег. пар. хир.	легкая	0,8	26	26	0	0	11,9	2	2	0	0	0,41	26	26	4,22	низкий
30	м	55-70	не курит	нет	рег. пар. хир.	тяжелая	0,58	22	20	2	0	15,32	6	6	0	0	0,48	22	22	5,46	низкий

Рис.1. Фрагмент данных

Для того, чтобы реализовать метод автоматизированных нейронных сетей для решения задач классификации или регрессии в STATISTICA был использован пакет «Добыча данных».

В результате построения модели классификации была (рис. 2) был выбрана сеть 3 с лучшим результатом, так как точность прогноза на обучающей и тестовой выборках достигла 88% и 87% соответственно. На контрольной выборке точность 75%.

Итоги моделей (Таблица прогноз2.sta)								
N	Архитектура	Производительность обуч.	Контр. производительность	Тест. производительность	Алгоритм обучения	Функция ошибки	Ф-я актив. скрытых нейр.	Ф-я актив. выходных нейр.
1	MLP 24-12-2	75,32468	81,25000	81,25000	BFGS 4	Сум. квадр.	Логистическая	Экспонента
2	MLP 24-11-2	88,31169	81,25000	81,25000	BFGS 5	Сум. квадр.	Гиперболическая	Тожественная
3	MLP 24-5-2	88,31169	75,00000	87,50000	BFGS 2	Сум. квадр.	Тожественная	Логистическая
4	MLP 24-7-2	85,71429	81,25000	81,25000	BFGS 6	Энтропия	Тожественная	Софтмакс
5	MLP 24-11-2	88,31169	81,25000	81,25000	BFGS 5	Сум. квадр.	Логистическая	Гиперболическая

Рис. 2. Итоги автоматического построения нейронных сетей

Отобразим веса нейронных сетей промежуточных слоев нейронной сети для каждой модели в рамке активных нейронных сетей.

На рисунке 3 первом столбце указаны обозначения нейронов промежуточных слоев, в том числе привязанных к независимым переменным на входе и зависимым на выходе. Во втором столбце указаны сами веса.

Веса ID	Веса (Таблица прогноз2.sta)	
	Соединения 3.MLP 24-5-2	Значения весов 3.MLP 24-5-2
1	ИН -> скрытый нейрон 1	-0,47138
2	ЧСЗ -> скрытый нейрон 1	0,34318
3	ГЗ 1 -> скрытый нейрон 1	0,30931
4	ГЗ 2 -> скрытый нейрон 1	-0,32221
5	ГЗ 3 -> скрытый нейрон 1	-0,22030
6	% Кр (зубы) -> скрытый нейрон 1	-0,23950
7	i -> скрытый нейрон 1	0,23487
8	ГЗi 1 -> скрытый нейрон 1	0,28264
9	ГЗi 2 -> скрытый нейрон 1	-0,17088
10	крі -> скрытый нейрон 1	-0,06649
11	пол(ж) -> скрытый нейрон 1	0,09499
12	пол(м) -> скрытый нейрон 1	-0,12952
13	возрастная группа(30-54) -> скрытый нейрон 1	0,67822
14	возрастная группа(55-70) -> скрытый нейрон 1	-0,72551
15	курение(курит) -> скрытый нейрон 1	0,15323
16	курение(не курит) -> скрытый нейрон 1	-0,21029
17	ОСЗ(есть) -> скрытый нейрон 1	-0,59208
18	ОСЗ(нет) -> скрытый нейрон 1	0,54108
19	АПЛ(консерв. тер.) -> скрытый нейрон 1	-0,83219
20	АПЛ(рег. пар. хир.) -> скрытый нейрон 1	0,73923

Рис. 3. Таблица весов нейронов

По данным анализа было разработано интерфейсное окно, которое, используя введенные данные, прогнозирует прогрессирование пародонтита в периоде поддерживающего лечения.

Прогнозирование пародонтита

Пол	ж	Индекс налета	0,4	Процент кровоточивости десны вокруг зубов	11,18
Возраст	30-54	Число сохраненных зубов	25	Число зубных имплантов	2
Курение	курит	Глубина поддесневого зондирования вокруг зубов:		Глубина зондирования десны вокруг имплантата:	
ОСЗ	нет	ГЗ 1 - глубина зондирования <= 4mm	20	ГЗi 1 - глубина зондирования <= 3mm	2
АПЛ	рег. пар. хир.	ГЗ 2 - глубина зондирования = 4-6mm	4	ГЗi 2 - глубина зондирования >= 3mm	0
Диагноз	средняя	ГЗ 3 - глубина зондирования >= 6mm	4	Число имплантатов с кровоточивостью десны, окружающей имплант	4
Индекс налета(отдаленный результат => 5 лет)		1,77			
Число сохраненных зубов(отдаленный результат => 5 лет)		24			
Глубина зондирования <= 4mm(отдаленный результат => 5 лет)		22			
Процент кровоточивости десны вокруг зубов(отдаленный результат => 5 лет)		9,38			
Уровень Риска		низкий			
Рассчитать					

Рис. 4. Работа приложения

Для реализации использовалась библиотека Tkinter.

Tkinter – это графическая библиотека, которая позволяет создавать программы с оконным интерфейсом. Эта библиотека представляет собой интерфейс к Python и инструмент создания графических приложений tcl/tk.

Для реализации интерфейсного окна использовался язык программирования Python.

В результате проделанной работы нами было создано приложение, для прогнозирования пародонтита в периоде поддерживающего лечения. (Рисунок 4).

Литература

1. Лекция 5. Data mining и перегрузка информацией URL - <https://studfile.net/preview/6172588/>
2. Классификация - Гуманитарный портал URL - <https://gtmarket.ru/concepts/6879#:~:text=Классификация%20–%20это%20общенаучный%20метод,сходства%20в%20определённых%20сущностных%20свойствах>
3. Основы линейной регрессии ХАБР URL - <https://habr.com/ru/post/514818/>
4. Общие сведения о языке программирования python URL - <https://clck.ru/qAvLB>
5. Tkinter в Python: руководство по использованию URL - <https://highload.today/tkinter-v-python/>

Сведения об авторах

Халафян Алексан Альбертович, доктор технических наук, доцент, профессор кафедры анализа данных и искусственного интеллекта Кубанского государственного университета.

Авраменко Александр Алексеевич, студент Кубанского государственного университета.

Патрушев Руслан Сергеевич, студент Кубанского государственного университета.

Хромых Анна Алексеевна

ПОСТРОЕНИЕ АДДИТИВНОЙ МОДЕЛИ ВРЕМЕННОГО РЯДА, ХАРАКТЕРИЗУЮЩЕГО КОЛИЧЕСТВО ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ С ПОСТРАДАВШИМИ НА ТЕРРИТОРИИ КРАСНОДАРСКОГО КРАЯ

В современном мире все стремительно меняется. По мере роста городов увеличиваются и расстояния, которые люди преодолевают каждый день. Это приводит к увеличению количества транспорта, в следствии чего увеличивается количество пробок и дорожно-транспортных происшествий [4, 6, 7].

В данной статье проводится статистический анализ временного ряда, характеризующего количество дорожно-транспортных происшествий с пострадавшими на территории Краснодарского края в период с января 2020 года по декабрь 2023 года (табл. 1) [5] и строится прогноз на первые два квартала 2024 года.

Таблица 1. Количество дорожно-транспортных происшествий

Год	Квартал	ДТП	Год	Квартал	ДТП
2020	I	1384	2022	I	994
	II	1305		II	1425
	III	2031		III	1712
	IV	1640		IV	1678
2021	I	1098	2023	I	1086
	II	1433		II	1474
	III	1742		III	1886
	IV	1683		IV	1709

Ниже приводится график исследуемых данных (рис. 1).

Не сложно заметить, что в период с января 2020 года по декабрь 2023 года явно выражена цикличность количества дорожно-транспортных происшествий. Ежегодно наибольшее значение наблюдается в третьем квартале, так в 2020 году зафиксировано 2031 происшествий, 2021 году – 1742, 2022 году – 1712, 2023 году – 1886.

Математическую модель прогноза количества дорожно-транспортных происшествий строим поэтапно по следующему алгоритму [1].



Рис. 1. Количество дорожно-транспортных происшествий, зарегистрированных в Краснодарском крае

На первом этапе определим вид модели временного ряда. Не сложно заметить, что амплитуда сезонных колебаний приблизительно постоянна (рис. 1), следовательно, для прогнозирования строим аддитивную модель временного ряда:

$$Y = T \cdot S \cdot E,$$

где T – трендовая компонента, S – циклическая (сезонная) компонента, E – случайная компонента.

На втором этапе изучим значения автокорреляционной функции. Для выявления сезонности (циклическости) определим коэффициенты автокорреляции уровней ряда $\tau=1, 2, \dots, 9$ (табл. 2) [3, 8]:

$$r(\tau) = \frac{(n-\tau) \sum_{t=\tau+1}^n y_t y_{t+\tau} - \sum_{t=\tau+1}^n y_t \sum_{t=\tau+1}^n y_{t+\tau}}{\sqrt{(n-\tau) \sum_{t=\tau+1}^n y_t^2 - \left(\sum_{t=\tau+1}^n y_t\right)^2} \sqrt{(n-\tau) \sum_{t=1+\tau}^n y_{t+\tau}^2 - \left(\sum_{t=1+\tau}^n y_{t+\tau}\right)^2}}.$$

Результаты вычислений представлены в таблице 2.

Таблица 2. Значения автокорреляционной функции временного ряда

τ	$r(\tau)$
1	-0,0272
2	-0,7854
3	-0,0379
4	0,8775
5	0,0003
6	-0,9075
7	-0,0186
8	0,7894
9	0,0617

Анализ значений автокорреляционной функции позволяет сделать вывод о наличии в изучаемом временном ряде сезонной составляющей (сезонных колебаний) с периодичностью в $\tau = 4$ квартала (рис. 2).



Рис. 2. Коррелограмма временного ряда

На третьем этапе произведем расчет значений компонент T , S и E для каждого уровня ряда выполнив следующие действия:

- 1) выравнивание исходного ряда методом скользящей средней;
- 2) расчет значений сезонной компоненты S ;
- 3) устранение сезонной компоненты из исходных уровней ряда и получение выровненных данных $(T+E)$ в модели;
- 4) аналитическое выравнивание уровней $(T+E)$ и нахождение значений линейного тренда T ;
- 5) расчет полученных по модели значений $(T+ S)$;
- 6) расчет ошибок модели.

Все найденные значения компонент аддитивной модели временного ряда представлены в таблице 2. В столбце 1 указаны исходные значения изучаемого показателя y_t , в столбце 3 – значения сезонной компоненты S_j , в столбце 4 – значения трендовой компоненты T , в столбце 6 – значение случайной компоненты E .

Таблица 2. Значения компонент аддитивной модели временного ряда

Квартал/год	1	2	3	4	5	6
	t	y_t	S_j	$T(t)$	$T+S$	E
I, 2020	1	1384	-435,17	1557,08	1121,92	262,08
II, 2020	2	1305	-53,29	1551,81	1498,51	-193,51
III, 2020	3	2031	322,21	1546,53	1868,74	162,26
IV, 2020	4	1640	166,25	1541,25	1707,50	-67,50
I, 2021	5	1098	-435,17	1535,97	1100,81	-2,81
II, 2021	6	1433	-53,29	1530,69	1477,40	-44,40
III, 2021	7	1742	322,21	1525,42	1847,63	-105,63
IV, 2021	8	1683	166,25	1520,14	1686,39	-3,39
I, 2022	9	994	-435,17	1514,86	1079,69	-85,69
II, 2022	10	1425	-53,29	1509,58	1456,29	-31,29
III, 2022	11	1712	322,21	1504,31	1826,51	-114,51
IV, 2022	12	1678	166,25	1499,03	1665,28	12,72
I, 2023	13	1086	-435,17	1493,75	1058,58	27,42
II, 2023	14	1474	-53,29	1488,47	1435,18	38,82
III, 2023	15	1886	322,21	1483,19	1805,40	80,60
IV, 2023	16	1709	166,25	1477,92	1644,17	64,83

Визуально графическая интерпретация результатов вычислений представлена на рисунке 2.

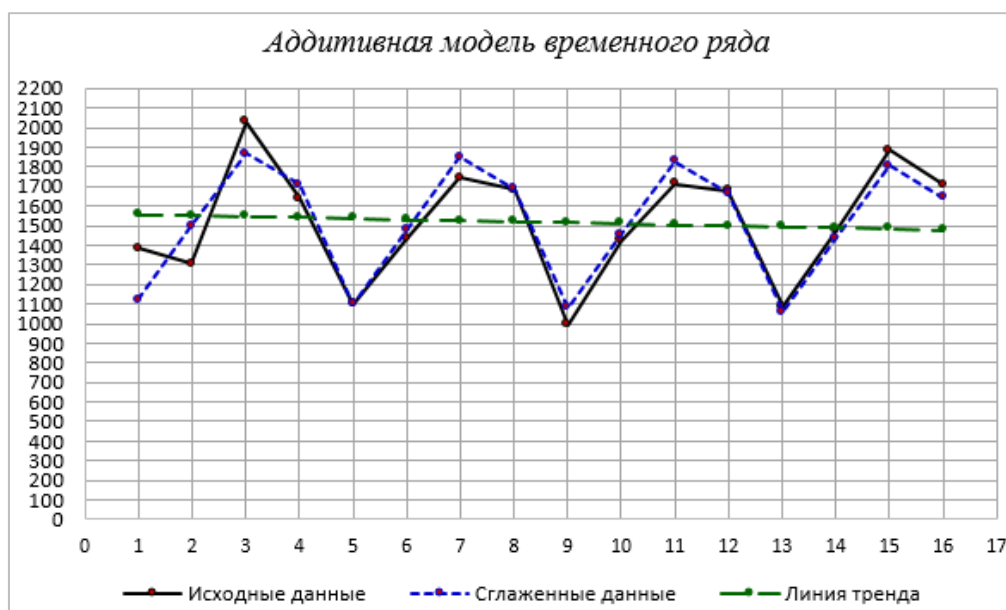


Рис 2. Аддитивная модель временного ряда

На следующем этапе исследования проверим построенную аддитивную модель на адекватность, для этого вычислим коэффициент детерминации [2]:

$$R^2 = 1 - \frac{\sum E^2}{\sum (y_t - \bar{y})^2}.$$

В нашем случае он равен $R^2 = 0,8589$. Таким образом, построенная аддитивная модель объясняет 85,89% общей вариации уровней временного ряда.

На завершающем этапе нашего исследования вычислим прогноз на первые два квартала 2024 года (табл. 3):

$$y_{17} = S_{17} + T_{17}, y_{18} = S_{18} + T_{18}.$$

Таблица 3. Прогнозные значения

Квартал/год	1	2	3	4
	t	T(t)	S _i	T+S
I, 2024	17	1472,64	-435,17	1037,47
II, 2024	18	1467,36	-53,29	1414,07

Таким образом, в первом квартале 2024 года ожидается 1037 ДТП, а во втором квартале – 1414.

В заключение следует отметить, что проблеме прогнозирования количества дорожно-транспортных происшествий уделяется особое внимание. Это связано с тем, что от правильной оценки ситуации с аварийностью на дорогах зависит своевременное принятие необходимых мер по управлению профилактикой ДТП со стороны организаций, обеспечивающих безопасность дорожного движения.

Литература

1. Анализ одномерных временных рядов: методические указания / О.Г. Модникова [и др.]. – М.: МАДИ, 2019. – 36 с.
2. Астафьев, Е. Р. Методы корреляционного и регрессивного анализа обработки статистических данных: учеб. пособие / Е.Р. Астафьев, Е.В. Михайленко. – Краснодар: Краснодарская академия МВД России, 2006.

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

4. Есина, М.Г. Построение модели прогнозирования количества дорожно-транспортных происшествий в Российской Федерации / М.Г. Есина, О.В. Хонгорова, И.Ю. Шарабанова, С.В. Базанов // Современные проблемы гражданской защиты. 2018. №2 (27). URL: <https://cyberleninka.ru/article/n/postroenie-modeli-prognozirovaniya-kolichestva-dorozhno-transportnyh-proisshествiy-v-rossiyskoy-federatsii> (дата обращения: 05.09.2024).

5. Краснодарский край в цифрах. 2023: Стат. сб. / Краснодарстат – Краснодар, 2024. – 169 с.

6. Ларионов, К.О. Прогнозирование статистических данных автомобильных дорожно-транспортных происшествий / К.О. Ларионов // Проблемы Науки. 2021. №6 (163). URL: <https://cyberleninka.ru/article/n/prognozirovanie-statisticheskikh-dannyh-avtomobilnyh-dorozhno-transportnyh-proisshествiy> (дата обращения: 05.09.2024).

7. Прокофьева, К.Д. Прогнозирование дорожно-транспортных происшествий в Пермском крае на основе математических многофакторных моделей / К.Д. Прокофьева, А.С. Федосеева // Управление строительством. – 2018. – № 3(12). – С. 123-129.

8. Старостенко, И.Н. Элементы статистической обработки данных: Учебное пособие / И.Н. Старостенко, А.А. Хромых. – Краснодар: КрУ МВД России, 2020.

Сведения об авторе

Хромых Анна Алексеевна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России.

**Чижов Илья Александрович,
Дрога Андрей Анатольевич**

ВИДЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Ни для кого ни секрет, что с каждым годом набирает всё большие обороты информационное развитие общества. Использование всё новых автоматизированных систем обработки и хранения информации зачастую облегчает многие сферы деятельности человека, позволяет выполнять многочисленные действия дистанционно, а также расширяет возможности для общения. Именно поэтому данные технологии являются уже составной жизнью практически каждого человека. Безусловно, невозможно очертить круг всех преимуществ внедрения и развития информационных технологий для нашей жизни, ввиду их разностороннего применения. Однако, конечно же, стоит понимать, что у данного явления имеются и свои существенные минусы. Так, активное использование информационных технологий, а также их стремительное развитие создало «твёрдую почву» для совершения противоправных действий. Масштабы данных преступлений с каждым годом лишь только стремительно набирают обороты. В настоящий промежуток времени, одним из наиболее популярных преступлений, совершенных с использованием информационных технологий является мошенничество с использованием информационных средств платежа. Разберёмся в данном вопросе подробнее.

Прежде всего, перед рассмотрением поставленного вопроса, необходимо понимать, что, в соответствии с п. 19 ст. 3 Федерального закона от 27 июня 2011 г. N 161-ФЗ «О национальной платёжной системе» электронное средство платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных

технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Также, согласно Уголовного Кодекса Российской Федерации (ч.1, ст. 159) мошенничество- «есть хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием». При этом, под понятием «электронное средство платежа» понимается такое средство, через которое непосредственно возможно осуществление безналичных денежных переводов с применением электронных носителей (чаще всего таким средством является банковская карта).

К сожалению, на сегодняшний день мошенники разработали достаточное количество способов совершения преступлений с использованием электронных средств платежа [3]. Указанное положение является следствием того, что информационное развитие делает людей более уязвимыми к таковому роду преступлений, ввиду недостаточной осведомленности о методах защиты и безопасности в данной среде, малой правовой образованности.

Так, согласно официальным статистическим данным, в России количество заявлений о мошенничестве по сравнению с прошлыми годами выросло на 5,1%, что превысило 249 тысяч [4]. Данную тенденцию к развитию числа такового вида преступлений можно объяснить тем, что в последнее время наличные деньги по сравнению со средствами электронного платежа используются менее активно. Такое явление, в большинстве своём, обусловлено многочисленными преимуществами операций, произведённых при помощи электронных средств платежа. К таковым может относиться простота в использовании, а также быстрота выполнения многих действий и операций.

Как уже было сказано ранее, ввиду трансформации способов совершения преступлений в цифровом формате, на сегодняшний день увеличилось количество видов мошенничества с электронными средствами платежа. Рассмотрим некоторые из них.

Так, одним из таких видов мошенничества является фрод. Фрод – «вид мошенничества в области информационных технологий, представляющий собой несанкционированные действия и неправомерное пользование ресурсами и услугами в сетях связи». Фрод осуществляется самыми различными способами, например: подменой доменов, которые ведут на иные, или незащищенные сайты; либо невидимыми объявлениями, при которых рекламу прячут так, чтобы пользователь не смог ее увидеть (одна реклама спрятана за другую - в связи с этим переход по «внешней» рекламе считается осуществленным по «внутренней»); либо мотивированным трафиком, при котором рекламу размещают в сторонних приложениях, обещая тем или иным пользователям бонусы за переходы по сторонним ссылкам.

Фишинг – получение конфиденциальных данных пользователя, выраженное в создании сайта (или ином способе), который будет пользоваться доверием у пользователей, лицами, стремящимися совершить мошеннические операции. В данном случае так называемые мошенники, например, создают сайт, похожий на сайт банка пользователя, через который впоследствии и происходит хищение реквизитов платежных карт [3]. В таком случае мошенники могут создать рассылку от якобы настоящего банка, в которой скажут об изменениях, проводимых в системе безопасности «доверительного учреждения» [1]. Так, естественно, поступит запрос о введении данных карты (логина, пароля) для того, чтобы войти в указанный банк (обновив данные карты). В данном случае и происходит хищение денежных средств, находящихся на карте. При этом нередки случаи фишинга в форме телефонного разговора. Так, мошенник, представляющийся сотрудником банка, якобы в целях обеспечения безопасности платежных средств, должен уточнить у пользователя данные его карты. Доверчивые граждане предоставляют мошеннику данные, после чего происходит списание денежных средств с кошелька первых.

Другой способ мошенничества с платежными средствами – скимминг. Он представляет собой высокотехнологичный способ хищения денежных средств,

при котором злоумышленник использует «инструмент для считывания магнитной дорожки платежной карты пользователя» или иные средства (включая накладную клавиатуру или скрытую камеру), которые позволяют получить данные карты пользователя. Так, механизм довольно прост: инструмент для считывания магнитной дорожки платежной карты крепится на картридер терминала, что делает возможным считывание данных карты пользователя. Такое приспособление практически невозможно обнаружить, именно поэтому попасться «на крючок» довольно просто. Существуют и иные способы скимминга, которые по своей сущности более просты для понимания и реализации в целом [1]. Так, используется накладная клавиатура, которая запоминает последовательность введенных логина или пароля. При этом используется и скрытая камера, которая фиксирует нажатые пользователем банкомата символов (логина и пароля). Оба данных способа так же способствуют факту «передачи» мошеннику своих данных платежной карты, что ведет к списанию средств на ней.

Один из самых опасных видов мошенничества – кардинг. Это вид мошенничества, при котором производится операция с использованием платежных реквизитов, взятых с серверов взломанных интернет-магазинов, серверов расчетно-платежных систем, а также личных компьютеров через внедренные в них вирусы. Кардинг является одним из самых опасных видов мошенничества ввиду того, что от жертвы в данном случае мало что зависит [1]. Хакеры могут взломать сервера интернет-магазинов или расчетно-платежных систем и таким образом получить платежные данные множества людей, которые соблюдали все меры компьютерной безопасности. В случае с заражением личных компьютеров вирусами важно отметить тот факт, что не все антивирусы могут распознать все вирусы, в связи с этим и случается заражение компьютера и выводение средств, в связи с этим пользователь может не ожидать взлома его персональных данных, соблюдая все меры предосторожности в информационной сфере.

Стоит упомянуть и о том, что сейчас с учётом информационно - технического прогресса, граждане активно используют различные приложения, средства телекоммуникации, социальные сети и мессенджеры. Самыми распространёнными являются «VK», «Telegram», «WhatsApp». Что касается данных приложений, с их использованием также зарегистрированы случаи обмана граждан [5].

В заключение ко всему вышесказанному стоит отметить, что развитие информационных технологий за последний промежуток времени оказало значительное влияние на развитие мошенничества, связанного с использованием электронных средств платежа. Одними из таких видов преступлений в данной сфере является фрод, фишинг, скимминг и кардинг. Зачастую большинство таких операций происходит с целью получения доступа к личной информации, а также финансовым составляющим объекта посягательства преступления. Именно поэтому, в целях предотвращения такого рода противоправных ситуаций необходимо соблюдать все меры предосторожности в информационной сфере, постоянно обновлять знания в области кибербезопасности.

Литература

1. Колескин Д. В. История развития мошенничества, современные виды мошенничества и способы борьбы с ними //Социально-гуманитарные проблемы современности: сборник научных трудов по материалам Международной научно-практической конференции. - 2020. - Т. 24. - С. 37-42.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.04.2024) //СПС «КонсультантПлюс».
3. Южин А. А. Уголовно-правовая характеристика и проблемы квалификации мошенничества с использованием платежных карт //Социально-экономические явления и процессы. – 2016. – Т. 11. – №. 1. – С. 141-145.
4. Данные официальной статистики МВД России [Электронный ресурс] // URL: <https://мвд.рф/reports/item/47525142/> (дата обращения 03.04.2024).

5. Способы хищения денежных средств с использованием приложений [Электронный ресурс] // URL: <https://кашарский.61.мвд.рф/news/item/42063222/> (дата обращения 07.04.2024).

6. Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 24.07.2023) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 21.10.2023) //СПС «КонсультантПлюс».

Сведения об авторах

Чижов Илья Александрович, кандидат юридических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института Министерства внутренних дел Российской Федерации имени И.Д. Путилина.

Дрога Андрей Анатольевич, заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института Министерства внутренних дел Российской Федерации имени И.Д. Путилина.

Чубырь Наталья Олеговна

АСИМПТОТИЧЕСКИЙ МЕТОД РЕШЕНИЯ КРАЕВОЙ ЗАДАЧИ ДЛЯ СТАЦИОНАРНОЙ СИСТЕМЫ УРАВНЕНИЙ

Для моделирования процессов переноса мембранной электрохимии используют краевые задачи для систем уравнений Нернста – Планка и Пуассона, которые содержат малый параметр при производной в уравнении Пуассона [6]. Для аналитического решения можно применять известные методы [2], но они не всегда устойчивы, поэтому разработка асимптотического решения для таких задач актуальна, более того, в отличие от численного решения оно справедливо в широком диапазоне изменения начальной концентрации [5].

Постановка задачи.

Рассмотрим следующую сингулярно возмущенную краевую задачу, полученную после перехода к безразмерному виду [2, 3, 4] с использованием характерных величин:

$$\frac{dC_1}{dx} = -C_1 \frac{d\varphi}{dx} \quad (1)$$

$$\frac{dC_2}{dx} = C_2 \frac{d\varphi}{dx} \quad (2)$$

$$\frac{dC_3}{dx} = -C_3 \frac{d\varphi}{dx} - \frac{1}{D_3} j_3 \quad (3)$$

$$\frac{dC_4}{dx} = C_4 \frac{d\varphi}{dx} - \frac{1}{D_4} j_4 \quad (4)$$

$$\varepsilon \frac{dj_3}{dx} = a(k_w - C_3 C_4) \quad (5)$$

$$\varepsilon \frac{dj_4}{dx} = a(k_w - C_3 C_4) \quad (6)$$

$$\varepsilon \frac{d^2 \varphi}{dx^2} = -C_1 + C_2 - C_3 + C_4 \quad (7)$$

Краевые условия

$$\left(-C_1 \frac{d\varphi}{dx} - \frac{dC_1}{dx} \right) (0, \varepsilon) = 0 \quad (8)$$

$$C_2(0, \varepsilon) = C_{2a} \quad (9)$$

$$\left(-C_3 \frac{d\varphi}{dx} - \frac{dC_3}{dx} \right) (0, \varepsilon) = 0, \quad (10)$$

$$\frac{dC_4}{dx} (0, \varepsilon) = 0, \quad (11)$$

$$\varphi(0, \varepsilon) = \varphi_0, \quad (12)$$

$$C_1(1, \varepsilon) = C_{1k}, \quad \left(C_2 \frac{d\varphi}{dx} - \frac{dC_2}{dx} \right) (1, \varepsilon) = 0, \quad \frac{dC_3}{dx} (1, \varepsilon) = 0,$$

$$\left(C_4 \frac{d\varphi}{dx} - \frac{dC_4}{dx} \right) (1, \varepsilon) = 0, \quad \varphi(1, \varepsilon) = 0, \text{ где } \varepsilon > 0, \quad k_w > 0 \text{ — параметры.}$$

где $\varphi(x, \varepsilon)$ — потенциал, I_c — ток проводимости Фарадея, $j_i(x, \varepsilon)$ — поток, $C_i(x, \varepsilon)$ — концентрации, D_i — коэффициенты диффузии i -го иона, k_w — константа равновесия. Так как в стационарной задаче $j_1 = j_2 = 0$, то общий ток равен току по ионам H^+ , OH^- : $I_c = j_3 - j_4$.

Алгоритм асимптотического решения.

В безразмерном виде отрезок $[0, 1]$ необходимо разбить на 7 частей, так как на каждом из них будет решение отличаться от остальных. Среди них есть 4 погранслоя, два из которых являются внутренними, получающиеся в результате реакции диссоциации/рекомбинации.

В данной работе асимптотическое решение ищется, следуя плану: сначала ищется внешнее решение, то есть в областях где выполняется условие электронейтральности и равновесия ($\varepsilon = 0$), затем решение вычисляется в погранслоях у мембран и во внутренних погранслоях и на последнем этапе производится сращивание асимптотических разложений (вычисляются константы интегрирования и границы областей).

Приведем результаты решения для потоков.

Таблица 1. Результаты асимптотического решения
для потоков на разных интервалах

	j_1	j_2	j_3	j_4
$[0; \delta_1)$	0	0	$I_c + \frac{ak_w}{\varepsilon}(x - \delta_1)$	$\frac{ak_w}{\varepsilon}(x - \delta_1)$
$(\delta_1; x_1 - \delta_2)$	0	0	I_c	0
$(x_1 - \delta_2; x_1 + \delta_3)$	0	0	$\frac{D_3}{D_3 + D_4} I_c +$ $\frac{D_4}{D_3 + D_4} I_c e^{-\sqrt{\frac{aC_3(x_1)(D_3 + D_4)}{D_3 D_4}} \frac{x - x_1}{\sqrt{\varepsilon}}}$	$-\frac{D_4}{D_3 + D_4} I_c +$ $\frac{D_4}{D_3 + D_4} I_c e^{-\sqrt{\frac{aC_3(x_1)(D_3 + D_4)}{D_3 D_4}} \frac{x - x_1}{\sqrt{\varepsilon}}}$
$(x_1 + \delta_3; x_2 - \delta_4)$	0	0	$\frac{D_3}{D_3 + D_4} I_c$	$-\frac{D_4}{D_3 + D_4} I_c$
$(x_2 - \delta_4; x_2 + \delta_5)$	0	0	$-\frac{D_4}{D_3 + D_4} I_c +$ $\frac{D_4}{D_3 + D_4} I_c e^{-\sqrt{\frac{aC_3(x_1)(D_3 + D_4)}{D_3 D_4}} \frac{x - x_2}{\sqrt{\varepsilon}}}$	$\frac{D_3}{D_3 + D_4} I_c +$ $\frac{D_4}{D_3 + D_4} I_c e^{-\sqrt{\frac{aC_3(x_1)(D_3 + D_4)}{D_3 D_4}} \frac{x - x_2}{\sqrt{\varepsilon}}}$
$(x_2 + \delta_5; 1 - \delta_6)$	0	0	0	$-I_c$
$(1 - \delta_6; 1)$	0	0	$\frac{ak_w}{\varepsilon}(x - 1 + \delta_6)$	$I_c + \frac{ak_w}{\varepsilon}(x - 1 + \delta_6)$

В данной работе проведено асимптотическое решение сингулярно-возмущенной краевой задачи стационарного переноса в сечении канала обессоливания на основании метода сращивания асимптотических разложений. Проведя численное и асимптотическое решение, выявлено возникновение 4 погранслоев, два из которых являются внутренними, возникающие в следствие реакции диссоциации/рекомбинации. Проведя анализ численного и асимптотического решения можно сделать вывод, что решения совпадают. Аналитическое решение в данном случае имеет преимущество перед численным, так как верно для более широкого спектра изменения начальной концентрации и удобство в проведении исследования и анализа процессов переноса [1].

Литература

1. Gudza V.A., Urtenov M.K., Chubyr N.O., Kirillova E.V. Numerical and asymptotic study of non-stationary mass transport of binary salt ions in the diffusion

layer near the cation exchange membrane at prelimiting currents / Applied mathematics and information sciences, 2021, p 411-422.

2. Васильева А.Б., Бутузов В.Ф. Асимптотические методы в теории сингулярных возмущений. – М., 1990.

3. Коваленко, А.В. Асимптотическое решение краевых задач двумерных моделей переноса тернарного электролита / А.В. Коваленко, А.А. Хромых, М.Х. Уртенев // Доклады Академии наук. – 2015. – Т. 464, № 5. – С. 529.

4. Коваленко, А.В. Декомпозиция двумерной системы уравнений Нернста-Планка-Пуассона для тернарного электролита / А.В. Коваленко, А.А. Хромых, М.Х. Уртенев // Доклады Академии наук. – 2014. – Т. 458, № 5. – С. 526.

5. Коваленко, А.В. Моделирование переноса бинарного электролита в канале обессоливания электродиализного аппарата в потенциостатическом режиме / А.В. Коваленко, М.Х. Уртенев, А.А. Хромых // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2012. – № 75. – С. 39-52.

6. Лаврентьев А.В., Уртенев К.М., Хромых А.А., Чубырь Н.О. Численное и асимптотическое решения неоднородной системы уравнений Нернста-Планка-Пуассона/Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки, 2010. № 5 (159). С. 17-22.

Сведения об авторе

Чубырь Наталья Олеговна, кандидат физико-математических наук, доцент, доцент кафедры прикладной математики Кубанского государственного университета.

Шарпан Мария Владимировна,
Сиякаев Данила Дмитриевич

ОСОБЕННОСТИ РЕАЛИЗАЦИИ РОЛЕВОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ НА ПРИМЕРЕ ОС LINUX

Статья посвящена исследованию особенностей реализации модели разграничения доступа в современных операционных системах, на примере Linux. Ролевая модель является одним из наиболее гибких и эффективных подходов к управлению доступом в компьютерных системах, она позволяет детально регулировать права и привилегии пользователей и процессов.

Для того, чтобы более подробно изучить и проанализировать особенности реализации ролевых моделей разграничения доступа в различных дистрибутивах операционных систем, использовались средства виртуализации, а именно программа VMware Workstation Pro.

RBAC

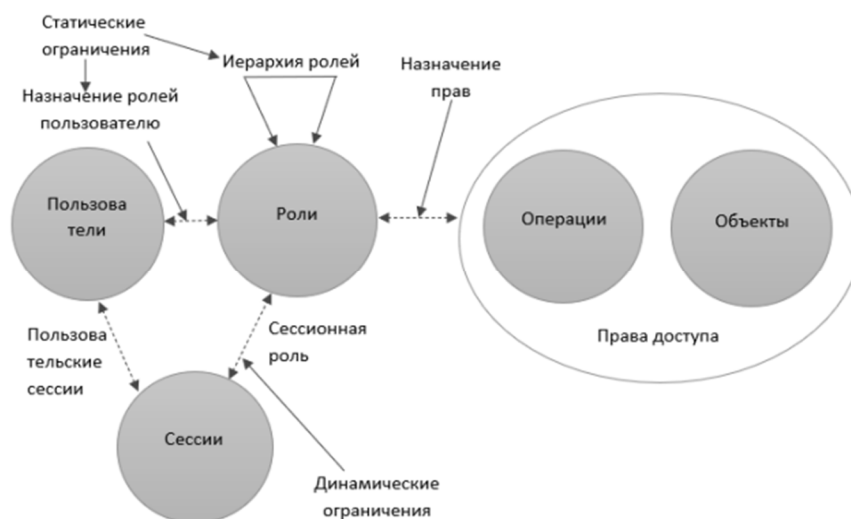


Рис. 1. Схема референтной модели

На рисунке 1 представлена схема референтной модели. В ней можно выделить 4 элемента: ядро, иерархичность, статическое и динамическое разделение обязанностей. Суть, представленной модели заключается в том, что права на доступ выдаются не напрямую пользователям и группам, а назначаются

в ходе пользовательских сессий. Ядро задает совокупность компонентов и связей между ними, необходимые для создания и функционирования единой системы. Иерархичность определяет отношения старшинства между ролями, что позволяет помещать одни роли внутри других и назначать одинаковые права на основе родительских ролей. Разграничения применяются для контроля за соблюдением политики конфликта интересов. Статическое разделение определяет, что для одного пользователя не может быть назначено несколько ролей, которые включают взаимоисключающие функции. А динамическое разделение говорит о том, что для одного пользователя могут быть определены сразу несколько ролей, содержащих взаимоисключающие функции, но в рамках процесса (сессии) он может находиться только в одной из этих ролей. Это базовые принципы на которых строятся все подсистемы разграничения доступом на основе RBAC.

SELinux

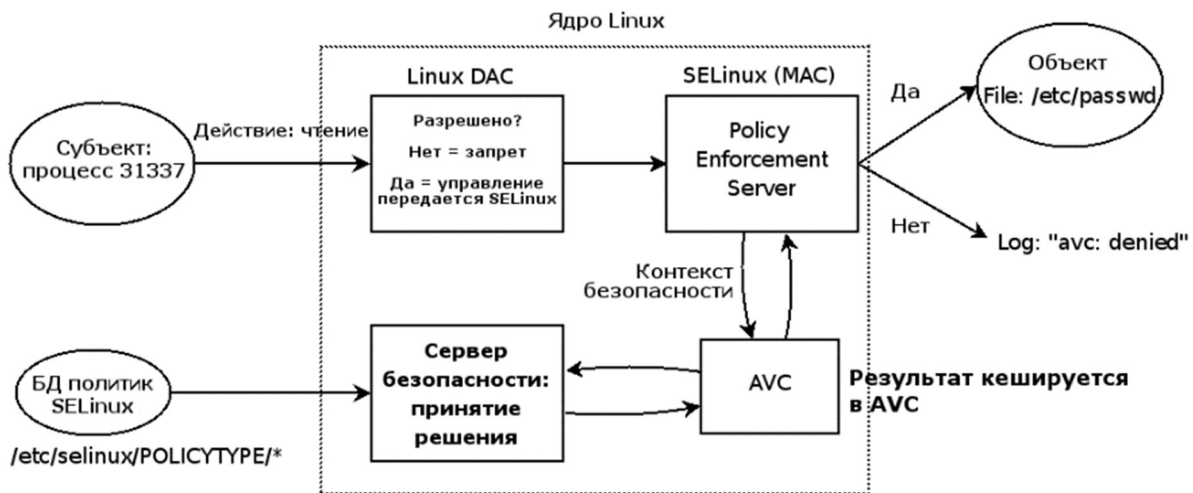


Рис. 2. Структура управления доступом SELinux

Структура управления доступом SELinux, реализуется в ядре ОС Linux через фреймворк LSM, которая представлена на рисунке 2. LSM – это модули, содержащие функции, которые могут перехватить управление и выполнить проверку прав доступа, дополнительно к стандартному механизму дискреционного разграничения доступом. Это улучшенный механизм, который

реализует принудительную модель управления доступом. SELinux имеет 3 режима работы: Enforcing – запрет доступа на основании правил политики, Permissive - ведение лога действий, нарушающих политику, которые противоречат правилам доступа, и Disabled – полное отключение SELinux. Сеанс подлежит проверки модулями LSM после того, как он успешно прошел проверку дискреционной подсистемой разграничения доступа и получил от нее разрешение на доступ к файлу. SELinux работает на основе политик – наборов правил, которыми руководствуется механизм безопасности при предоставлении доступа. Предусмотрено 3 политики: targeted – защищает основные системные сервисы, но не трогает все остальные программы, strict – самая строгая политика, которая управляет не только сетевыми службами, но и программами пользователя, и MLS, содержащая в себе не только правила, но и различные уровни безопасности. Контекст безопасности опирается на такие понятия, как роль – список доменов, которые могут быть применены; домен – список действий, которые может выполнять процесс, тип – набор действий, которые допустимы по отношению к объекту и контекст безопасности, который включает в себя все атрибуты (роли, типы, домены). Сам по себе механизм SELinux не реализует в себе никаких конкретных правил, но включает в себя такие модели разграничения доступа, как RBAC, MLS, а также Type Enforcement. TE – основной механизм контроля доступа, используемый в целевых политиках, позволяющий детально управлять разрешениями. RBAC в SELinux реализуется в качестве ролей и по сути является дальнейшим развитием Type Enforcement. Multi-level Security является многоуровневой моделью безопасности, в которой всем объектам системы присваивается определенный уровень доступа, а разрешение или запрет доступа определяется соотношением этих уровней. Модель SELinux предоставляет администраторам большой уровень гибкости и большое количество вариантов написания политик безопасности для комбинирования RBAC, MAC и TE. С одной стороны, это является несомненным плюсом, но с другой стороны это значительно сказывается на удобстве анализа

и администрирования данных политик. На текущий момент SELinux является наиболее популярным решением и используется в дистрибутивах Red Hat, Fedora, CentOS, Debian, Ubuntu и ряде других.

RSBAC

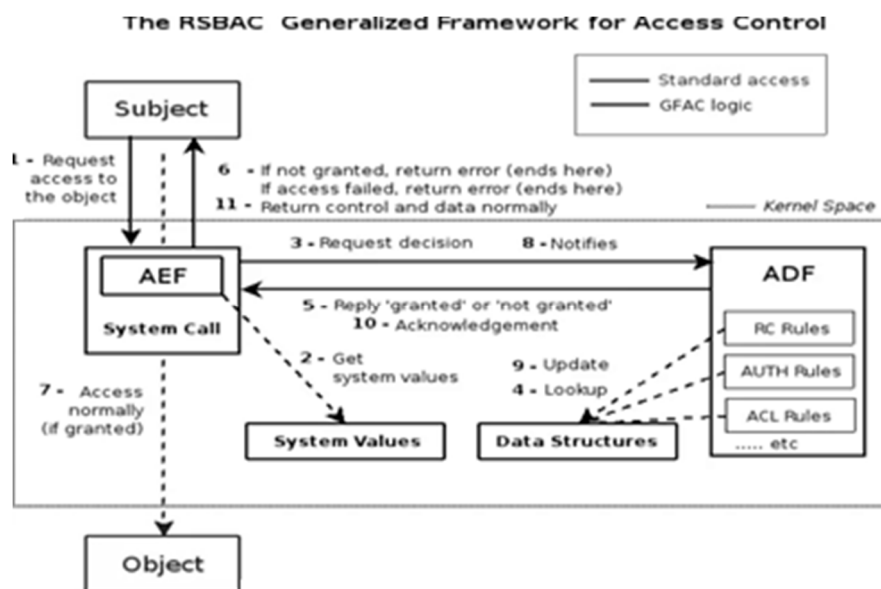


Рис. 3. Модель RSBAC

Модель RSBAC, представляет собой надстройку над ядром и набор утилит для администрирования. Состоит из нескольких модулей безопасности, каждый из которых реализует определенную политику безопасности (рисунок 3). В системе RSBAC реализованы механизмы безопасности, использующие следующие политики управления доступом: RC – политика совместимости ролей; MAC – политика принудительного контроля доступа; ACL – дискреционная политика на основе механизма списков доступа; PM – политика защиты персональных данных; FF – политика назначения флагов доступа к файлам и Auth – политика авторизации пользователей. Основными особенностями RSBAC являются: ассоциирование с каждой сущностью ОС множества атрибутов; использование большого количества различных видов доступа и прав доступа; использование многоуровневой решетки безопасности; при реализации MAC задаются верхние и нижние уровни безопасности; интерпретация роли как набора расширенных прав доступа и сущностей

определенного типа. Модель RSBAC предоставляет администратору очень гибкую систему, состоящую из модулей, которые можно настроить в соответствии с необходимыми требованиями безопасности, но в некоторых ситуациях это может привести к неприятным последствиям в виде блокировки или вовсе потери доступа к данным.

МРОСЛ ДП-модель



Рис. 4. Иерархическое представление МРОСЛ ДП-модели

Мандатная сущностно-ролевая ДП-модель в полной мере реализована в ОС Astra Linux. Основным ее отличием, от классических мандатных моделей разграничения доступа является объединение RBAC и MAC, т.е. это та же MAC-модель, но усиленная за счет ролевой модели и мандатного контроля целостности. На рисунке 4 видно, что ее элементами являются RBAC, MIC и управление информационными потоками. MIC – добавляет в стандартную MAC систему контроль уровня целостности, что позволяет гарантировать, что субъекты с низким уровнем целостности не могут влиять на объекты с высоким уровнем целостности. Еще одной особенностью МРОСЛ ДП-модели является учет иерархичности, что позволяет приводить подобные объекты к единой сущности, внутри которой создаются отношения подчинения. Это справедливо

как для файлов и директорий, так и для пользователей. Также стоит отметить, что данная модель помимо индивидуальных и административных ролей предусматривает запрещающие роли. Запрещающие роли аналогичны другим и настраиваются таким же способом, только они не разрешают, а напротив запрещают совершать те или иные действия, которые предписаны правилом.

PARSEC

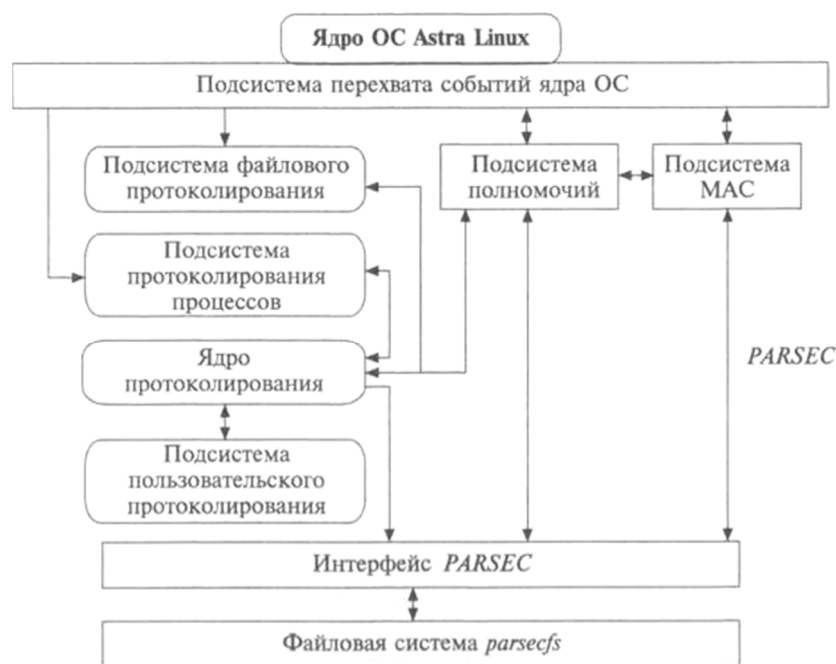


Рис. 5. Архитектура модуля PARSEC

На рисунке 5 изображена архитектура модуля PARSEC. Он представляет собой подсистему безопасности в ОС Astra Linux. Он устанавливает в ядре системы собственные обработчики контролируемых информационных потоков. Они получают управление всякий раз, когда необходимо принять решение о разрешении или запрете обращения субъекта к сущности. PARSEC реализует мандатный контроль целостности и дополнительные функции аудита. Он включает в себя: программный интерфейс и модуль расширения ядра; виртуальную файловую систему `/parsecfs`; набор системных вызовов для управления политикой безопасности.

НІМАСF



Рис. 6. Модель НІМАСF

Заключительной моделью, которая будет рассмотрена, является модель НІМАСF. Она состоит из RBAC, МАС, МІС и информационных потоков. В модели присутствует 4 уровня, которые состоят между собой в иерархической структуре и верхний уровень уточняет и дополняет нижний, что обеспечивает нам высокий уровень безопасности даже при возникновении скрытых каналов передачи информации (рис. 6).

Роли в модели НІМАСF подразделяются на обычные и административные, которые отличаются в типах прав. Обычные роли оперируют стандартным набором прав, а административные в добавок имеют права на приписывание или удаление ролей, а также на модификацию прав ролей. Обычные и административные роли так же не пересекаются. Иерархия сущностей – ациклична, т.е. контейнер не может содержаться в себе самом. Субъекты так же имеют иерархию, которая так же является ацикличной, но может иметь несколько корневых субъектов. Для каждого субъекта имеется роль-владелец, которая может выполнять любые операции над субъектом. Роли имеют свою иерархию, иерархии обычных и административных ролей не пересекаются. У одной роли может быть несколько родителей. Иерархия ролей ациклична и может иметь несколько корней.

На текущий момент модель NIMACF не реализована ни в одном дистрибутиве ОС Linux и является своего рода эталонной моделью, но наиболее близкой по своей реализации МРОСЛ ДП-модель, которая реализована в ОС Astra Linux.

На основе проведенного анализа составлена сравнительная таблица по некоторым важным, с точки зрения обеспечения безопасности, критериям.

Таблица 1. Сравнение различных подсистем ролевого разграничения доступа

Модель	SELinux	RSBAC	МРОСЛ ДП-модель	NIMACF
Тип	MAC + RBAC	Набор модулей	RBAC + MAC + MIC	RBAC + MAC + MIC + ИП
Управление доступом	+	+	+	+
Мандатное разграничение	+	+	+	+
Ролевое разграничение	+	+	+	+
Атрибутивное разграничение	+	+	+	+
Гибкость	Средняя	Высокая	Высокая	Высокая
Контроль доступа на уровне системы	+	+	+	+
Расширяемость	Средняя	Низкая	Высокая	Высокая
Управление информационными потоками	-	-	+	+
Поддержка дополнительных функций безопасности	Аудит, контроль целостности, ограничение привилегий, метка безопасности файлов, категории безопасности	Аудит, контроль целостности, мониторинг событий	Аудит, контроль целостности, ограничение привилегий	Аудит, контроль целостности, управление событиями, контроль доступа на уровне приложений

По представленным данным можно сделать следующий вывод, что мандатная сущностно-ролевая ДП-модель и NIMACF являются более совершенными моделями в области ролевого разграничения доступа, но в ситуациях, когда нам достаточно реализовать надежное мандатное разграничение доступом SELinux тоже будет хорошим вариантом.

Важно отметить, что в реализации ролевого разграничения доступа еще есть пространство для развития и совершенствования этой подсистемы, о чем свидетельствует модель HIMACF.

Литература

1. Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/integratsiya-mandatnogo-i-rolevogo-upravleniya-dostupom-i-mandatnogo-kontrolya-tselostnosti-v-verifitsirovannoy-ierarhicheskoy/viewer> (дата обращения: 03.03.2024).

2. Операционные системы Astra Linux - Справочный центр - Справочный центр Astra Linux [Электронный ресурс]. URL: <https://wiki.astralinux.ru/> (дата обращения: 26.06.2024).

3. SELinux Wiki [Электронный ресурс]. URL: https://selinuxproject.org/page/Main_Page (дата обращения: 14.02.2024).

4. Rule Set Based Access Control для Linux: Журнал СА 1.2004 [Электронный ресурс]. URL: <https://samag.ru/archive/article/228> (дата обращения: 05.02.2024).

5. Денисов Д. Стандарты ролевого подхода к управлению доступом // Digital Enterprise [Электронный ресурс]. URL: <https://cleverics.ru/digital/2015/10/incits-rbac-standards/> (дата обращения: 13.01.2024).

Сведения об авторах

Шарпан Мария Владимировна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России.

Сиякаев Данила Дмитриевич, курсант Краснодарского университета МВД России.

**Яхонтов Илья Сергеевич,
Крепышев Дмитрий Александрович**

CDN: ПРИНЦИПЫ РАБОТЫ И ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

За последние десять лет число пользователей Интернета по всему миру возросло. Величина веб-страниц так же значительно увеличилась: из простых текстовых документов они выросли в полноценные интерактивные ресурсы, насыщенные графикой, видео и аудио-контентом. В связи с этим возникает проблема обеспечения быстрой и надежной доставки контента пользователям из разных уголков мира. В этом контексте технология CDN все больше становится актуальной, ибо она позволяет оптимизировать загрузку веб-страниц и обеспечивать высокую производительность даже при росте объема контента.

CDN (Content Delivery Network) – это географически распределённая сетевая инфраструктура, обеспечивающая быструю доставку контента пользователям веб-сервисов и сайтов. CDN используют как крупные ресурсы с большим трафиком, например, агрегатор AliExpress, так и небольшие бизнесы, ведь проектам любой тематики и масштаба необходимо улучшать пользовательский опыт и применять решения для роста коммерческих метрик. Использование сетей доставки контента помогает веб-сайтам снизить потребление пропускной способности, а также уменьшить время загрузки страниц. За счет этого экономятся временные ресурсы, которые необходимо было бы потратить на обработку запроса каждого пользователя в отдельности на ресурсе без CDN [1].

Принцип работы CDN довольно прост. По определенной территории разбросаны удаленные сервера – так называемые центры обработки данных, в которых хранится кэш и которые соединены с основным хостом. Пользователь получает запрашиваемый контент с ближайшего сервера. Поэтому, в независимости от того, где расположена клиентская площадка, посетитель увидит страницу с минимальной задержкой, потому что получит кэш веб-страницы с ближайшей к нему точки [3].

Как правило, для нахождения ближайшего к пользователю сервера CDN использует две популярные технологии: GeoDNS и AnyCast. Принцип работы GeoDNS основан на том, что при запросе DNS сервер анализирует местоположение пользователя, а затем выбирает IP-адрес сервера, который находится ближе всего к пользователю, и возвращает этот IP-адрес для обработки запроса. Технология AnyCast позволяет использовать один и тот же IP-адрес для нескольких компьютеров в разных местах сети. Когда клиент отправляет запрос к такому IP-адресу, система выбирает сервер, находящийся ближе к клиенту, и направляет запрос на этот сервер [2].

Однако даже грамотно и последовательно выполненная предварительная работа не даст гарантий того, что скорость сайта будет увеличена. Проведем обзор и сравнительный анализ CDN-провайдеров (таблица 1).

Таблица 1. Обзор лучших провайдеров услуг CDN

№	Название	Основные характеристики	Достоинства	Недостатки
1	G-Core Labs	100+ точек; время отклика менее 30 мс; более 6000 партнеров по пирингу(техническое взаимодействие по обмену трафиком между операторами)	лучшая производительность в России и СНГ; единая стоимость трафика по всем регионам; идеален для проектов с ограниченным бюджетом	платный фаервол(защита веб-содержимого); в базовом тарифе Start отсутствует защита от ботов
2	Cloudflare	150+ точек; время отклика менее 14 мс; более 5700 партнеров по пирингу; общая емкость сети более 50 Тбит/сек; есть бесплатный тариф	эффективный фаервол; можно подключать различные приложения; ускоренная отдача контента через Rocket Loader	мало точек в России и СНГ
3	Cdnnow!	22 точки присутствия; более 4000 партнеров по пирингу; общая емкость сети более 500 Гб/сек	есть собственное приложение для SmartTV; доступна технология оптимизация изображений сайта “на лету”; современные стандарты защиты контента	отсутствует расширенный фаервол для борьбы с накруткой; нет бесплатного тарифа
4	NGenix	41 точка; 1000 партнеров по пирингу; среднее время отклика 17 мс; общая емкость сети более 2,75 Тбит/сек	распределенный защищенный DNS; защита от парсинга цен и контента; отдельные API для управления	подходит только для проектов в России;
5	Akamai	300+ точек присутствия; среднее время отклика 39 мс; общая емкость сети более 50+ Тбит/сек	большой спектр настроек фаервола; управление нагрузкой на сайт через интерфейс Global Traffic Manager; самое продвинутое обнаружение ботов	нет смысла подключать к маленьким проектам

Сравнительный анализ сервисы CDN показал, что все они имеют примерно одинаковый набор опций и функционал. Выбор зависит разве что от величины веб-сервиса. Для успешного масштабирования по России, СНГ и всему миру специалисты рекомендуют обратить внимание на G-Core Labs или Akamai. Оба провайдера обеспечивают наилучшее соотношение цены, качества услуг, и производительности [2].

Перейдем от обзора к реальным примерам. В России и странах СНГ множество компаний пользуются услугами CDN от различных провайдеров. Как правило, их сервисы имеют обширную аудиторию. Среди них:

1. Яндекс. Крупнейший российский интернет-поисковик и интернет-провайдер, использует CDN от провайдера Qrator Labs для обеспечения быстрой загрузки и доступности своих сервисов;

2. ВКонтакте. Российская социальная сеть с посещаемостью более 100 млн человек в месяц. Использует CDN-решения от провайдера Cloudflare для ускорения загрузки контента и повышения безопасности сайта. Оригинальный сервер расположен в Санкт-Петербурге;

3. Ozon. Российский маркетплейс, работающий также в Армении, Белоруссии, Казахстане, Кыргызстане и Узбекистане. Использует CDN-решения от различных провайдеров, включая Cloudflare, для обеспечения быстрой загрузки страниц каталога товаров и обработки заказов;

4. Delivery Club. Сервис для заказа еды онлайн. Использует CDN от различных провайдеров, точной информации о конкретном нет;

5. Кинопоиск. Онлайн кинотеатр, совместно с «Плюс Студией», продюсерским центром «Яндекса», производит и распространяет оригинальные фильмы и сериалы. Использует CDN от провайдера Amazon CloudFront;

6. Mail.ru. Компания, имеющая одноименный почтовый сервис, а также предоставляющая множество других услуг. Для улучшения производительности и надежности своих сайтов они используют CDN от провайдера Akamai;

7. HeadHunter(hh.ru). Крупнейшая российская компания для поиска работы в России, Белоруссии, Казахстане. Клиентами являются свыше 515 тыс. компаний. Обширная база содержит более чем 55 млн резюме, а среднее дневное количество вакансий превышает 933 тыс. Использует CDN от Cloudflare.

Приведенные примеры говорят о том, что множество известных компаний активно применяют CDN для улучшения скорости загрузки сайтов, обеспечивая быстрый доступ к контенту для своих пользователей. Это позволяет им удерживать большие аудитории, улучшать клиентоориентированность и успешно вести Интернет-бизнес. Однако это не означает, что CDN нужен только компаниям-гигантам. Более мелкие бизнесы используют CDN, например: Читай-город(интернет-магазин книг и канцелярии), 123.ru (интернет-магазин электроники), MrCable (интернет-магазин профессиональных кабелей для аудио и видео).

В заключение хочется сказать, что технология CDN является неотъемлемой частью современной веб-инфраструктуры и играет ключевую роль в улучшении пользовательского опыта, оптимизации работы веб-сайтов и обеспечении их стабильной работоспособности в условиях возрастающего интернет-трафика. Активное использование CDN становится все более необходимым для владельцев сайтов, стремящихся обеспечить быструю и надежную работу своих онлайн-проектов.

Литература

1. Камардина В.Р. Организация электронного документооборота и его внедрение в государственные структуры в Краснодарском крае / В. Р. Камардина, Д.А. Крепышев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2021. – № 168. – С. 86-95.

2. Что такое CDN и как это работает [электронный ресурс] // habr.ru. URL: <https://habr.com/ru/companies/selectel/articles/463915/> (дата обращения: 25.05.2024)

3. CDN: что это простыми словами, как работает сеть доставки контента [электронный ресурс] // SKILLFACTORY MEDIA. URL: <https://blog.skillfactory.ru/glossary/cdn/?ysclid=lwm5g9nsbt164958745>. (дата обращения: 25.05.2024).

Сведения об авторах

Крепышев Дмитрий Александрович, кандидат экономических наук, доцент Кубанского государственного аграрного университета имени И.Т. Трубилина.

Яхонтов Илья Сергеевич, студент Кубанского государственного аграрного университета имени И.Т. Трубилина.

**Яхонтова Ирина Михайловна,
Ковыляев Роман Александрович**

ВИЗУАЛИЗАЦИЯ ДАННЫХ В VBA: ПРИНЦИПЫ, ПРИМЕНЕНИЕ И ПРЕИМУЩЕСТВА

Визуализация данных является неотъемлемой частью анализа информации, позволяя лучше понимать и интерпретировать сложные наборы данных. В среде Microsoft Office одним из наиболее мощных инструментов для создания визуализаций является Visual Basic for Applications (VBA) [5]. VBA предоставляет возможности для автоматизации создания графиков и диаграмм в Excel, что значительно упрощает обработку и представление данных [1]. В этой статье мы рассмотрим основные принципы работы с визуализациями данных в VBA, продемонстрируем практические примеры создания различных типов графиков и диаграмм, а также обсудим преимущества использования VBA для автоматизации процессов визуализации. Начнем с рассмотрения основных возможностей VBA для создания графиков, после чего перейдем к более сложным сценариям, включая динамическое обновление данных и создание комбинированных диаграмм [3].

Рассмотрим пример создания столбчатой диаграммы с помощью VBA. Предположим, у нас есть данные о продажах за несколько месяцев, расположенные в диапазоне ячеек A1:B6.

Таблица 1. Входные данные для примера

Месяц	Продажи
Январь	1000
Февраль	1500
Март	1300
Апрель	1200
Май	1700
Июнь	1600

Чтобы создать столбчатую диаграмму для этих данных, используем следующий код VBA:

```
Sub CreateBarChart()
    Dim ws As Worksheet
    Dim chartObj As ChartObject
    Dim chartRange As Range
    ' Устанавливаем рабочий лист
    Set ws = ThisWorkbook.Sheets("Sheet1")
    ' Устанавливаем диапазон данных
    Set chartRange = ws.Range("A1:B6")
    ' Создаем объект диаграммы
    Set chartObj = ws.ChartObjects.Add(Left:=100, Width:=375, Top:=50,
Height:=225)
    ' Настраиваем диаграмму
    With chartObj.Chart
        .SetSourceData Source:=chartRange
        .ChartType = xlColumnClustered
        .HasTitle = True
        .ChartTitle.Text = "Продажи по месяцам"
        .Axes(xlCategory, xlPrimary).HasTitle = True
        .Axes(xlCategory, xlPrimary).AxisTitle.Text = "Месяц"
        .Axes(xlValue, xlPrimary).HasTitle = True
        .Axes(xlValue, xlPrimary).AxisTitle.Text = "Продажи"
    End With
End Sub
```

Этот код создаст столбчатую диаграмму на основе данных в диапазоне A1. Диаграмма будет отображать месяцы по оси X и продажи по оси Y, а также будет иметь заголовок «Продажи по месяцам».

Комбинированные диаграммы позволяют одновременно отображать несколько типов данных. Рассмотрим пример создания комбинированной

диаграммы, которая объединяет столбчатую диаграмму продаж и линейный график плановых показателей.

```
Sub CreateComboChart()  
    Dim ws As Worksheet  
    Dim chartObj As ChartObject  
    Dim chartRange As Range  
    ' Устанавливаем рабочий лист  
    Set ws = ThisWorkbook.Sheets("Sheet1")  
    ' Устанавливаем диапазон данных  
    Set chartRange = ws.Range("A1:C6")  
    ' Создаем объект диаграммы  
    Set chartObj = ws.ChartObjects.Add(Left:=100, Width:=375, Top:=50,  
Height:=225)  
    ' Настраиваем диаграмму  
    With chartObj.Chart  
        .SetSourceData Source:=chartRange  
        .ChartType = xlColumnClustered  
        ' Добавляем линию плановых показателей  
        .SeriesCollection.NewSeries  
        .SeriesCollection(2).Name = "Плановые показатели"  
        .SeriesCollection(2).Values = ws.Range("C2:C6")  
        .SeriesCollection(2).ChartType = xlLine  
        .HasTitle = True  
        .ChartTitle.Text = "Продажи и плановые показатели"  
        .Axes(xlCategory, xlPrimary).HasTitle = True  
        .Axes(xlCategory, xlPrimary).AxisTitle.Text = "Месяц"  
        .Axes(xlValue, xlPrimary).HasTitle = True  
        .Axes(xlValue, xlPrimary).AxisTitle.Text = "Значения"  
    End With  
End Sub
```

Этот код создаст комбинированную диаграмму, отображающую данные о продажах в виде столбцов и плановые показатели в виде линии.

Визуализация данных с помощью VBA в Excel предоставляет широкие возможности для автоматизации и настройки графиков и диаграмм [2]. С использованием макросов можно создавать разнообразные визуализации, динамически обновлять данные и улучшать представление информации. Это делает VBA мощным инструментом для аналитиков и специалистов, работающих с данными в Microsoft Office [4].

Возможности VBA включают не только создание и настройку стандартных диаграмм, но и разработку сложных визуализаций, которые могут адаптироваться к изменениям данных в реальном времени. Автоматизация рутинных процессов экономит время и снижает вероятность ошибок, связанных с ручным вводом и обработкой данных. Кроме того, использование VBA для визуализации данных способствует повышению эффективности принятия решений на основе данных. Визуально представленные данные легче интерпретировать, что способствует более глубокому анализу и пониманию ключевых тенденций и аномалий. Это, в свою очередь, может значительно улучшить качество управленческих решений.

Литература

1. Джексон С. Визуализация данных в Excel с помощью VBA // O'Reilly Media. 2017. С. 45-60.
2. Майерс К. Создание настраиваемых диаграмм в Excel: Применение VBA // Packt Publishing. 2020. С. 134-150.
3. Мхитарян Э.Г. Интерфейсы прикладного программирования как основа инструментальных средств / Э.Г. Мхитарян, Е.А. Иванова // Цифровизация экономики: направления, методы, инструменты: Сб. материалов IV Всероссийской научно-практической конференции. – Краснодар: КубГАУ, 2022. – С. 278-280.

4. Соболевский Р.А. Microsoft Office и платформа.NET FRAMEWORK / Р. А. Соболевский, Т. А. Крамаренко // Информационное общество: современное состояние и перспективы развития: сб. материалов IX студенческого Междунар. форума. – Краснодар: КубГАУ, 2017. – С. 339–342.

5. Яхонтова И.М. Разработка приложений на макроязыках: Учебное пособие / И.М. Яхонтова, Т.А. Крамаренко. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2022. – 192 с.

Сведения об авторах

Яхонтова Ирина Михайловна, кандидат экономических наук, доцент Кубанского государственного аграрного университета.

Ковыляев Роман Александрович, студент Кубанского государственного аграрного университета.

Яценко Владимир Михайлович

ВЫБОР МЕТОДА АППРОКСИМАЦИИ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ ДЛЯ ОПИСАНИЯ РОСТА ПОКРЫТИЯ В ПРОЦЕССЕ МИКРОДУГОВОГО ОКСИДИРОВАНИЯ

Для исследования режимов обработки при микродуговом оксидировании (МДО) и построении математических моделей, связывающих режимы обработки с параметрами покрытий, необходимо производить расчет значений данных в точках, расположенных вне экспериментальных точек. Наличие различных методов аппроксимации ставит проблему оценки выбора наилучшего варианта с точки зрения исследователя. В статье рассматривается критерий оценки функциональных зависимостей для случая роста толщины МДО покрытий при ограниченном количестве экспериментальных данных.

Для последующего использования данных в процессе синтеза моделей, связывающих параметры режима обработки с параметрами получаемого покрытия, необходимо построение зависимостей описывающих изменения параметров покрытий от времени обработки. Что требует выполнения аппроксимации экспериментальных данных, причем точность вычисления промежуточных данных тем выше, чем больше экспериментальных точек будет иметь исследователь. Вместе с тем необходимо ограничивать количество экспериментальных данных, в связи с трудоемкостью и длительностью процессов МДО обработки, а также трудоемкости проведения измерений многих интересующих параметров покрытий (фазовый и компонентный состав, пористость, толщина рабочего слоя и т.д.). Априорные знания об известной функциональной зависимости между параметрами режима обработки и параметром покрытия могли бы увеличить статистическую значимость вычисленной неизвестной функции аппроксимации $f(x)$, но в рассматриваемом случае, при процессе МДО, характер зависимостей зачастую остается неизвестным. Тогда из возможных вариантов функции аппроксимации $f_i(x)$, необходимо выбрать наиболее приемлемый вариант, учитывая характерные

особенности процесса МДО и известные знания об описываемой зависимости. В общем случае можно предположить, что характер изменения параметров покрытия носит непрерывный и плавный характер с течением времени.

При получении образцов в процессе МДО, где время процесса измеряется часами, важным является возможность сокращения общего времени получения образцов. В случае, когда установка МДО обеспечивает возможность формирования режима обработки состоящего из нескольких последовательных режимов (последовательности режимов) [7], можно за один цикл обработки получить необходимое количество образцов. Тогда процесс получения образцов можно представить в виде следующего алгоритма:

1. Выбирается необходимое число образцов (по необходимому числу экспериментальных точек, обычно при характерных для МДО процессах, количество точек N лежит в диапазоне от 5 до 12;

2. Задается последовательность режимов обработки: с общим временем T , с количеством этапов равным N , с временем обработки на каждой ступени равном $t = \frac{T}{N}$;

3. Для каждой ступени устанавливаются параметры режима P_i , зависящие от площади поверхности S^0 обрабатываемой детали, как $P_i^n = (N - n - 1) \cdot P_i^0$, где P_i^n – значение i -го параметра режима на n – ой ступени, P_i^0 – значение i -го параметра режима для детали площадью S^0 , n - номер ступени ($n = 1..N$);

4. Запускается одновременная обработка N деталей на первой этапе, после завершения этапа процесс останавливается, одна обработанная деталь извлекается, а процесс продолжается до завершения общего времени T .

Однако какими бы частыми не были получаемые экспериментальные точки все равно требуется описание в виде функциональных зависимостей для определения значений в любой из промежуточных точек. В случае известной априорной информации о функциональной зависимости используют различные степенные, логарифмические, экспоненциальные функции в регрессионных

моделях, а также применяют нейронные сети для описания регрессионных зависимостей [6].

Рассмотрим задачу поиска рациональной модели, аппроксимирующей экспериментальные данные роста толщины рабочего слоя МДО покрытия для различных режимов обработки (образцы с №1...№6 соответствуют различным параметрам режима обработки) алюминиевого сплава АК12ММгН (таблица 1).

Рассмотрим основные возможные варианты интерполирующих функций, которые могут быть использованы для аппроксимации неосциллирующих функций: интерполяция степенной функцией $f(x) = \sum_{i=0}^n a_i x^i$, где n - степень полинома, интерполяция классическим кубическим сплайном класса C^2 , интерполяция кубическим сплайном с сохранением монотонности и формы данных C^1 [4], интерполяция модифицированным алгоритмом Akima[8]. Для математических расчетов использовался пакет математических программ MatLAB R2023a.

Таблица 1. Рост толщины покрытия при различных параметрах режима обработки

№ образца	Параметры режима обработки			Толщина МДО покрытия, мм				
	Концентрация, г/л		Удельная емкость, мкФ/дм ²	Время обработки, минут				
	КОН	Na ₂ SiO ₃		30	60	90	120	150
1	6,4	5	220	0,02	0,02	0,04	0,08	0,16
2	6,4	5	300	0,01	0,01	0,02	0,03	0,06
3	6,4	10	220	0,05	0,10	0,10	0,11	0,22
4	9	5	300	0,03	0,04	0,045	0,05	0,10
5	9	10	220	0,06	0,10	0,12	0,18	0,288
6	9	10	300	0,10	0,12	0,14	0,16	0,20

На рисунке 1 приведен пример аппроксимации экспериментальных данных для одного из образцов (№ 1) с помощью указанных алгоритмов. Также для аппроксимации экспериментальных данных используются некоторые типы нейронных сетей NN (Neural Networks) [1-3, 5], к ним можно отнести GRNN (Generalized Regression Neural Networks), RBF (Radial Basis Function neural networks) и FNN-сети (Feed forward Neural Networks). В случае, когда количество экспериментальных данных мало (не превышает нескольких десятков), обучение

FFN сети сопряжено с проблемами в виде переобучения. Сети RBF и GRNN могут успешно использоваться при решении задач аппроксимации, при этом сеть GRNN по сути вмещает в себя все обучающие данные, тогда как RBF-сеть может содержать как меньшее, так и большее число кластеров (центров базисных функций). По-видимому, если мы хотим использовать все экспериментальные данные и иметь меньшее переобучение сети, то использование сети GRNN является предпочтительным.

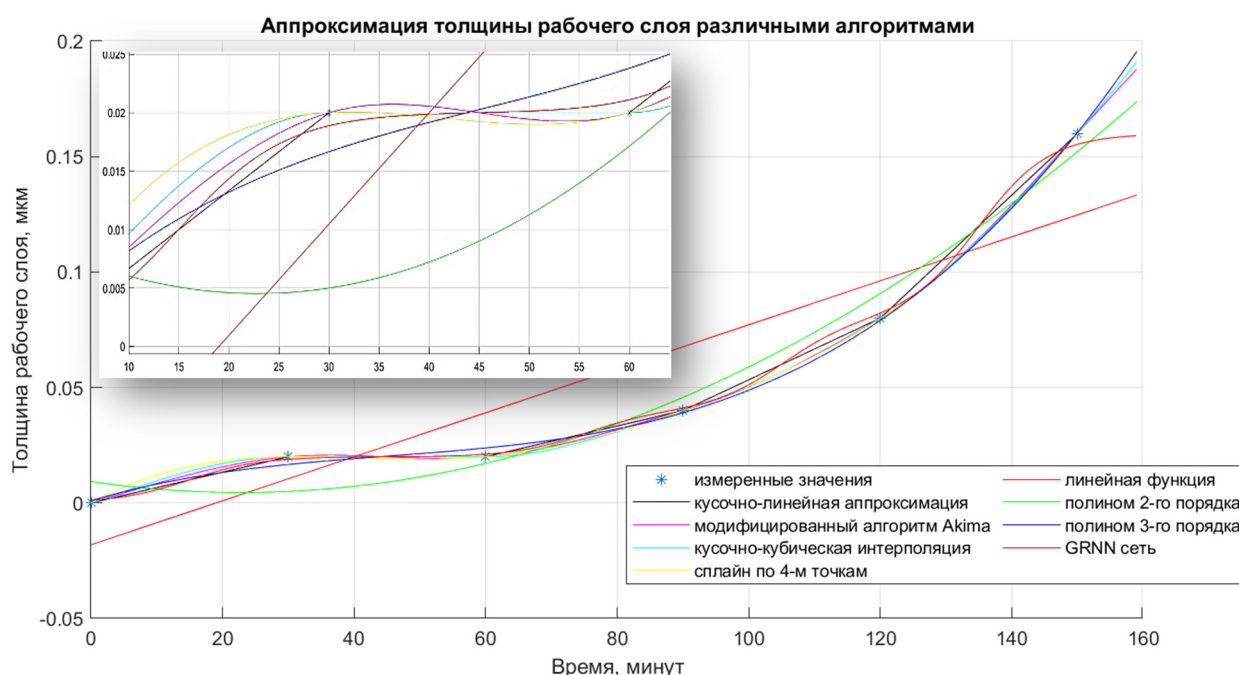


Рис. 1. Результаты аппроксимации толщины рабочего слоя МДО-покрытия от времени обработки для образца № 1 при различных видах аппроксимирующей

Оценка может быть выполнена с помощью различных качественных критериев, среди них можно выделить следующие:

1. Среднюю абсолютную ошибку:

$$MAE = \frac{1}{n} \sum_{i=1}^n |y_i - \hat{y}_i|,$$

2. Общую сумму ошибок (для сравнения вариантов с одинаковым размером выборки):

$$SAD = \sum_{i=1}^n |y_i - \hat{y}_i|;$$

3. Сумму квадратов ошибок:

$$SSE = \sum_{i=1}^n (y_i - \hat{y}_i)^2;$$

4. Коэффициент детерминации:

$$R^2 = 1 - \frac{\sum_{i=1}^n e_i^2}{\sum_{i=1}^n (y_i - \bar{y})^2} = \frac{\sum_{i=1}^n (y_i - \hat{y})^2}{\sum_{i=1}^n (y_i - \bar{y})^2}.$$

В том случае если используются сплайны (вид функции аппроксимации 1-3 в таблице 1) то невозможно использовать указанные оценки MAE, SAD, SSE и R^2 , так как оценки будут равны между собой (так как аппроксимирующие функции проходят через все экспериментальные точки). В таком случае можно предложить использовать оценки, рассчитанные не только по экспериментальным точкам, но также и по промежуточным. В этом случае для расчета критериев отсутствуют данные в промежуточных точках $y \notin Y$, в качестве них возможно использовать например значения, полученные в результате кусочно-линейной аппроксимации по исходным экспериментальным точкам. Рациональным выбором в таком случае будет тот вид функции аппроксимации который в данном случае даст лучшие показатели SAD и SSE критериев (в том числе и в совокупности для всех образцов). Это будет означать, что аппроксимирующая функция на интервале $[y_{i-1}; y_i]$ будет иметь функцию, минимально отклоняющуюся от функции кусочно-линейной аппроксимации, но вместе с тем учитывать характер функции на предыдущем и последующем интервалах. Так как показатели являются интегральными, то и общее поведение функций по аппроксимации данных для всей совокупности интервалов может быть характеризовано указанными критериями.

На рисунке 2 приведены графики критериев оценки алгоритмов аппроксимации для различных режимов обработки (образцы № 1 - № 6) и выбранных алгоритмах аппроксимации данных (вид функции аппроксимации 1 - 7), а в таблице 2 – полученные числовые оценки критериев.

Можно отметить что линейная функция и полином 2-го порядка не подходят для описания рассматриваемой зависимости. В случае использования полинома 3-го порядка, кубического сплайна и кусочно-кубической интерполяции, сохраняющей форму и монотонность кривых - результат получается лучше. Но самые лучшие результаты дают алгоритмы Akima и аппроксимация с помощью GRNN сети.

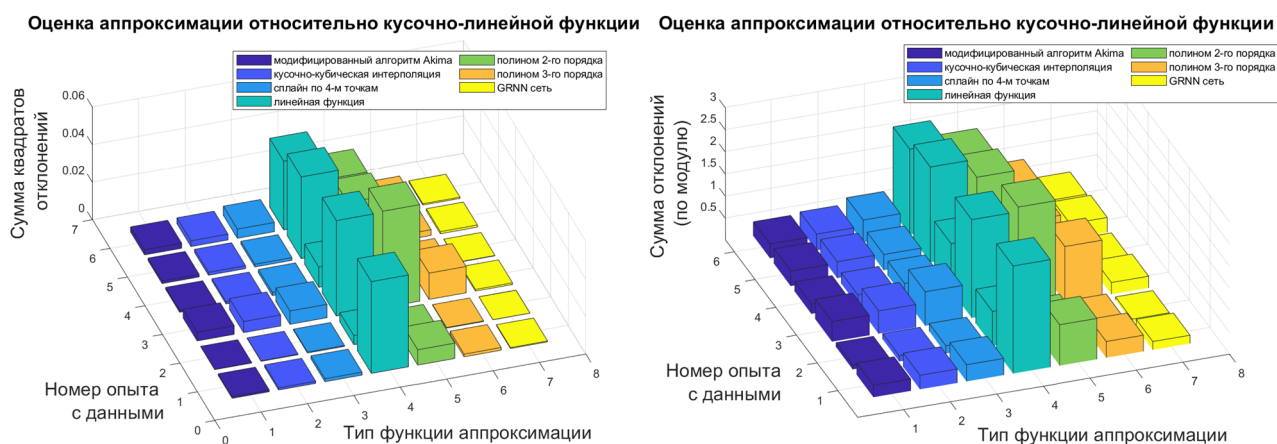


Рис. 2. Оценка качества аппроксимации экспериментальных данных при различных параметрах режима обработки (образцы № 1 - № 6) для различных видов аппроксимирующих функций (1-7)

Таблица 2. Значения критериев оценки качества аппроксимации толщины покрытия при различных видах функции аппроксимации

№ образца	Вид функции аппроксимации						
	1	2	3	4	5	6	7
	Алгоритм takima	Кубический сплайн	Сплайн по 4-м точкам	Линейная	Квадратичная	Кубическая	GRNN-сеть spread=15
Сумма абсолютных отклонений SAD (относительно кусочно-линейной функции)							
1	0,27692	0,32464	0,38486	2,44000	0,93139	0,37412	0,19442
2	0,10977	0,13735	0,18729	0,78386	0,34969	0,17394	0,07342
3	0,46178	0,52442	0,77747	2,23051	2,33619	1,26523	0,27240
4	0,22612	0,25597	0,33837	1,05999	1,06425	0,41455	0,12153
5	0,34919	0,37973	0,36405	2,16333	1,75390	0,57324	0,34418
6	0,33113	0,37458	0,51443	1,94000	1,58473	0,70674	0,24268
Сумма квадратов оценки ошибок SSE (относительно кусочно-линейной функции)							
1	0,00083	0,00114	0,00156	0,04876	0,00815	0,00140	0,00046
2	0,00018	0,00025	0,00049	0,00485	0,00128	0,00028	0,00006
3	0,00456	0,00588	0,00710	0,05072	0,05126	0,01397	0,00087
4	0,00100	0,00120	0,00168	0,01078	0,01016	0,00141	0,00018
5	0,00133	0,00156	0,00144	0,04343	0,02547	0,00304	0,00111
6	0,00267	0,00307	0,00487	0,03652	0,02286	0,00410	0,00067
Коэффициент детерминации R² (относительно экспериментальных точек)							
1	-	-	-	0,6694	0,9695	0,9980	0,9976
2	-	-	-	0,7282	0,9547	0,9917	0,9969
3	-	-	-	0,7384	0,7979	0,9492	0,9944
4	-	-	-	0,7141	0,8049	0,9855	0,9941
5	-	-	-	0,8985	0,9596	0,9983	0,9982
6	-	-	-	0,8788	0,8541	0,9750	0,9957

Согласно полученным результатам можно отметить, что самые высокие значения коэффициента детерминации R^2 в большинстве опытов, а также минимальные значения оценок SAD и SSE (для всех опытов) достигаются при аппроксимации данных с помощью GRNN сети.

В случае, когда необходимо определить рациональную функцию аппроксимации на ограниченной выборке экспериментальных данных возможно использовать критерии SAD и SSE, вычисленные не только по экспериментальным данным, но и по данным функции кусочно-линейной аппроксимации. Допущениями в данном случае является то, что характер изменения параметров носит плавных характер, и вместе с тем неизвестны точные аналитические функции, которые могли бы быть использованы при выборе вида аппроксимирующей функции.

В случае с выбором функции для описания роста рабочего слоя МДО-покрытия от времени процесса наиболее предпочтительно использование GRNN нейронных сетей (дающие минимальное значение суммы квадратов ошибок и минимальное значение суммы абсолютных отклонений из рассмотренных вариантов).

Литература

1. Агеев, В.Н. О применении искусственной нейронной сети для решения задачи аппроксимации нелинейных зависимостей // Научный вестник МГТУ ГА. 2018. № 2.
2. Галкин, В. А., Гавриленко, Т.В., Смородинов, А. Д. Некоторые аспекты аппроксимации и интерполяции функций искусственными нейронными сетями, Вестник КРАУНЦ. Физ.-мат. науки, 2022, том 38, номер 1, 54–73.
3. Овчинников, К.А. Методы прогнозирования параметров телекоммуникационных систем с использованием нейронных сетей // ВЕЖПТ. 2012. № 9 (58).
4. Ромаданова, М.М. Построение кубических сплайнов, сохраняющих выпуклость данных // Известия ТулГУ. Технические науки. 2019. №3.

5. Филатова, Т.В. Применение нейронных сетей для аппроксимации данных // Вестн. Том. гос. ун-та. 2004. № 284.
6. Шолтанюк, С.В. Сравнительный анализ нейросетевой и регрессионных моделей прогнозирования временных рядов. Цифровая трансформация. 2019;(2): 60-68.
7. Яценко, В.М. Функциональные возможности электротехнического оборудования для микродугового оксидирования [Текст] / В.М. Яценко [и др.] // Научное обозрение. – 2015. – № 22. – С. 264-274.
8. Akima, H.A. New Method for Interpolation and Smooth Curve Fitting Based on Local Procedure / H. Akima // Journal of the Association for Computing Machinery. – 1970. – Vol. 17. – P. 589–602.

Сведения об авторе

Яценко Владимир Михайлович, директор ООО «Электронные системы БелГУ».

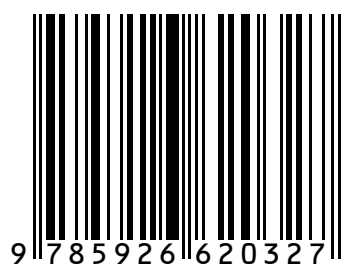
Научное издание

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ
И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА**

Материалы
XX Всероссийской научно-практической конференции
(6 июня 2024 г.)

В авторской редакции

ISBN 978-5-9266-2032-7



Подписано в печать 15.11.2024.
Авт. л. 13,0. Заказ 302.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.