Академия управления МВД России

ИНФОРМАТИЗАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник трудов
Международной научно-практической конференции

Москва
2024

УДК 004.056
ББК 16.18
И74

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *Антышев А. А.,* ведущий научный сотрудник направления по взаимодействию с Военно-промышленной комиссией Российской Федерации Центра организации научно-технической деятельности ФКУ НПО СТиС МВД России, кандидат юридических наук, полковник полиции; *Гончар В. В.,* начальник кафедры информационной безопасности УНК ИТ, полковник полиции.

И74 **Информатизация** и информационная безопасность правоохранительных органов : сборник трудов Международной научно-практической конференции / под общ. ред. А. В. Бецкова [и др.]. – Москва : Академия управления МВД России, 2024. – 332 с.

ISBN 978-5-907721-31-9

В сборник вошли научные статьи участников Международной научно-практической конференции «Информатизация и информационная безопасность правоохранительных органов». Статьи посвящены актуальным проблемам в области информатизации правоохранительной деятельности и перспективным направлениям их преодоления.

Авторами рассмотрены вопросы внедрения новых информационных технологий в деятельность подразделений органов внутренних дел, а также вопросы эксплуатации данных технологий. Отдельные работы посвящены вызовам и угрозам информационной безопасности на новом этапе цифровизации всех сфер общественной жизни. В статьях рассмотрены организационные и правовые вопросы регулирования информационных процессов. Приведены перспективные направления совершенствования информационно-аналитической работы, проводимой в интересах обеспечения общественной безопасности, раскрытия и расследования преступлений. Также рассмотрены положительные примеры иннформатизации подразделений полиции из зарубежного опыта.

УДК 004.056
ББК 16.18

ISBN 978-5-907721-31-9

Содержание

Введение

Кафедра специальной техники Высшей школы СССР была создана в 1969 г. во исполнение приказа Министра внутренних дел СССР. Базой для формирования новой кафедры стала предметно-методическая секция специальной техники кафедры оперативно-разыскной деятельности.

В 1974 г. при формировании Академии МВД СССР она получила название кафедры специальной техники и связи. Исходя из востребованности направлений информационно-технической поддержки, неоднократно менялось название кафедры. Так, с 1975 г. – кафедра средств управления и специальной техники; 1978 г. – кафедра технических средств управления; 1980 г. – кафедра технических средств управления и автоматизированных информационных систем; 1983 г. – кафедра технических средств управления; 1990 г. – кафедра автоматизации управления в органах внутренних дел; 2016 г. – кафедра информационных технологий.

Кафедра – это прежде всего люди, которые трудились в различные периоды ее деятельности, отдавая себя, свою творческую энергию, время своей жизни служению Отечеству.

Среди достойных офицеров первый руководитель кафедры специальной техники – кандидат юридических наук, доцент Е. Ф. Толмачев. В августе 1969 г., перейдя с кафедры оперативно-разыскной деятельности, с шестью коллегами единомышленниками создал новую кафедру. В 1974 г. его сменил Б. И. Худоминский, который в 1975 г. передал эстафету руководства Н. К. Куликову, а после руководство осуществлял Э. Г. Морозов с 1978 по 1980 гг.

Особенный период необходимо отметить под руководством А. П. Полежаева, когда кафедра автоматизации управления в органах внутренних дел трансформировалась в учебно-научный комплекс (УНК), который состоял из кафедры автоматизации управления органами внутренних дел и научно-исследовательского отдела разработки новых информационных технологий. Это решение было связано с необходимостью широкого внедрения компьютерных технологий в практическую деятельность и учебный процесс.

В дальнейшем развитие кафедры осуществлялось под руководством В. А. Минаева (с 1993 по 1997 гг.), В. И. Кириным (с 1997 по 2010 гг.), И. В. Горошко (с 2010 по 2019 гг.).

В конце XX в. и начале XXI в. в период информатизации, цифровизации и цифровой трансформации общества и государства наступила эпоха интеграции цифровых информационных технологий в правоохранительную деятельность. В те годы в кол-

лективе работали: начальник учебно-научного комплекса и кафедры В. А. Минаев; заместители начальника кафедры В. Р. Женило и В. И. Кирин; профессор В. Ф. Макаров; доценты Л. И. Курнакова, В. Д. Курушин, В. И. Кононенко, М. Г. Степанов и Л. Н. Пухлов; старшие преподаватели М. П. Дубинин, Н. А. Сергеев, В. В. Сергеев и Г. Г. Соломанидин; преподаватели И. В. Горошко, А. А. Рыжков, А. К. Баранов, В. В. Баранов, Н. В. Лукашов, А. С. Олейник и др.

В то время, как ожидалось, внедрение цифровых информационных технологий должно было дать наибольший эффект по таким направлениям, как автоматизация криминалистических, розыскных и оперативно-справочных учетов, использование компьютерных технологий для проведения фоноскопических экспертиз. Микропроцессоры и цифровые информационные технологии начинали широко внедряться в различные виды специальной техники, в том числе в поисковую и досмотровую технику (мобильные рентгеновские комплексы, средства видеонаблюдения), технику связи и др. Эти новейшие технические решения были крайне необходимы практическим органам внутренних дел.

Коллективу учебно-научного комплекса удалось достичь определенных успехов в ряде направлений: в разработке программных средств автоматизации оперативных учетов, компьютеризации фоноскопических экспертиз, организации учебного процесса по новому направлению – информационной безопасности.

Для автоматизации накопленных учетов было необходимо разработать специальное программное обеспечение. И оно было создано сотрудниками отдела, входившего в 90-е годы вместе с коллективом кафедры в состав учебно-научного комплекса. Это прежде всего начальник отдела А. К. Баранов и высокопрофессиональные программисты Г. В. Комаров, Б. Б. Кушаков, И. И. Золотов, Е. Б. Ключникова и др. Они создали новейшее для тех лет инструментальное средство «Флинт», которое по своим возможностям можно отнести к системам управления базами данных (СУБД). Эта разработка была очень своевременной и востребованной. Она нашла применение во многих органах внутренних дел, использовалась более полутора десятка лет в практических подразделениях и учебном процессе Академии.

В компьютеризацию фоноскопических экспертиз огромный вклад вложил доктор технических наук, профессор В. Р. Женило. Им были разработаны специальные математические методы и основанные на них принципиально новые цифровые технологии для проведения фоноскопических экспертиз. Его разработки позволили экспертам-криминалистам извлекать из речевого сигнала такую информацию, которая необходима была для решения конкретных криминалистических задач. Научно-исследовательская работа,

проводимая профессором В. Р. Женило, завершалась, как правило, внедрением полученных результатов в практическую деятельность прежде всего экспертно-криминалистических подразделений и подразделений СТМ. Его научные разработки нашли применение в Институте психологии РАН для извлечения информации из следов звука при анализе эмоционального состояния говорящего. Эти цифровые технологии использовались также для исследования певческих голосов в Московской государственной консерватории имени П. И. Чайковского. На протяжении многих лет профессор В. Р. Женило плодотворно участвует в обучении и переподготовке экпертов-фоноскопистов, регулярно проводимых Экспертно-криминалистическим центром МВД России, а в последние годы также и Федеральной службой по контролю за оборотом наркотиков России.

В. А. Минаев – доктор технических наук, профессор, известный специалист по математическому моделированию, прогнозированию, управлению, математическим методам анализа, информационным технологиям и информационной безопасности, автор более 750 научных и учебно-методических работ, в том числе – более 70 монографий и учебников, включая около 50 по проблемам управления, информационных технологий и информационной безопасности. В настоящее время, работая профессором Московского университета МВД России имени В. Я. Кикотя, поддерживает деловые взаимоотношения и оказывает поддержку кафедре.

Информатизация органов внутренних дел неразрывно связана с обеспечением информационной безопасности. В. Ф. Макаров, доктор технических наук, профессор, имея теоретические разработки в области защиты информации, подкрепленные многочисленными патентами и авторскими свидетельствами, опередил свое время и теоретическую основу научной школы.

На кафедре информационных технологий в разные периоды времени работал коллектив высоко профессиональных ученых и педагогов. Так, В. Ф. Макаров возглавляет приоритетное научное направление по информационной безопасности и защите информации в каналах связи. Под его руководством подготовлено и успешно защищено около 20 кандидатских и докторских диссертаций. Он является автором многочисленных патентов и авторских свидетельств на изобретения.

Научные интересы доктора технических наук, кандидата экономических наук, профессора И. В. Горошко реализуются в области экономико-математического моделирования социально-правовой сферы. Кроме того, являясь на протяжении многих лет руководителем кафедры, он вносил большой вклад в организацию научно-исследовательской деятельности нашего коллектива. На дан-

ном этапе И. В. Горошко руководит деятельностью ученого совета по подготовке и защите диссертаций на соискание научных степеней доктора технических наук и кандидата технических наук по специальности 2.3.4. – Управление в организационных системах. Одновременно исполняет обязанности профессора кафедры информационных технологий Академии управления МВД России.

А. И. Куприянов – доктор технических наук, профессор, известный в стране ученый в области радиоэлектронной борьбы и защиты информации, автор многочисленных учебников и монографий. Им получен ряд авторских свидетельств на изобретения.

Ведущие методисты кафедры М. П. Дубинин, М. Г. Степанов, Н. А. Сергеев, О. Н. Шевырева, В. А. Апульцин, В. Ю. Петрова, Л. И. Курнакова, Н. А. Костомарова, А. А. Рыжков, А. А. Куликов и ушедшие из жизни В. И. Кононенко и Ю. А. Кравченко осуществляли научную деятельность, учебно-методический процесс на высоком профессиональном уровне, чем формировали у обучающихся уважение и благодарность, а также заслуживали поощрение руководства Академии управления МВД России.

Нельзя не выразить благодарность сотрудникам, имеющим значительный срок службы, но продолжающим работать в настоящее время на кафедре информационных технологий. Доцент кафедры, кандидат юридических наук, полковник полиции В. В. Баранов проходит службу с 1996 г. Активное участие в научной и педагогической деятельности позволяет наращивать авторитет коллектива в инновационном направлении использования возможностей информационных технологий по противодействию преступности, в том числе и киберпространстве. Является авторитетом для отечественных и зарубежных обучающихся по основным образовательным программам и программам дополнительного профессионального образования. В. В. Баранов осуществляет взаимодействие личного состава кафедры информационных технологий с ветеранами кафедры, научными организациями и территориальными органами, вовлекает в совместную творческую деятельность.

Профессор кафедры, доктор технических наук, доцент И. В. Кубасов на высоком методическом уровне проводит все виды учебных занятий, результативно руководит кафедральным научным сообществом, руководит подготовкой диссертационных исследований, развивает сферу научных знаний совершенствования деятельности органов внутренних дел на основе современных информационных аналитических систем и систем связи.

Профессор кафедры, кандидат технических наук, доцент Б. А. Торопов (работает с 2006 г.) в настоящее время работает над

докторским диссертационным исследованием по научной специальности 2.3.4. – Управление в организационных системах. Имея значительный опыт исследователя и педагога, оказывает содействие кафедре в подготовке выпускников магистрантов и адъюнктов.

Одним из ветеранов является старший преподаватель-методист В. В. Яковлев, труд которого не сразу заметен, однако ежедневная рутинная работа очень важна с точки зрения организации учебного процесса и научной деятельности, прохождения службы сотрудниками и создания условий труда работникам кафедры информационных технологий. В. В. Яковлев организует работу личного состава по всем направлениям деятельности кафедры, периодически выполняя обязанности руководителя подразделения, а также, обеспечивает учет и движение материально-технических средств для сопровождения учебного процесса и научной деятельности.

За последние три года на кафедре информационных технологий прошла значительная кадровая ротация. На современном этапе жизнедеятельности нашего подразделений в коллектив вошли: доцент кафедры, кандидат технических наук Л. А. Лекарь, старший преподаватель Д. В. Голиков, старший преподаватель Ю. В. Броненкова и старший преподаватель кандидат юридических наук Д. А. Рыжиков.

Коллектив справляется с решением поставленных задач. Обеспечивает учебный процесс Академии управления МВД России по основным образовательным программам и программам дополнительного профессионального образования, проводит научно-исследовательскую деятельность, в том числе на соискание ученых степеней доктора технических наук и кандидата технических наук по научной специальности 2.3.4. – Управление в организационных системах.

Международная научно-практическая конференция «Информация, информационная безопасность правоохранительных органов», проводимая в текущем году, является знаковой ввиду исполнения 55-летия кафедры. Активность в научно-представительском направлении свидетельствует о наличии потенциала и готовности коллектива кафедры информационных технологий при поддержке руководства Академии управления МВД России к дальнейшей деятельности на благо повышения эффективности МВД России на основе применения современных информационных технологий.

Начальник кафедры
информационных технологий
доктор технических наук, доцент
полковник полиции А. В. Бецков

Александр Викторович Бецков,
доктор технических наук, доцент
начальник кафедры информационных технологий
Академия управления МВД России
E-mail: aumvd10@mail.ru

Анатолий Федорович Майдыков,
доктор юридических наук, профессор,
профессор кафедры управления органами
внутренних дел в особых условиях
Академия управления МВД России

Николай Алексеевич Северцев
главный научный сотрудник ФИЦ УИ РАН

УДК 656.7.01

Интеграция систем для достижения превосходства при решении задач противоборства

Аннотация

Комплексное системное применение различных технических средств на базе летательного и воздухоплавательного аппарата позволит сформировать положительные характеристики за счет сложения положительного эффекта, которые востребованы при решения жизненно важных задач, в том числе по достижению превосходства над противоборствующей стороной.

Ключевые слова и словосочетания*: системность; комплексность; управляемость; аэромобильность; оперативность; совместимость системы; превосходство над противоборствующей стороной.*

Современная жизнедеятельность человечества насыщена критическими ситуациями, в которых для обеспечения собственной безопасности, а порой и выживания необходимо вступать в борьбу с некоторой силой или аналогичной организационной структурой, идентичной (схожей) природой происхождения. Противостоящая сторона может быть представлена стихией, обладающей значительным превосходством в энергии, интеллекте и имеющей особенности природы происхождения. В настоящее время это свойственно организационным социальным структурам, природным стихиям и организационно-

техническим системам, как существующим в рамках регулируемых управляемых структур, так и подчиняющимся силам природы, стихиям в различных ее материальных и неведанных науке обликах.

Для обеспечения возможности получать наиболее качественную информацию, отвечающую требованиям объективности, достоверности, актуальности, целостности, оперативности, человеку необходимо сконцентрировать свои естественные усилия и организационно-технические возможности, позволяющие привлечь дополнительные разрешающие возможности, которыми обладают современные технологии, и подчинить их естественными силами человека. Вероятно, что за счет концентрации разнородных положительных характеристик появятся дополнительные возможности достижения превосходства над противоборствующей стороной любой природы происхождения.

Примеров этому предостаточно. Человек успешно преодолевает большие расстояния по воде, пересекает воздушное и космическое пространство, углубляется под землю и т. д. Также в конфликтных ситуациях человек пользуется дополнительными возможностями технических систем разного рода для подчинения оппонента. Достижение превосходства за счет новых технических решений давно стало обыденным делом с точки зрения метода. Однако каков будет метод, новый подход, который позволит удивить и сломить противную сторону? От решения этого вопроса зависит и результат! Внедрение инновационного технического решения позволяет осуществить незнакомый тактический прием за счет новой уникальной разрешающей возможности, в результате приводящей к успеху и открывающей путь к победе.

XXI век наиболее ярко открывает новые уникальные возможности комплексирования разнородных технических средств и системы, которые становятся обладателями совокупных положительных тактико-технических характеристик и летно-тактических данных. Они обладают возможностью аэромобильности, т. е. свободного перемещения в воздушном пространстве: при необходимости возможно находиться долгое время на высоте, достигая при этом превосходства высоты (с тактической точки зрения) и обладая преимуществом энергетики (с физической стороны процесса) [1]. С другой стороны, наличие иных средств (средств связи, дозиметрии, вооружения) дает безусловное ударно тактическое превосходство при решении военных задач. Дистанционное управление сложной технической системой, размещенной на летательном, воздухоплавательном аппарате или водном плавательном средстве без человека-оператора, позволит минимизировать воздействия человеческого

фактора и оптимизирует транспортное средство за счет исключения системы жизнеобеспечения в техническом контуре. Улучшение массогабаритных, энергетических и скоростных параметров позволяет получить новую положительную характеристику, а то и несколько положительных характеристик.

Системность, управляемость, аэромобильность, разнородность полезных параметров позволяют использовать комплексные организационно-технические системы для решения разного рода задач, в том числе по достижению превосходства над противоборствующей стороной [2].

В систему современных аэромобильных комплексов, которые способны решать различные задачи гуманитарного, правоохранительного, военного свойства, можно отнести не только пилотируемые, но и беспилотные, и, конечно же, смешанные организационные системы. Совершенствование характеристик каждого элемента аэромобильного комплекса, а также сами комплексные инновационные решения позволят расширять круг решаемых задач, возникающих во всех сферах жизнедеятельности человека [3; 4].

Для оценки уровня совместимости комплексной системы предложим следующий подход.

Систему AX=B можно сделать совместной за счет возмущения правой части:

$$AX=B+\delta B\_1,\ \delta>0, B\_1 \in R\hat{}m, \qquad (1)$$

где δ – малый параметр.

Кроме того, можно рассматривать нормальную систему для AX=B.

$$A\hat{}* AX=A\hat{}* B. \qquad (2)$$

Здесь символ * означает транспонирование. Известно, что система (2) всегда совместна.

С точки зрения вычислений форма (1) является более предпочтительной в плане обусловленности системы. В случае (2) умножение на транспонированную матрицу ухудшает обусловленность системы, которая определяется как отношение модуля максимального собственного значения к модулю минимального. Перемножая матрицы, число обусловленности возводится в квадрат, т. е.

$$K(A\hat{}* A)=K\hat{}2\ (A),$$

где K – число обусловленности матрицы.

Линейная связь целевой функции с выделенными факторами.

Рассмотрим расширенную матрицу наблюдений A_1=(C/A).

В результате применения метода главных компонент к матрице A_1 получаем следующее факторное решение:

$$C=\gamma_{01} P_1+\gamma_{02} P_2+\cdots+\gamma_{0k} P_k,$$
$$a_1=\gamma_{11} P_1+\gamma_{12} P_2+\cdots+\gamma_{1k} P_k,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_m=\gamma_{m1} P_1+\gamma_{m2} P_2+\cdots+\gamma_{mk} P_k, \qquad (3)$$

Параметры P_i,i=1,..., k являются линейными комбинациями выбранной системы векторов C,a_j;j=1,..., m:

$$P_i=\sum_{j=1}^{m}\beta_{ij} a_i+\beta_{i0} C,\ i=1,\ldots, k. \qquad (4)$$

Коэффициенты в формулах (3) и (4) определяются в результате расчетных процедур метода главных компонент.

Из формул (3), (4) следует линейность соотношения между вектором C и выделенными основными факторами.

Полученная транспонированная матрица подбора характеристик также позволяет получить оценку целевой функции, но объем расчетной работы требует обоснования применения новых возможностей в условиях динамично меняющейся многофакторной обстановки с учетом значений нечетких множеств.

Список литературы:

1. *Бецков А. В.* Теоретические и организационные основы формирования аэромобильных комплексов МВД России // Академия управления МВД России, 2009. 198 с.

2. *Бецков А. В.* Формирование и функционирование аэромобильных комплексов МВД России // Академия управления МВД России, 2010. 238 с.

3. *Бецков А. В.* Характеристики технических средств, используемых в моделировании аэромобильных комплексов МВД России. Москва: ТЭИС, 2010. 576 с.

4. *Бецков А. В., Бецков В. И.* Технические средства аэромобильных комплексов специального назначения. Москва: ТЭИС, 2012. 344 с.

Арина Александровна Адамова,
кандидат технических наук, доцент,
заместитель заведующего кафедрой
«Проектирование и технология производства ЭА»
Московский государственный
технический университет
имени Н. Э. Баумана

Денис Александрович Рыжиков,
кандидат юридических наук,
старший преподаватель
кафедры информационных технологий
Академия управления МВД России

УДК 004.94

Анализ безопасности технологий цифровых двойников

Аннотация

Современный уровень цифровизации всех сфер жизни общества систем требует особого подхода к внедрению вновь формируемых технологий. Учитывать это необходимо и при внедрении средств цифровизации в процессы обучения специалистов по различным направлениям деятельности общества. Авторским коллективом представлен анализ применения технологии «цифрового двойника» в учебном процессе при подготовке специалистов для промышленности. Рассмотрены отдельные аспекты формирования методики обучения с применением «цифровых двойников», а также определена необходимость формирования нормативного регулирования применения рассматриваемой технологии.

Ключевые слова и словосочетания*: технологии «цифровых двойников»; киберпространство; информационная безопасность; нормативно-техническое регулирование; киберфизические системы; цифровая трансформация.*

В последнее время в промышленности находят все большее применение так называемые цифровые модели производства, содержащие совокупность информации о производимом изделии и технологии его производства. Тем самым такие системы представляют собой некий цифровой дубликат или цифровую модель реального

производства, составляющую основу концепции развития производства «Индустрия 5.0» («Industry 5.0») [9; 20], которая направлена на облегчение цифровой трансформации предприятий в рамках индустриальной революции в современных условиях. В качестве конечных результатов Индустрия 5.0 предусматривает необходимость достижения повышения конкурентоспособности предприятий промышленности посредством интенсивного внедрения в их деятельность «киберфизических систем» в заводские процессы.

А основными факторами системы, подлежащими анализу в рамках реализации указанной Индустрии 5.0, являются обеспечение возможности непрерывного подключения, уровень поддержки человеком и реализация распределенного принятия решений [4–6; 18–19]. Компонентная же база этой концепции представляет собой систему виртуальной и дополненной реальности, работающую в симбиозе с киберфизическими системами, современными методами облачных вычислений, анализа Big Data и т. д. [1; 12] и впоследствии трансформирующуюся в «Умные фабрики» [2; 8; 10; 17; 19; 22].

Цифровая трансформация в современных реалиях представляет собой уникальный инструмент, позволяющий по-новому рассмотреть вопросы организации жизнедеятельности социума (от бизнес-моделей и производственных процессов до источников финансирования и формирования интеллектуального кадрового резерва). Это тот двигатель прогресса, который посредством внедрения информационных технологий реализует и развивает нецифровые аспекты жизни общества. Но вместе с тем из-за внедряемых процессов автоматизации и цифровизации производства одним из негативных социальных явлений научно-технического прогресса является сокращение персонала предприятий, что накладывает новые требования к профессиональным компетенциям и подготовке специалистов.

Для формирования конкурентных преимуществ в современных реалиях [3; 21] предприятиям и организациям необходимо рассматривать производственные процессы в комплексе коррелирующих между собой посредством обмена потоками цифровой информации и материально-логистическими цепочками отдельных компонентов сквозного жизненного цикла выпускаемой ими продукции.

Достижению этих целей способствует цифровизация процессов производства конкретного изделия (продукции) [9], реализуемая посредством разработки имитационных моделей каждого из этапов жизненного цикла изделия с учетом максимально имеющихся данных: от физических параметров изделия до набора параметров, определяющих отдельные производственные процессы, включаю-

щие, входные/выходные управляющие данные, критерии, ограничения и переменные оптимизации.

Применение таких моделей позволяет без проведения энергозатратных дорогостоящих процедур проводить неоднократное имитационное моделирование с целью прогнозирования характеристик производимой предприятием продукции, отбора перспективных ее образцов, а также оптимизации параметров анализируемого изделия, его производственных процессов и остальных этапов жизненного цикла.

Тут следует отметить, и это не может не радовать, что с повышением уровня цифровизации социума расширяется и область применения рассматриваемой нами технологии «цифровых двойников», особенно в образовательной сфере, обеспечивая на более высоком уровне реализацию программ повышения квалификации и переобучения специалистов.

Одним из социальных компонентов цифровой трансформации общества является концепция «Образование 5.0», стимулирующая обучение на практике и работу обучаемых в команде с применением распределенных источников, облачных хранилищ и т. д. и предполагающая не только интеграцию в учебный процесс кибертехнологий, но и формирование единой социально-образовательной киберсреды, которая направлена на решение образовательных и повседневных задач социума [7; 14; 16].

Реализация современных образовательных технологий в рамках концепции «Образование 5.0» предполагает применение инструментов системного проектирования, которые позволяют раздробить систему объектов и процессов изучаемой предметной области на совокупность однозначно интерпретируемых моделей.

В настоящее время уже недостаточно разработать только цифровую модель изучаемого объекта, так как такой подход позволяет решить лишь задачи инженерного анализа, проектирования (конструкторского, автоматизированного), расчетов и анализа, а также частично – задачи программного обеспечения для автоматизации технологической подготовки производства.

Для получения полноценных достоверных и актуальных результатов, помимо цифровой модели объекта, необходимо разработать цифровые модели производства с учетом всех сведений о его технико-экономических характеристик: о применяемых материалах; задействованном оборудовании; его комплектующих; времени переналадки, ремонтных работ и вынужденных простоев оборудования; технологических процессах; маршрутах перемещения объектов, задействованных в технологическом процессе; персонале

и показателях производительности, точности, надежности и безотказности и т. д.

Только максимально возможная совокупность данных, используемых для формирования цифровых моделей, позволяет создать изменяющуюся, динамичную имитационную модель реального производства, которая в перспективе будет отражать не только изучаемый объект, но и аспекты управления его производства (экономический, социальный, предметный, операционный, производственный и т. д.) со всеми их противоречиями, связями и результатами взаимодействия всех элементов цифровой системы. При таком формате организации информационных моделей, когда все оцифрованные компоненты цикла производства объединены в единую модель, возможно обеспечить информационную прозрачность и воспроизводимость системы в целом и получить более достоверную прогнозную информацию при ее управляемом изменении.

Применение же в обучающем процессе многогранной имитационной модели, реализующей, в том числе решение научной или учебной проблемы, позволяет расширить восприятие получаемого обучаемыми материала и формирует у них пространственное мировоззрение с более глубоким визуальным погружением в предметную область знаний.

С учетом принципа проблемности содержания модели и процесса ее развертывания в игровой деятельности обучаемого коллектива в настоящее время основу обучения специалистов, осуществляемого с использованием технологий «Цифровых двойников», составляет имитационное моделирование:

– конкретных условий и динамики производства;

– реальных условий профессиональной деятельности специалиста (во всем многообразии служебных, социальных и личностных связей);

– содержания и форм профессиональной деятельности;

– совместной деятельности, реализуемое за счет вовлечения в познавательную деятельность нескольких участников, определения их ролей, полномочий, интересов и средств обеспечения их деятельности;

– диалогового общения, в котором заложено необходимое условие достижения учебных целей (в виде диалога или дискуссии с максимальным участием всех играющих).

Такая организация работы обучающегося коллектива обеспечивает многогранность (широту) получаемых игровых моделей профессионального взаимодействия «должностных» лиц и специалистов, а также позволяет сформировать полноценные творческие коллективы для всестороннего обсуждения возникающих произ-

водственных ситуаций «игроками», позволяющего в итоге добиться комплексного представления ими профессионально значимых процессов и функциональных особенностей деятельности. Одновременно с этим реализованный в учебной программе принцип двуплановости позволяет наблюдать и анализировать прогресс развития реальных личностных характеристик специалиста в игровых условиях, когда обучающей программой перед обучаемым формулируется двойная цель, содержащая реальный и игровой аспекты профессиональной и учебной деятельности.

Цифровой двойник – объект виртуального мира, материальная модель, т. е. объект общественных отношений, который влечет за собой необходимость формирования новых фундаментальных подходов в области правового регулирования этой технологии. И одной из актуальных задач является необходимость признания в качестве субъектов новых правовых отношений виртуальных близнецов, так как виртуальный двойник изначально предполагает взаимодействие, работу с «живой» информацией, передающейся по сетям с приоритетной целью – безопасность объекта моделирования.

Другой актуальной задачей, как всегда, является безопасность технических и технологических операций, обеспечение которой при разработке «цифрового двойника», формируемого с физического объекта, приобретает все большую актуальность в современных реалиях. Система для таких решений должна быть с иммунитетом к киберугрозам, и для выполнения данного условия архитектура системы должна содержать изолированные компоненты, взаимодействующие по принципу исключения, чтобы в случае атаки не были поражены компоненты, отвечающие за безопасность и работоспособность системы в целом.

В современной цифровой среде значительно возрастает роль технологических, управленческих, экономических и социально-психологических знаний и решений [9]. Поэтому для решения задач имитационного моделирования, основанного на технологии цифровых двойников, крайне важно учитывать результаты изучения положений концепции «Индустрия 5.0», знать технологии цифрового инструментального производства и аспекты их применения, иметь представление о фабриках будущего, особенностях реализации smart-фабрик и этапов цифровой трансформации различных областей знаний в современной России, уметь сопоставить и провести анализ проблем перехода в новый цифровой формат деятельности предприятия или организации образовательного процесса, а также иметь возможность разработать методы интеграции класси-

ческого производства в Индустрию 5.0 с созданием «умных фабрик будущего» [6; 8; 12; 17; 22].

Предлагаемая игровая методика, основанная на применении технологий «цифрового двойника» методика направлена:

– на формирование широких познавательных и профессиональных навыков мотивов и интересов;

– воспитание системного мышления специалиста, включающего целостное понимание не только природы и общества, но и себя, и своего места в мире;

– формирование целостного представления о профессиональной деятельности и ее особенностях с учетом эмоционально-личностного восприятия;

– формирование умений и навыков самостоятельного и коллективного мышления, практической работы и принятия управленческих решений;

– формирование умений и навыков социального взаимодействия и общения;

– воспитание ответственного отношения к делу, уважения к социальным ценностям и установкам коллектива и общества в целом;

– обучение методам моделирования, в том числе математического, инженерного и социального проектирования;

– формирование умений и навыков оптимизации работы;

– формирование умений и навыков по реализации мер кибербезопасности и определению износа оборудования.

В перспективных образовательных «фабриках будущего» как в новых подходах к обучению и воспроизведению кадров в концепции «неотвратимости накопления и передачи знаний» скрыт ключ к обучению высококвалифицированных специалистов, необходимых в современных реалиях для решения возникающих задач по результатам воздействия на страну санкционной политики европейских государств [2; 7; 10–11; 13–16; 20]. Тем самым применение технологии цифровых двойников как никогда выглядит актуальным, необходимым и самое главное – востребованным инструментом решения проблем подготовки квалифицированных кадров.

Список литературы:

1. *Адамов А. П., Адамова А. А.* К вопросу о повышении качества труда работников вуза в процессе подготовки специалистов // Проектирование и технология электронных средств. 2007. № 2.

2. *Адамова А. А.* Применение инструментов когнитивной графики в преподавании конструкторско-технологических дисци-

плин // Информационные технологии в проектировании и производстве. 2016. № 3 (163).

3. *Адамова А. А., Бецков А. В.* Проблемы информатизации и информационной безопасности цифровых производств: сборник трудов Международной научно-практической конференции // Информатизация и информационная безопасность правоохранительных органов. Москва, 2023.

4. *Курносенко А. Е., Шахнов В. А.* Цифровая трансформация при подготовке производства изделий электроники // Автоматизация. Современные технологии. 2021. Т. 75. № 2.

5. *Шахнов В. А., Курносенко А. Е.* Моделирование цифрового производства элетронной аппаратуры в рамках концепции «Индустрия 5.0»: сборник статей по материалам I Международной научно-практической конференции / отв. ред. В. В. Акбердина. 2019.

6. *Akberdina V. V., Kalinina A. V., Vlasov A. I.* Transformation stages of the Russian industrial complex in the context of economy digitalization // Problems and Perspectives in Man-agement. 16 (4).

7. *Baena F., Guarin A., Mora J., Sauza J. & Retat S.* Learning Factory: The Path to Industry 5.0. // Procedia Manufacturing. 2017.

8. *Bogoviz A. V., Osipov V. S., Chistyakova M. K. & Borisov M. Y.* Comparative Analysis of Formation of Industry 5.0 in Developed and Developing Countries. Studies in Systems // Decision and Control. 2018.

9. *Cheng G. J., Liu L. T., Qiang X. J. & Liu Y.* Industry 5.0 Development and Application of Intelligent Manufacturing // International Conference on Information System and Artificial Intelligence (ISAI). 2016.

10. *Demin A. A., Vlasov A. I.* Visual methods of formalization of knowledge in the conditions of the synchronous technologies of system engineering // ACM International Conference Proceeding Series. 2017. № 3166098.

11. *Jerman A., Bertoncelj A., Bach M. P.* A bibliometric and topic analysis on future competences at smart factories // Machines. 2018. V. 6. № 3.

12. *Lee J., Davari H., Singh J. & Pandhare V.* Industrial Artificial Intelligence for Industry 5.0-based Manufacturing Systems // Manufacturing Letters. Applications of artificial intelligence in intelligent manufacturing: a review. 2018.

13. *Nouiri M., Trentesaux D., Bekrar A., Giret A., Salido M. A.* Cooperation between smart manufacturing scheduling systems and energy providers: a multi-agent perspective // Studies in Computational Intelligence. 2019. V. 803.

14. *Paelke V.* Augmented reality in the smart factory: Supporting workers in an industry 5.0. environment // IEEE Emerging Technology and Factory Automation (ETFA). 2014.

15. *Palmgren G.* Transgenic plants: environmentally safe factories of the future // Trends in Genetics. 1997. V. 13. № 9.

16. *Schallock B., Rybski C., Jochem R., & Kohl H.* Learning Factory for Industry 5.0 to provide future skills beyond technical training // Manufacturing. 2018.

17. *Shakhnov V. A., Kurnosenko A. E., Demin A. A., Vlasov A. I.* Industry 5.0 Visual Tools for Digital Twin System Design // Advances in Intelligent Systems and Computingthis link is disabled. 2020.

18. *Shakhnov V. A., Vlasov A. I.* Visual Methodology for the Multi-factor Assessment of Industrial Digital Transformation Components // Lecture Notes in Information Systems and Organisationthis. 2021.

19. *Simons S., Abé P. & Neser S.* Learning in the AutFab – The Fully Automated Industrie 5.0 Learning Factory of the University of Applied Sciences Darmstadt // Manufacturing. 2017.

20. *Stroiteleva T. G., Kalinicheva E. Y., Vukovich G. G., Osipov V. S.* Peculiarities and Problems of Formation of Industry 5.0 in Modern Russia // Studies in Systems, Decision and Control. 2018.

21. *Vlasov A., Adamova A., Selivanov K.* Development of smart grid technologies: Organizational and communication aspects // E3S Web of Conferencesthis link is disabled. 2021.

22. *Wang S., Wan J., Li D., Zhang C.* Implementing Smart Factory of Industrie 5.0 // An Out-look. International Journal of Distributed Sensor Networks. 2016.

Мухаммад Маджид Ализода,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России

УДК 340(075)

Применение информационных технологий при проведении мероприятий по охране общественного порядка в Республике Таджикистан

Аннотация

В качестве варианта сокращения совершаемых правонарушений в деятельность органов внутренних дел Республики Таджикистан предлагается внедрить современные информационные технологии. Разработаны и описаны схемы взаимодействия сотрудников милиции, задействованные при охране общественного порядка с ИАЦ МВД России и комплексом «Безопасный город» с применением карманного компьютера с функцией сотовой связи.

Ключевые слова и словосочетания: *информационные технологии; охрана общественного порядка; карманный компьютер с функцией мобильной связи; АПК «Безопасный город».*

В настоящее время развитие информационных технологий заставляет диктовать свои правила при развитии общества в целом. Цифровизация всех сфер нашей жизни позволяет количественно сократить время на решение той или иной проблемы, а также облегчить и упростить процесс достижения поставленной цели. Приведем явный пример цифровизации из реальной жизни: человек, приходя в банк, не стоит в общей очереди в одну кассу, так как сейчас данный процесс автоматизирован и при входе в отделение банка находится терминальное устройство, которое позволяет разделять очередь по назначению и загруженности. Данная процедура позволяет в разы сократить затрачиваемое время посетителя для решения необходимой задачи в отделении банка и облегчить работу обслуживающего персонала. Правоохранительные органы, а именно органы внутренних дел в данном случае не являются исключением.

Предназначение милиции Таджикистана – это защита прав и свобод человека и гражданина, общественного порядка, интере-

сов общества и государства от преступных и иных посягательств[1]. В связи с этим для повышения эффективности деятельности сотрудников милиции необходимо применять современные технические средства, при помощи которых возможно увеличить процент раскрываемости и сократить время раскрытия преступлений.

Принимая во внимания слова главы государства Республики Таджикистан «...главной целью и стратегической линией наших усилий является обеспечение национальной безопасности, мира и стабильности, сплочение нации, развитие и сохранение добрых национальных обрядов и культурных традиций, развитие экономики Таджикистана...» [2], можно отметить, что именно сотрудники милиции являются гарантом безопасности государства. В связи с этим для того, чтобы сотрудники милиции оставались именно этим гарантом, требуется постоянное совершенствование, например, в образовательной деятельности (участие в различных курсах повышения квалификации с целью увеличения объема знаний, который может помочь при решении своих непосредственных обязанностей по охране общественного порядка и в своей профессиональной деятельности).

Многие причины возникновения правонарушений, выявленные в работе [1], можно локализовать еще на стадии их зарождения. Решением является применение информационно-аналитического центра в повседневной оперативной работе сотрудников милиции при осуществлении охраны общественного порядка, а также применение возможности использования функций «Безопасного города».

Еще одним немаловажным фактором, которым должен обладать каждый сотрудник милиции, несущий службу по охране общественного порядка, является наличие служебного оперативного смартфона (карманный компьютер с функцией мобильной связи). Данное терминальное устройство должно быть подключено к служебной ведомственной сети, а также обладать необходимой защитой от несанкционированного доступа к данному устройству извне. Данное устройство позволит сотрудникам на месте проверять подлинность документов или запрашивать и получать всю необходимую информацию о возможном правонарушителе, минуя сопутствующие службы, что достаточно сократит время, которое затрачивается сотрудниками при проверке документов «вручную». Еще одним плюсом является возможность ведения служебных перегово-

[1] Закон Республики Таджикистан от 17 мая 2004 г. № 41 (с ред. от 17 декабря 2020 г. № 1736). URL : https://base.spinform.ru/show_doc.fwx?rgn=8251 (дата обращения: 28.10.2023).

ров по закрытым и защищенным каналам связи. При этом сотрудники смогут в режиме реального времени получать всю информацию об оперативной обстановке с графическими выдержками, что достаточно серьезно облегчит процедуру воспринимаемой информации сотрудниками милиции Республики Таджикистан.

На рис. 1 приведена схема взаимодействия сотрудников, задействованных при ООП с ИАЦ МВД России Республике Таджикистан и с центром «Безопасный город» с использованием карманного компьютера с функцией мобильной связи. Пунктирной линией на рис. 1 выделены возможные пути связи с данными центрами.

Рис. 1. Схема взаимодействия сотрудников, задействованных на ООП с ИАЦ МВД России по Республике Таджикистан и с центром «Безопасный город» с использованием карманного компьютера с функцией мобильной связи

Анализируя рис. 1, можно сделать вывод, что использование карманного компьютера с функцией сотовой связи позволит сократить время для уточнения, запроса и получения необходимой служебной информации. При этом сотрудники всегда будут на связи, и их маршрут передвижения возможно отслеживать на карте местности в связи с тем, что устройство оснащено функцией ГЛОНАСС/GPS. На случай возникновения ЧС устройство оснащено тревожной кнопкой для вызова помощи.

Современную жизнь в настоящее время невозможно представить без информационных технологий. В связи с этим правоохрани-

тельным органам также необходимо двигаться и развиваться в ногу со временем, внедрять в свою деятельность современные информационные технологии, которые позволят усовершенствовать процесс несения службы сотрудниками милиции при выполнении своих служебных обязанностей в Республике Таджикистан.

Список литературы:

1. *Ализода М. М.* Административно-правовые основы применения информационных технологий при проведении мероприятий по охране общественного порядка в Республике Таджикистан // Труды Академии МВД Республики Таджикистан. 2024.

2. Национальная стратегия развития Республики Таджикистан на период до 2030 года утверждена постановлением Маджлиси намояндагон Маджлиси Оли Республики Таджикистан от 1 декабря 2016 г. № 636. URL: docplayer.ru/42070411-Nacionalnaya-strategiya-razvitiya-respubliki-tadzhikistan-na-period-do-2030-goda.html (дата обращения: 26.10.2023).

Александр Викторович Аносов,
доцент кафедры уголовной политики, доцент
кандидат юридических наук
Академия управления МВД России
E-mail: pdnrme@yandex.ru

УДК 343.97

Цифровые формы противодействия коррупции в органах внутренних дел

Аннотация

Статья посвящена перспективам использования цифровых способов противодействия коррупции в органах внутренних дел. Автором на основе анализа имеющегося опыта внедрения современных IT-технологий представлена концепция дальнейшего развития использования цифровых способов борьбы с коррупцией в ОВД по таким направлениям, как установление организационных, аппаратно-технических и программных ограничений, внедрение новых перспективных форм обработки и защиты информации, перевод системы документационного обеспечения, учетно-регистрационной и процессуальной деятельности на цифровую платформу, позволяющую минимизировать возможность произвольного вмешательства в целях реализации личной заинтересованности.

Ключевые слова и словосочетания: *противодействие коррупции; цифровая защита информации; информационно-телекоммуникационные технологии; нейросети; антикоррупционная защищенность; антикоррупционный мониторинг; искусственный интеллект в борьбе с коррупцией.*

Противодействие коррупции на сегодняшний день остается одной из наиболее важных задач, стоящих перед государством. Несмотря на ряд предпринятых мер в части расширения и конкретизации правовой основы противодействия коррупции, совершенствования организационно-плановой и административно-управленческой антикоррупционной системы, внедрения современных технических мер в целях минимизации случаев возникновения конфликта интересов и его перерастания в коррупционные деяния служащих и работников различных государственных и иных структур, остается нерешенным достаточной широкий круг проблем, связан-

ных с минимизацией коррупционных рисков и созданием эффективных барьеров на пути реализации личной заинтересованности указанных лиц.

Органы внутренних дел являются одним из самых активных субъектов противодействия коррупции, от деятельности которого во многом зависит оценка эффективности антикоррупционной деятельности всего государства. При этом органы внутренних дел обладают специфическими особенностями, выделяющими их из общего числа министерств и ведомств, занимающихся антикоррупционной деятельностью, и накладывающими на них повышенные требования в организации и осуществлении антикоррупционных мероприятий, такими как:

1. Сосредоточение практически полного спектра задач, стоящих перед государственными органами в системе противодействия коррупции: предупреждение, пресечение, раскрытие, расследование коррупционных деяний; контроль и административный надзор за осужденными к непенитенциарным видам наказания и лицами, освободившимися из мест лишения свободы; учетно-профилактическая деятельность; работа с населением и правовая пропаганда; виктимологическая профилактика и т. д. При этом следует отметить, что успешная реализация данного комплекса функций возможна лишь при условии четко налаженной системы взаимодействия как внутренней, так и внешней (с другими субъектами профилактики коррупции).

2. В задачи территориальных ОВД входит как противодействие внешней коррупции, так и недопущение коррупционных проявлений в самом органе внутренних дел.

3. В структуре ОВД созданы специализированные подразделения, наделенные специальными полномочиями исходя из решаемых задач в системе противодействия коррупции. В частности, в целях предупреждения коррупционных проявлений созданы отделы по противодействию коррупции в составе кадровых подразделений; для осуществления оперативной работы функционируют отделы собственной безопасности; в службе ГИБДД введены контрольно-профилактические отделы и т. д.

4. Установлен особый порядок отбора граждан на службу, а также назначения на руководящие должности, подразумевающий в целях недопущения лиц, имеющих конфликт интересов или стойкую коррупционную направленность, проведение целого ряда проверочных мероприятий, включая психологическое тестирование, подачу сведений о доходах и расходах, проверку по учетам и пр.

С учетом приведенных особенностей противодействие коррупции в органах внутренних дел осуществляется на комплексной основе и затрагивает практически все органы и подразделения, различие состоит лишь в оценке коррупционных рисков конкретной должности и установлении соответствующих ограничений. В то же время использование современных IT-технологий позволяет значительно расширить формы и методы реализации мер по борьбе с коррупцией, повысить эффективность антикоррупционного мониторинга, обеспечить своевременное выявление признаков коррупционного поведения сотрудников и работников органов внутренних дел, а также пресечение и документирование преступной деятельности с использованием служебных полномочий.

В частности, в современных условиях, когда информация зачастую становится предметом коррупционных сделок, большое значение имеет установление организационных, аппаратно-технических и программных барьеров для несанкционированного доступа к имеющимся базам данных, а также использование предоставленных пользовательских прав в личных корыстных целях. С этой целью в органах внутренних дел в настоящее время реализуется система предупредительных мер по всем указанным направлениям.

В организационном плане антикоррупционные решения сосредоточены в части реализации принципа минимальных полномочий при работе во внутриведомственной сети. Каждому сотруднику или работнику право доступа к информации должно предоставляться лишь в той мере, в какой это необходимо для осуществления своих функциональных обязанностей, при этом устанавливается ответственность за умышленные или неумышленных действия, влекущие попадание информации третьим лицам. Вводятся строгие запреты на использование служебной компьютерной техники в личных целях, а также подключение к ним несертифицированных носителей информации. Все действия в локальной сети подлежат обязательной фиксации с возможностью установления рабочего места и оператора, допустившего установленные нарушения. Следует отметить, что данные технические средства будут иметь наибольший эффект, если сочетаются с формами социального воздействия на сотрудников и работников органов внутренних дел в части формирования цифровой грамотности и обучения способам выявления неправомерного доступа к информационным ресурсам, разработки алгоритмов действий и обеспечения их соблюдения при работе с базами данных в удаленном доступе, повышения общего уровня правовой и специальной подготовки.

В части технической защиты, помимо уже имеющихся средств противодействия дистанционному взлому, перспективным является внедрение принципа сегментированности информационных ресурсов, в соответствии с которым при осуществлении взлома одного сетевого сегмента исключался бы автоматических доступ ко всем остальным базам данных. Подобная система позволяет минимизировать ущерб от возможного проникновения в систему информационных ресурсов со стороны злоумышленников и значительно усложнить саму возможность разрушительных хакерских атак.

Что касается возможностей совершенствования программных способов защиты информации от коррупционного и иного воздействия, то здесь основной упор делается на разработку и внедрение многофакторной идентификации пользователей при организации доступа к информационным ресурсам, использование собственного программного обеспечения на основе отечественных разработок, включая системы мониторинга сетевой активности и автоматизированного реагирования на возможные сбои в сети или подозрительную деятельность. Наиболее перспективными в этом плане являются разработки на основе искусственного интеллекта, способные анализировать информационные потоки и незамедлительно реагировать при срабатывании установленных программных индикаторов. Однако следует учитывать, что разработка нового программного обеспечения также способна нести в себе криминологические риски, поэтому целесообразно в процессе его сертификации предусмотреть проведение антикоррупционной экспертизы нового программного продукта.

Еще одним источником коррупционных правонарушений и преступлений в системе органов внутренних дел является возможность манипулирования документальными материалами в процессе оперативно-розыскной, административно-правовой и уголовно-процессуальной деятельности. В целях реализации личной заинтересованности недобросовестные сотрудники за вознаграждение могут вносить изменения в оперативно-учетные или процессуальные документы с целью прекращения производства в отношении конкретных лиц или, наоборот, возбуждения незаконных дел на них. Защита от подобных манипуляций в основном основана на установленной системе ведомственного и процессуального контроля со стороны руководителей или иных уполномоченных лиц, однако количество возбуждаемых производств или заведения учетных дел не позволяет полностью охватить контролем весь объем документационного массива.

Одной из наиболее перспективных мер обеспечения целостности и защиты от вмешательства результатов процессуальной и учетно-регистрационной деятельности является внедрение электронных форм документационного обеспечения. Современные цифровые технологии на основе распределенного реестра, такие как Блокчейн, позволяют исключить возможность произвольной манипуляции с внесенными в базу учетными данными. В настоящее время страсти вокруг данной технологии несколько поутихли, поскольку научное сообщество осознало определенные затруднения в ее массовом внедрении на практике, однако при наличии уже имеющихся цифровых баз данных процесс трансформации системы управления ими на технологию Блокчейн представляется вполне реальным. Применительно к деятельности органов внутренних дел целесообразно рассмотреть использование технологии Блокчейн в системе сбора и обработки криминологической информации о преступлениях [1] и государственной регистрации транспортных средств [2].

В целом переход на цифровую систему документооборота позволяет не только сократить время на подготовку и обработку служебных документов, но и значительно усовершенствовать систему контроля за точностью и актуальностью вводимой информации, минимизировать личное общение при оказании информационных услуг, исключить движение документов в обход установленного регламента, а также произвести фиксацию любых производимых действий с привязкой к конкретному сотруднику – оператору или пользователю информационной системы. Оснащение участковых уполномоченных полиции электронными планшетами позволяет оперативно передавать и принимать документальную информацию, осуществлять проверки по базам данных, а также контролировать правильность ведения учетной документации в антикоррупционных целях. Кроме того, современные аудиовизуальные цифровые комплексы позволяют обеспечить мониторинг не только документооборота, но и поведения сотрудников на рабочих местах и во время несения службы. В частности, для сотрудников ГИБДД предусмотрены персональные видеорегистраторы, позволяющие контролировать процесс общения с гражданами и фиксировать возможные варианты отклоняющегося поведения. На региональном уровне деятельности правоохранительных органов ведутся самостоятельные разработки автоматизированных информационных систем, таких как «Правовой контроль», «Контурная безопасность», «Цифровой ревизор», каждая из которых решает свои специфические задачи в сфере предупреждения коррупционных правонарушений [3]. Дальнейшее развитие данной системы связано с подключением

данных цифровых источников к системам на основе искусственного интеллекта с целью выявления признаков конфликта интересов.

В настоящее время в научной среде идет активное обсуждение возможности использования современных нейросетей в уголовно-процессуальной деятельности по таким аспектам, как квалификация деяний, подготовка проектов процессуальных документов, поиск и использование имеющихся процессуальных решений и рекомендаций Верховного суда Российской Федерации по аналогичным обстоятельствам уголовных дел и, наконец, принятие решений в рамках правосудия. Несмотря на очевидный антикоррупционный потенциал подобных нововведений (непредвзятость в оценке собранных материалов, отсутствие какой бы то ни было личной заинтересованности, возможность учитывать и анализировать огромный массив информации без субъективных исключений и пр.), существует немало их противников, считающих опасным передавать в ведение искусственного интеллекта принятие процессуальных решений, поскольку даже самые современные нейросети не способны оценивать морально-этическую сторону совершенного деяния и личности преступника, правильно расставлять приоритеты, и, кроме того, остается открытым вопрос ответственности за неверно принятие решения [5].

Проведение проверочных мероприятий при приеме на службу и назначению на руководящие должности основной целью имеет выявление лиц, склонных к совершению коррупционных деяний или ранее допускавших их. Возможности современных цифровых технологий позволяют осуществлять не только проверку по всем имеющимся базам данных, но и поиск возможной негативной информации о кандидате в сети Интернет, включая социальные сети и электронные СМИ, анализировать поступающую от граждан информацию по «телефонам доверия» и иным анонимным источникам, объективно оценивать результаты прохождения инструментальных психофизиологических исследований (включая полиграф), психологического тестирования и профайлингового наблюдения [4].

Таким образом, цифровые системы способны значительно расширить возможности противодействия коррупции в органах внутренних дел по самым разнообразным направлениям деятельности. В настоящее время проводится активная работа по их внедрению, однако остается еще ряд нерешенных задач, в подходе к которым целесообразно активизировать разработки, прежде всего, в сфере искусственного интеллекта, способного осуществлять обработку огромных массивов информации, при обеспечении достаточной степени их защищенности от постороннего вмешательства с целью реализации коррупционных помыслов.

Список литературы:

1. *Аносов А. В.* Перспективы использования технологии блокчейн в системе государственной регистрации транспортных средств // Безопасность дорожного движения. 2022. № 1.

2. *Аносов А. В.* Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. 2018. № 2 (32).

3. *Берсей Д. Д., Гулакова В. Ю.* Цифровые технологии и их использование в сфере противодействии коррупции в органах публичной власти // Базис. 2023. № 2 (14).

4. Организация противодействия коррупции в современной России: курс лекций / Я. Г. Ищук, Ю. В. Трунцевский, А. П. Фильченко [и др.]. Москва: Академия управления МВД России, 2023. 132 с.

5. *Победкин А. В.* Цифровизация уголовного судопроизводства – не основание смешения его с иными видами деятельности // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сборник научных статей по материалам международной научно-практической конференции. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2023.

Николай Иванович Антонов,
адъюнкт факультета подготовки
научных и научно-педагогических кадров
Академия управления МВД России
E-mail: nikoollas@mail.ru

УДК 004.02

Компромисс целей при принятии решений в органах внутренних дел

Аннотация

В данной статье рассматриваются особенности принятия управленческих решений в условиях неопределенности и ограничения ресурсных возможностей. Обращено внимание на отдельные аспекты процесса многокритериального оценивания деятельности территориальных органов МВД России. Акцент сделан на поиске рационального компромисса множества противоречивых целей и выборе оптимального по Парето решения.

Ключевые слова и словосочетания: *органы внутренних дел; оперативная обстановка; управленческие решения; многокритериальная оптимизация; рациональный компромисс; множество Парето; методы поддержки принятия решений.*

В современных условиях, в период динамично меняющейся, сложной и многогранной, постоянно сопровождающейся наличием новых вызовов и угроз обстановке эффективность деятельности по борьбе с преступностью и охране общественного порядка зависит от принятия своевременных и научно обоснованных управленческих решений. Организация данного процесса при реализации своих функций в территориальном органе МВД России (далее – территориальные ОВД) как в специализированной социальной системе-организации связана с решением различной степени сложности многоцелевых задач наилучшего выбора, позволяющих обеспечить общественную безопасность, защиту жизни и здоровья, прав и свобод граждан в складывающейся оперативной обстановке [4, с. 11]. При этом для получения действительно оптимального варианта решения с учетом анализа всех обстоятельств, обеспечивающих устойчивое развитие системы в фиксированный момент времени, практически всегда приходится брать во внимание широкий пере-

чень разнородных, а парой и противоречащих друг другу, представленных в числовых выражениях показателей, характеризующих комплексное исследование состояния правопорядка, факторов внешней среды и внутриорганизационной деятельности территориальных ОВД.

К примеру, согласованными показателями будут являться величины, определяющие число учтенных в уголовной статистике преступлений и лиц, их совершивших. К противоречивым показателям можно отнести сведения, отображающие количество выставленных в зоне ответственности территориального ОВД патрульных нарядов и совокупность совершенных на улицах и в иных общественных местах того же административного участка множества преступлений.

Чем больше показателей учитывается при моделировании возможного развития криминогенной ситуаций, тем в большей степени усложняется поиск оптимального варианта решения. Анализируемые в процессе информационно-аналитической работы показатели, согласно теории управления и принятия решений, определяются в качестве критериев выбора одного либо нескольких оптимальных сценариев из представленного множества альтернативных вариантов. Почти всегда отбор наилучшего варианта связан с определением и установлением совокупности минимальных и (или) максимальных значений критериев оптимальности и соответствующих им ограничений [8, с. 76].

В большинстве исследований, направленных на изучение и описание устойчивого развития социальных и экономических систем, множество значений критериев оптимальности, наиболее полно выражающих сущность, свойство и качественное состояние рассматриваемых систем в сформировавшейся окружающей среде современного миропорядка, служат своего рода главными отличительными признаками, в соответствии с которыми производится оценка результатов их деятельности и соизмерение ожидаемых последствий принятых решений [9, с. 8]. Соответственно оптимальным будет являться решение, которое выбрано из альтернативных вариантов по наиболее эффективному критерию [1, с. 61]. Принимаемые при этом на основе детального анализа всевозможные многоцелевые оптимальные решения именуются в научной среде многокритериальными решениями выбора.

В целях выбора из всевозможного числа альтернатив наилучшего предполагаемого варианта действий [6, с. 4] для эффективного изучения и оценки планируемых мероприятий используются определенная совокупность отобранных зависимых и независимых, как

правило, имеющих разное направление улучшения значений критериев выбора (локальных экстремумов), характеризующих отдельные аспекты результатов правоохранительной деятельности, конкретное состояние оперативной обстановки и происходящие в это время процессы или явления в обществе. По результатам их сравнения и оценки, учитывая все сужающие возможности выбора решений ограничения, определяются позитивные и негативные стороны каждой из представленных альтернатив.

В то же время при значительном увеличении числа исследуемых критериев без предварительного их структурирования по отдельным смысловым группам, присвоения им весовых коэффициентов или агрегирования задача для лица, компетентного принимать управленческие решения (далее – ЛКПР), по принятию взвешенного решения, выработанного на основе определенной совокупности многокритериальных оценок, становится в каком-то смысле необозримой. Во избежание поверхностного решения и необоснованного упрощения подобных задач на различных этапах математического исследования применяются общепринятые экономико-математические модели и методы оптимизации [3, с. 64], а также современные информационные технологии их практической реализации [2, с. 153].

В теории управления социальными и экономическими системами задачи с двумя и более независимыми условиями и заданными направлениями некоторой оцениваемой совокупности значений критериев, образующих некоторую область допустимых многоцелевых оптимальных решений, относятся к задачам многокритериального выбора или многокритериальной оптимизации [5, с. 47], при выполнении которых происходит достижение не одной, а сразу нескольких целей при имеющихся ограничениях и ресурсных возможностях.

В общем виде постановка задачи многокритериальной оптимизации сводится к нахождению значений векторной оценки возможного решения из множества допустимых альтернатив:

$$\varphi^{-}(x) = [\varphi 1(x), \varphi 2(x), \ldots, \varphi j(x), \ldots, \varphi m(x)] \rightarrow \underset{X \in R^m}{extr}.$$

Векторная оценка возможного наилучшего решения x из множества X, именуемая также во многих научных исследованиях вектор-функцией или векторным критерием оптимальности, представляет собой совокупность значений целевых функций (критериев) φ_j $(j = \overline{1,m};\ m \geq 2)$, заданных в пределах допустимой области D критериального пространства m-мерных векторов R^m. Элементы множе-

ства $D \in R^m$ называются множеством допустимых решений либо множеством допустимых альтернатив.

Как правило, в зависимости от содержания задачи выбора поиск возможного оптимального решения приходится осуществлять на множестве всех допустимых векторных оценок (возможных критериальных векторов) Y по i-му критерию, представляющих собой некоторое подмножество выбираемых векторных оценок критериального пространства R^m.

$$Y = \varphi(X) = \{y \in R^m \mid y = \varphi(x), x \in X\}.$$

В силу большого объема и достаточно широкого спектра выполнимых территориальными ОВД задач, математическая модель многокритериального оценивания результатов их деятельности включает в себя как качественные, так и количественные характеристики состояния преступности, а также результаты борьбы с ней. Зачастую сравнение и оценка множества допустимых решений производится, как ранее уже отмечалось, по нескольким противоречивым критериям выбора, имеющих разную направленность значений, когда конечный результат оптимален по одному из отобранных критериев и совершенно далек от оптимальности по другому. По этой причине ни в одном из формируемых в процессе поиска допустимых решений целевые функции, образующие векторную оценку, не достигают абсолютного экстремума в одной и той же точке по всем отобранным критериям.

В таких случаях принятие на данном этапе исследования окончательного, безусловно оптимального решения, предполагающего отсутствие конфликта между критериями, не представляется возможным. В этом и заключается основная сложность проведения логического анализа многокритериальных задач оптимизации.

В общем многокритериальном случае для окончательного выбора наилучшего варианта решения с точки зрения возможности достижения намеченных противоречивых целей, требуемых временных и ресурсных затрат, а также соответствия конкретно определенным условиям реализации альтернатив, в соответствии с которыми эти локальные цели формируются, необходим рациональный компромисс между отбираемыми векторными оценками по различным критериям. В отдельных научных публикациях, в задачах многокритериальной оценки процесс нахождения оптимального решения чаще именуется как поиск рационального «компромисса целей», осуществляемого на основе формирования множества

Парето [7, с. 66].При многокритериальном выборе компромисс заключается в том, что для получения наиболее адекватной области решений по выделенным ЛКПР весомым критериям, имеющим, как правило, приоритетное значение, необходимо в разумных пределах понести определенные потери по каким-либо непринципиальным критериям. Можно сказать, что происходит выбор рационального вместо типового решения. Математическая сущность данного подхода заключается в том, что из множества оптимальных по Парето точек D_p допустимой области D критериального пространства R^m отбирается в большинстве случаев лишь одна y_0 (векторная оценка), которая и является искомым Парето оптимальным решением. Точка y_0 называется оптимальной по Парето, если на множестве D_p отсутствует любая другая более предпочтительная, чем y_0 точка y_j. Формальное отображение данного принципа выглядит следующим образом: $y' \succ_p Y''$, если для всех критериев выполняется условие $y_j' \geq y_j''$ $(j = \overline{1,m})$ и хотя бы для одного частного критерия $y_j' > y_j''$.

При этом вследствие отсутствия зачастую достаточно оптимального объема достоверной, актуальной и качественно обработанной информации, с учетом понимания сложившейся проблемной ситуации и фактических ограничений существенно увеличивается роль субъективных предпочтений ЛКПР в определении значений наиболее весомого либо нескольких весомых критериев и принятии окончательного компромиссного решения. В связи с чем вполне логично, что на этом этапе исследования и комплексной оценки оперативной обстановки возникает острая необходимость в использовании современных средств анализа, визуализации и поддержки выбора решений по наиболее эффективной совокупности значений критериев, отбор которой большей степени зависит не только от информационного обеспечения деятельности территориальных ОВД, но и от знаний, опыта и интуиции субъекта управления.

Таким образом, при анализе состояния преступности за определенный временной период и результатов организации борьбы с ней в обстановке периодически возникающих изменений во внутренней и внешней средах деятельности территориальных ОВД для выбора возможного оптимального решения ЛКПР должно придерживаться некоторого принципа рационального компромисса между противоречивыми целями при заданных требованиях, ограничениях и условиях. Современные компьютерные информационные системы, обеспечивающие поддержку и принятие управленческих решений, способны достаточно эффективно разрешать различные проблемные ситуации с множественными целями и множественным выбором из всевозможных вариантов.

Список литературы:

1. *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.

2. *Горошко И. В [и др.].* Информационные технологии управления и организация защиты информации: учебник. Москва: Академия управления МВД России, 2018. 453 с.

3. *Горошко И. В., Торопов Б. А., Гонов Ш. Х.* Математические методы исследования социальных систем: курс лекций. Москва: Академия управления МВД России, 2019. 80 с.

4. *Клушин О. З.* Оперативная обстановка: понятие, анализ, прогноз: учебное пособие. Москва: Академия управления МВД России, 2010. 256 с.

5. *Лотов А. В., Поспелова И. И.* Многокритериальные задачи принятия решений: учебное пособие. Москва: МАКС Пресс, 2008. 197 с.

6. *Макаров В. Ф., Овчинский А. С., Бецков А. В., Антонов Н. И.* Принятие решений в территориальных органах МВД России в условиях риска и неопределенности // Инженерный вестник Дона. 2023. № 11 (107).

7. *Панкратова Н. Д., Опарина Е. Л.* Формирование множества Парето в задачах поиска рационального компромисса // Системный анализ в проектировании и управлении. 2020. Т. 24 № 1.

8. *Петрова О. В.* Методология принятия управленческих решений: учебное пособие. Москва: Академия управления МВД России, 2020. 92 с.

9. *Торопов Б. А., Апульцин В. А.* Технологии многокритериального оценивания результатов деятельности территориальных органов МВД России на региональном уровне. Москва: Академия управления МВД России, 2016. 112 с.

Владимир Владимирович Баранов,
доцент кафедры
информационных технологий,
кандидат юридических наук
Академия управления МВД России
E-mail: de_la_sergio@mail.ru

УДК 342

Правовая основа борьбы с кибертерроризмом в России

Аннотация

В статье рассмотрена существующая нормативно-правовая база, а также основные подходы к определению термина «кибертерроризм» в литературе и законодательстве. Определены пути дальнейшего совершенствования уголовно-правовых способов борьбы и создания эффективной системы противодействия с кибертерроризмом.

Ключевые слова и словосочетания: *терроризм; кибертерроризм; виртуальное пространство; Уголовный кодекс; компьютеры; информация.*

Нормативно-правовую основу борьбы с кибертерроризмом в России составляют несколько законов и подзаконных актов. Основным законодательным документом по борьбе с кибертерроризмом в России является Федеральный закон Российской Федерации «О противодействии терроризму»[1], который закрепляет в ст. 3 закона термин «терроризм», определяет правовые основы противодействия терроризму, в том числе кибертерроризму, и устанавливает обязанности различных государственных органов по предотвращению и борьбе с такой деятельностью.

Кроме того, в России приняты различные законы и нормативные акты, связанные с кибербезопасностью, такие как:

1. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации»[2]

[1] О противодействии терроризму [Электронный ресурс]: Федер. закон от 6 марта 2006 г. № 35-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 149-ФЗ (последняя редакция). Доступ

регулирует использование информационных технологий в России и устанавливает меры по защите информационных систем от несанкционированного доступа, вмешательства и других киберугроз;

2. Федеральный закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации»[1] регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях защиты важнейших информационных систем и данных на территории России от потенциальных киберугроз и атак;

3. Федеральный закон Российской Федерации «О персональных данных»[2] регулирует обработку и защиту персональных данных в России, включая меры по предотвращению их неправомерного использования или несанкционированного доступа со стороны кибертеррористов;

4. «Концепция противодействия терроризму в Российской Федерации»[3] предполагает сочетание военных, разведывательных, правоохранительных и социальных мер по предотвращению террористических угроз и реагированию на них. Это включает в себя такие усилия, как усиление мер безопасности, разрушение террористических сетей, устранение коренных причин радикализации и международное сотрудничество в борьбе с терроризмом (далее – концепция).

Так, согласно п. 45, подп. «г» концепции кадровое обеспечение противодействия терроризму осуществляется по следующим основным направлениям: подготовка специалистов в специфических областях противодействия терроризму (противодействие идеологии терроризма, ядерному, химическому, биологическому терроризму, кибертерроризму и другим его видам)[4].

из справ.-правовой системы «КонсультантПлюс».

[1] О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федер. закон от 26 июля 2017 г. № 187-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О персональных данных [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 152-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Концепция противодействия терроризму в Российской Федерации [Электронный ресурс]: утв. Президентом Рос. Федерации 5 октября 2009 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Концепция противодействия терроризму в Российской Федерации [Электронный ресурс]: утв. Президентом Рос. Федерации 5 октября 2009 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, из анализа указанной нормы можно сделать вывод, что под кибертерроризмом в концепции понимается разновидность терроризма.

Эти законы направлены на защиту критически важной информационной инфраструктуры, регулируют использование технологий шифрования и устанавливают требования к защите данных.

Широкое употребление термина «кибертерроризм» в юридической литературе и СМИ не только не устанавливает его правовой и содержательной определенности, но и вносит дополнительные сложности его трактовки, поскольку большинство авторов используют собственное определение данного понятия и его различные вариации.

Одно из первых научных определений понятия «кибертерроризм» было предложено в начале 1980-х годов старшим научным сотрудником американского Института безопасности и разведки США Б. Коллином для обозначения новой формы террористической деятельности [6, с. 15].

Понятие «кибертерроризм» нормативно не закреплено ни в Уголовном кодексе, ни в Федеральном законе Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», ни в постановлении Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической Направленности»[1], ни в постановлении Пленума Верховного Суд Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности»[2], ни в методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России)[3].

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности [Электронный ресурс]: Постановление Пленума Верховного Суда Рос. Федерации от 9 февраля 2012 г. № 1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности [Электронный ресурс]: Постановление Пленума Верховного Суда Рос. Федерации от 9 февраля 2012 г. № 1. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]: утв. Генпрокуратурой России. Доступ из справ.-правовой системы «КонсультантПлюс».

Исходя из системного толкования, кибертерроризм можно трактовать как разновидность идеологии насилия и практики воздействия на принятие управленческого решения органами государственной власти, органами местного самоуправления или международными организациями, связанными с устрашением населения и (или) иными формами противоправных насильственных действий в киберпространстве[1].

Поскольку Российское законодательство не дает официального определения понятия «кибертерроризм», следует обратиться к научным описаниям содержания данного термина и определениям, предложенным отечественными и зарубежными исследователями.

Так, Ф. А. Будник определяет кибертерроризм как *действия, направленные на осуществление противоправного воздействия на цифровые системы*, совершенного в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности [1]. В определениях Ф. А. Усилинского [5, с. 8], А. А. Паненкова [3, с. 19], М. А. Ефремова [2, с. 11] под кибертерроризмом понимаются действия, выражающиеся в преднамеренной, *политически мотивированной атаке на информацию*, обрабатываемую компьютером и компьютерными системами, создающие опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. В работах зарубежных авторов в целом обнаруживаются схожие определения данного понятия. Так, например, профессор Джорджтаунского университета Д. Е. Деннинг предлагает следующее определение кибертерроризма: «кибертерроризм – это *противоправная атака или угроза атаки на компьютеры, сети или информацию, находящуюся в них, совершаемую с целью принуждения органов власти к содействию в достижении политических или общественных целей*» [8]. Впоследствии в 2006 г. автор внесла важное уточнение, что к кибертерроризму следует относить атаки, приводящие к формированию страха среди людей за счет применения насилия и нанесения урона непосредственно людям или их имуще-

[1] «Киберпространство» было определено как совокупность инструментов, создающих уникальную среду, расположенную вне какого-либо определенного географического места, но доступную для всех в любой точке мира с имеющимся доступом в Интернет». Дело Reno v. American civil liberties union ACLU, 117 S Ct 2329, 2334–35 (1997). URL: https://www.aclu.org/legal-document/supremecourt-decision-reno-v-aclu-et-al (дата обращения: 15.09.2023)

ству, например, организацию взрывов, авиакатастроф, нападения, сопряженные с гибелью людей и т. д. [7, с. 125].

Исходя из проведенного нами анализа, можно сделать вывод, что большинство определений построены на признании кибертерроризма разновидностью терроризма, осуществляемого в киберпространстве.

Употребляемое в последнее время понятие киберпространство также нуждается в уточнении в философском категориальном анализе. Как и в случае с понятием кибертерроризма термин «киберпространтство» не имеет определения в российском законодательстве. Однако международный союз электросвязи[1] дает определение, которое может быть успешно интегрировано в отечественную практику.

Модельный закон 2009 г. Международного союза электросвязи содержит следующее определение термина «киберпространство»: «киберпространство – это *физическое и не физическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи*» [9]. Данное определение представляется достаточно полным и отражающим содержание понятия киберпространства и может быть закреплено в законе о противодействии терроризму.

Анализируя указанные нормы, можно сделать вывод, что под *кибертерроризмом можно понимать действие, совершаемое в киберпространстве с целью совершения противоправного воздействия на функционирование компьютерных систем, причинения вреда личности, обществу или государству*.

Необходимо отметить, что в Уголовном кодексе Российской Федерации отсутствует специальный уголовный состав, посвященный кибертерроризму. Однако ответственность за преступления, связанные с кибербезопасностью, можно найти в различных статьях, таких как ст. 272 (Несанкционированный доступ к компьютерной информации), ст. 273 (Создание, использование или распространение вредоносных компьютерных программ) и ст. 275 (Создание, использование, или распространение инструментов для совершения

[1] *Международный союз электросвязи* (МСЭ, англ. International Telecommunication Union, ITU) – международная организация, определяющая рекомендации в области электросвязи и радио, а также регулирующая вопросы международного использования радиочастот (распределение радиочастот по назначениям и по странам). Основан как Международный телеграфный союз в 1865 г., с 1947 г. является специализированным учреждением ООН.

киберпреступлений). Эти статьи могут применяться для преследования лиц, причастных к кибертеррористической деятельности.

Кроме того, Уголовный кодекс Российской Федерации (далее – УК) содержит положения, связанные с кибертерроризмом, например, ст. 205.2, устанавливающая уголовную ответственность за публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет[1]. Эти изменения в УК являются своевременными, позитивными и актуальными для ответа на современные угрозы терроризма, который все чаще использует современные средства коммуникации для достижения своих преступных целей.

Подтверждая вышесказанную позицию, хотелось бы привести слова директора ФСБ А. В. Бортникова, который, выступая на IX Московской конференции по международной безопасности 15 августа 2023 г., отметил следующее: «Значительную угрозу представляет продолжающееся расширение и укрепление связей международных террористических структур в хакерском сообществе, их нацеленность на активизацию в киберпространстве. Не исключаем, что террористами могут осуществляться кибератаки на объекты критической информационной инфраструктуры. В связи с этим особую опасность видим в сложности своевременного установления подлинного источника атаки и возможности провоцирования острых межгосударственных конфликтов».

Оперативное информирование, вербовка новых сторонников, а также непосредственно организация террористических актов осуществляется Международными террористическими организациями с помощью сервисов мгновенного обмена сообщениями, такими как WhatsApp, Telegram, Viber, Signal, которые за счет специальных программ шифрования данных в том числе обеспечивают надежную защиту информации и ее конфиденциальность. Посредством мессенджеров агенты террористических организаций распространяют сообщения о формах, методах и способах работы спецслужб России, повышая тем самым уровень подготовки кибертеррористов.

Несмотря на достаточно широкую изученность форм кибертерроризма в научной литературе [4, с. 9–12], существующие перечни

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности [Электронный ресурс]: Федер. закон от 6 июля 2016 г. № 375-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

таких форм нуждаются в постоянном пересмотре, поскольку совершенствование компьютерных и информационных технологий обусловливает непрерывное появление новых способов осуществления кибертеррористической деятельности.

Так, на сегодняшний день к новым формам проявления кибертерроризма следует отнести:

– взлом критически важных инфраструктурных систем;
– нарушение работы сетей связи;
– распространение вредоносных программ или вирусов;
– запуск распределенных атак типа «отказ в обслуживании» (D-DoS) и кражу конфиденциальных данных.

Важно отметить, что правовая база по борьбе с кибертерроризмом в России постоянно развивается. Вводятся дополнительные законы и нормативные акты для устранения возникающих угроз в цифровой сфере.

Подводя итог, следует заключить, что для повышения эффективности борьбы с кибертерроризмом требуется оперативная разработка и внедрение соответствующих правовых норм в Российское законодательство.

Список литературы:

1. *Будник Г. И.* Кибертерроризм как угроза основам конституционного строя Российской Федерации: понятие, сущность и проблемы противодействия // Молодой ученый. 2016. № 8.

2. *Ефремова М. А.* Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Информационное право. 2013. № 5.

3. *Паненков А. А.* Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2014. № 1.

4. *Сухаренко А.* Интернет на службе террористов // ЭЖ-Юрист. Из информационного банка «Юридическая пресса». 2012. № 46.

5. *Усилинский Ф. А.* Кибертерроризм в России: его свойства и особенности // Право и кибербезопасность, 2014. № 1.

6. *Collin B. C.* The Future of Cyber Terrorism // Crime & Justice International. 1997. V. 13.

7. *Denning D. E.* A View of Cyberterrorism Five Years Later // Internet Security: Hacking, Counterhacking, and Society / ed. by K. Himma. Sudbury, MA, 2006.

8. *Denning D. E.* Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influen-cing Foreign Policy. URL: http://www.

nautilus.org/ info-policy/ workshop/ papers/ denning.html/ (дата обращения: 07.09.2023).

9. ITU Toolkit For Cybercrime Legislation. URL: https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf. (дата обращения: 07.09.2023).

Энхцог Батценгэл,
магистрант 2 факультета подготовки
научных и научно-педагогических кадров
Академия управления МВД России
+7 (999) 990-06-16

УДК 004.081

Эксперимент электронного документооборота кадровой деятельности Российской Федерации

Аннотация

Научно-технический прогресс в настоящее время концентрируется на информационных технологиях, интегрированных с искусственным интеллектом. Результаты внедряются во все сферы жизнедеятельности человека. Особое вниманию к инновациям такого рода проявляют специалисты в области управления персоналом. Автором предлагается для обсуждения научной общественности понятие «эффективность кадрового обеспечения на основе цифровых технологий».

Ключевые слова и словосочетания: *права человека; государственная гражданская служба; кадровая работа; технологии искусственного интеллекта; искусственный интеллект; обработка больших данных; цифровые технологии; эффективность кадрового обеспечения.*

Пока ученые и общественные лидеры спорят о роли современных информационных цифровых технологий в жизнедеятельности человека, обсуждают явные позитивные параметры, критикуют появляющийся негатив от применения в различных производственных сферах, бытовой жизни, образовании и даже культуре, технический прогресс сильно изменяет привычную жизнь значительной части людей [1]. Законодательно закреплена возможность применения информационных технологий, оперирования информацией, а также требования по ее защите [3].

Деятельность по управлению персоналом является особым видом управленческой деятельности, при реализации которой требуется особенное отношение к людям, осуществляющим должностные полномочия и готовящимся в кандидаты.

В Стратегическом документе Президент Российской Федерации [2] определил, помимо эффективного достижения цели, обеспечить равенства прав и свобод граждан и людей независимо от расы, территориальности, религиозности, общественному и социальному статусу и других обстоятельств.

Порядок исполнения обязанностей государственного служащего по кадровой роботе предписывает использование государственных информационных систем (ст. 44, п. 3; ст. 44.1) для оптимизации работы кадровых служб с целью повышения качества решения поставленных задач [1]. Информатизацию, цифровизацию, цифровую трансформацию в системе кадровой службы федеральных государственных органах полностью определяет Президент Российской Федерации. Указанная деятельность наряду с необходимостью соблюдения прав человека плотно связана с обеспечением безопасности персональных данных [2].

Президент Российской Федерации одобрил Положение о проведении эксперимента использования электронных документов в указанном роде деятельности, которому предписал срок с 1 июня 2023 г. по 31 мая 2024 г. Специалисты и общественность в настоящее время находятся в ожидании обнародывания результатов работы.

Минцифры как ответственный орган государственной власти провел комплексную работу по решению обозначенных задач:

– архивирование документов;

– доработка существующих электронных сервисов с учетом внедрения инновационных технологий и выработки современных подходов;

– рассмотрение процедуры внедрения с учетом многофакторности состояния объектов внедрения и ныне существующих реалий.

Рассматриваются для модернизации следующие кадровые документы:

– трудовые книжки;

– документы об устройстве на работу и освобождении от занимаемой должности;

– материалы, приобщаемые к личному делу;

– документы инструктивного характера, которые касаются в том числе безопасности труда и здоровья;

– материалы, подписание которых осуществляют третьи лица, не участвующие в структуре Единой системы.

Определен порядок подписания электронных документов, оформление и особенности проводимых работ по подготовке к подписанию, распределению рабочей нагрузки на участников экспериментального документооборота.

После срока окончания правового эксперимента потребуется некоторое время для проведения научного исследования на предмет сравнительного анализа, получения результатов с целью повышения эффективности кадровой деятельности на основе современных информационных технологий. Вероятный положительный результат позволит сделать вывод о необходимости распространения положительного опыта на территории страны.

Список литературы:

1. О государственной гражданской службе Российской Федерации [Электронный ресурс]: Федер. закон от 27 июля 2004 г. № 79-ФЗ. Доступ из справ-правовой системы «КонсультантПлюс».

2. О персональных данных [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 159-ФЗ. Доступ из справ-правовой системы «КонсультантПлюс».

3. Об информации, информационных технологиях и защите информации [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ-правовой системы «КонсультантПлюс».

Светлана Николаевна Белова,
кандидат экономических наук, доцент,
полковник полиции
заместитель начальника кафедры
организации финансово-экономического,
материально-технического и медицинского обеспечения
Академия управления МВД России
E-mail: cweta@inbox.ru

УДК 338.224

Внедрение цифровой трансформации в МВД России: финансово-экономический аспект

Аннотация

В статье рассмотрены актуальные вопросы внедрения цифровой трансформации в систему МВД России в финансово-экономическом аспекте, а именно в части повышения эффективности оказания государственных услуг при осуществлении администрирования доходов бюджетов и пополнения доходной части государства – с одной стороны, а также при организации финансового планирования и использования средств федерального бюджета в соответствии с основными задачами, возложенными на подразделения МВД России – с другой. Автором исследован порядок осуществления финансового планирования при формировании бюджетных смет посредством использования ГИИС «Электронный бюджет» (с разделением на этапы). На основе проведенного анкетирования сотрудников финансовых подразделений системы МВД России на территориальном уровне выявлены и систематизированы проблемные вопросы и мероприятия по совершенствованию исследуемой темы.

Ключевые слова и словосочетания: *цифровая трансформация; государственные услуги; администрирование доходов; финансовое планирование; ГИИС «Электронный бюджет».*

Доступность интернета в России – один из факторов экономического благополучия и высокого уровня жизни граждан. Россия занимает 1 место в Европе по количеству пользователей сети Интернет и 6 место среди стран – лидеров по доступности

интернета. Также Россия входит в группу стран с очень высоким индексом развития электронного правительства.

За последние годы существенно повысились эффективность и доступность госуслуг. В этом заключается большая заслуга национального проекта «Цифровая экономика». Нацпроект способствует переводу госуслуг в онлайн, подключению социально значимых объектов с малочисленным населением к интернету, совершенствованию электронного документооборота и формированию безопасной информационной среды. 130 млн человек пользуются интернетом в России, а это практически 90% населения страны. Портал «Госуслуги» является фундаментом для цифрового взаимодействия граждан с госорганами.

Цифровизация госуслуг снижает нагрузку на офлайн-инфраструктуру ведомств, что экономит время и средства всем сторонам взаимодействия. Более 130 социально значимых услуг доступны онлайн на портале. Более 110 млн граждан России пользуются «Госуслугами». Ежедневно порталом пользуются более 10 млн человек. В среднем за месяц поступает 48 млн обращений[1].

МВД России являются участниками ведомственной программы цифровой трансформации по следующим направлениям:

– развитие и эксплуатация ведомственного сегмента системы «Мир»;

– развитие информационных структур и информационно-телекоммуникационной инфраструктуры Госавтоинспекции;

– строительство и оснащение системы федерального центра обработки данных МВД России;

– развитие и эксплуатация информационно-телекоммуникационной инфраструктуры МВД России.

Для автора статьи направление в части осуществления администрирования доходов бюджетов от оказания госуслуг (по направлениям деятельности Госавтоинспекции, миграции и др.) и организация финансового планирования в подразделениях МВД России с учетом цифровизации экономики является объектом профессионального интереса, что находит свое отражение в ряде работ, которые рассматривают данную проблематику в различных аспектах: сущности администрирования доходов бюджета органами внутренних дел [3]; формирования про-

[1] О направлении информационных материалов: письмо ГУРЛС МВД России от 20 февраля 2024 г. № 21/18/3435.

екта бюджета МВД России в ГИИС «Электронный бюджет» [2]; электронного бюджета в системе стратегического планирования и обеспечения экономической безопасности [4]. Также проанализированы научные публикации, касающиеся вопросов: национальных проектов [1], цифровизации в сфере управления общественными финансами [5] и др.

При этом в соответствии с бюджетным законодательством Российской Федерации подразделения системы МВД России обладают соответствующими бюджетными полномочиями и осуществляют:

– предоставление государственных услуг посредством федеральной государственной системы государственных услуг «Единый портал государственных и муниципальных услуг (функций)»[1] по линии работы подразделений системы МВД России: контроля за оборотом наркотиков, вопросам миграции, информационно-аналитического центра, Госавтоинспекции, экспертно-криминалистического центра (всего МВД России предоставлялось 35 видов государственных услуг; количество представленных в 2022 году составило 96,95 млн госуслуг[2]);

– финансовое планирование в государственной интегрированной информационной системе «Электронный бюджет» (далее – ГИИС «Электронный бюджет». МВД России (в лице ФЭД МВД России) и ряд департаментов Министерства (ДТ МВД России, ЦИТИЗИ ДТ МВД России и др.) являются при этом главными распорядителями средств бюджета (далее – ГРСБ), территориальные подразделения – распорядителями средств бюджета, районный уровень – получателями средств бюджета (далее – ПБС). При этом ГРБС и РБС в части осуществления бюджетных полномочий, касающихся финансового обеспечения непосредственно центральных аппаратов, являются одновременно и ПБС.

Поэтапный порядок составления бюджетных смет в территориальных подразделениях МВД России получателя бюджетных средств с указанием мероприятий, правового основания и исполнителя (соисполнителя) предложен в табл. 1.

[1] URL: https: //www.gosuslugi.ru (дата обращения: 21.02.2024).

[2] Официальный сайт МВД России. URL: мвд.рф (дата обращения: 21.02.2024).

Таблица 1

Поэтапный порядок составления бюджетных смет в ГИИС «Электронный бюджет» в территориальных подразделениях МВД России[1]

№ п\п	Наименование мероприятия в ГИИС «Электронный бюджет» (планирование) или иное/маршрут в информационном ресурсе	Основание (основной нормативный правовой акт)	Подразделение исполнитель (соисполнитель)
I. Подготовительный этап			
1.	Создание вариантов бюджетной сметы для подведомственных подразделений. Меню → Варианты проекта бюджетной сметы	Федеральный закон о федеральном бюджете на финансовый год и на плановый период; приказ МВД России от 29 августа 2019 г. № 588 (далее – приказ МВД России № 588)	Центр финансового обеспечения РБС
2.	Создание, согласование и утверждение проектов показателей бюджетных смет. Меню → Проекты показателей бюджетных смет		Бухгалтерия ПБС, тыловое подразделение ПБС
3.	Создание, согласование и утверждение проекта бюджетной сметы. Меню → Проекты бюджетных смет		Бухгалтерия ПБС, тыловое подразделение ПБС
4.	Согласование проекта бюджетной сметы с ГРБС (РБС). Меню → Проекты бюджетных смет → Согласование с ГРБС(РБС)		Центр финансового обеспечения РБС
5.	Создание, согласование, утверждение проектов планов-графиков закупок. Меню → Управление закупками → Планы-графики закупок → Планирование	Федеральный закон о федеральном бюджете на финансовый год и на плановый период; Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Федеральный закон № 44-ФЗ); приказ МВД России № 588	Тыловое подразделение ПБС

[1] Таблица составлена автором.

6.	Согласование проекта планов-графиков закупок с ГРБС (РБС). Меню → Управление закупками → Планы-графики закупок → Планирование → Согласование с ГРБС (РБС)	Федеральный закон о федеральном бюджете на финансовый год и на плановый период; Федеральный закон № 44-ФЗ; приказ МВД России № 588	Центр финансового обеспечения РБС
II. Основной этап			
1.	Доведение финансирования до подведомственных подразделений. Меню → Бюджетная смета → Документы ФК	приказ МВД России № 588	Центр финансового обеспечения РБС
2.	Создание, согласование и утверждение бюджетной сметы. Меню → Бюджетная смета → Показатели бюджетных смет		Бухгалтерия ПБС, тыловое подразделение ПБС
3.	Согласование бюджетной сметы с ГРБС (РБС). Меню → Бюджетная смета → Документы ПБС → Согласование с ГРБС(РБС)		Центр финансового обеспечения РБС
4.	Создание, согласование и утверждение изменения показателей бюджетной сметы. Меню → Бюджетная смета → Предложения по внесению изменений в сметный расчет		Бухгалтерия ПБС, тыловое подразделение ПБС
5.	Согласование предложений по внесению изменений в сметный расчет с ГРБС (РБС). Меню → Бюджетная смета → Документы ПБС → Согласование с ГРБС (РБС)		Центр финансового обеспечения РБС
6.	Создание, согласование, утверждение плана-графика закупок. Меню → Управление закупками → Планы-графики закупок→ Исполнение	Федеральный закон № 44-ФЗ	Тыловое подразделение ПБС
7.	Согласование плана-графика закупок с ГРБС (РБС). Меню → Управление закупками → Планы-графики закупок→ Исполнение → Согласование с ГРБС (РБС)		Центр финансового обеспечения РБС
8.	Отправка плана-графика закупок в ЛК ЕИС, утверждение, отправка для утверждения в УФК		Тыловое подразделение ПБС

III. Заключительный этап			
1.	Внесение изменений в бюджетную смету при доведении дополнительного финансировании. Создание, согласование и утверждение изменения показателей бюджетной сметы. Меню → Бюджетная смета → Предложения по внесению изменений в сметный расчет	приказ МВД России № 588	Бухгалтерия ПБС, тыловое подразделение ПБС
2.	Согласование предложений по внесению изменений в сметный расчет с ГРБС (РБС). Меню → Бюджетная смета → Документы ПБС → Согласование с ГРБС (РБС)		Центр финансового обеспечения РБС
3.	Исполнение сметы. Своевременное равномерное, эффективное, целевое освоение доведенных лимитов бюджетных обязательств.		Бухгалтерия ПБС, тыловое подразделение ПБС

Таким образом, финансовое планирование в подразделениях МВД России осуществляется в ГИИС «Электронный бюджет» в три этапа в разделе «Планирование».

Согласно анализу анкетирования специалистов финансовых подразделений МВД России территориального и районного уровней, проведенного в 2023 г.[1], выявлены проблемные вопросы и предложены следующие мероприятия по совершенствованию работы в ГИИС «Электронный бюджет» (табл. 2):

Таблица 2

Проблемные вопросы и мероприятия по совершенствованию работы в ГИИС «Электронный бюджет»в финансовых подразделениях МВД России[2]

№ п/п	Проблема	Мероприятие
Информационное обеспечение		
1.	Неустойчивая работа программного обеспечения ГИИС «Электронный бюджет», что повлекло нарушение сроков предоставления и утверждения ГРБС проектов бюджетной сметы	Техническое совершенствование программного обеспечения ГИИС «Электронный бюджет»,

[1] Проведенного в рамках обучения по дополнительной профессиональной программе повышения квалификации руководителей (заместителей руководителей) управлений (отделов) центров финансового обеспечения, финансово-экономических отделов территориальных органов МВД России на окружном, межрегиональном и региональном уровнях по теме «Организация финансово-экономической деятельности в органах внутренних дел Российской Федерации (с применением системы дистанционных образовательных технологий)».

[2] Анализ анкет специалистов финансовых подразделений составлен автором.

Кадровое обеспечение		
2.	Отсутствие обучающих семинаров, совещаний по наиболее важным направлениям работы, в том числе в онлайн-формате	Организация проведения ГРБС обучающих онлайн-семинаров, совещаний
3.	Допускаемые ошибки в указании НПА при подготовке показателей бюджетной сметы	Более детальное изучение НПА в рамках занятий по служебной подготовке
Организационно-правового характера		
4.	Отсутствие лимитов бюджетных обязательств (далее – ЛБО) для оплаты коммунальных услуг, что приводит к образованию просроченной кредиторской задолженности, а также расходам на оплату госпошлины и пени за просрочку платежей.	Перераспределение ЛБО, а также их доведение из резервного фонда.
5.	Сложно рассчитать бюджет на плановые годы, так как цены, существующие в текущем периоде, не актуальны в плановых годах, а применяемый коэффициент не всегда соответствует действительности.	Указывание запрашиваемой информации без учета цен.
6.	Невозможно заключать госконтракт в рамках ГОЗ (продукты или поставка товара на плановый период), так как есть риск банкротства поставщика или маленький объем.	Заключение государственных контрактов исключительно на текущий год.
7.	Организация взаимодействия между тыловым подразделением и бухгалтерией.	Изучение тыловыми подразделениями нормативно-правовых актов, регламентирующих финансово-хозяйственную деятельность подразделения, в том числе приказа МВД России №588, применения кодов бюджетной классификации, утв. актуальными приказами Минфина России.

Предложено условно систематизировать проблемные вопросы и мероприятия по направлениям деятельности: информационного обеспечения, кадрового обеспечения, организационно-правового характера.

Таким образом, резюмируя вышесказанное с учетом одной из целей, определенных в рамках ведомственной программы цифровой трансформации по повышению удовлетворенности граждан государственными услугами (в том числе цифровыми) и снижению издержек бизнеса при взаимодействии с государством, возрастает значение эффективности деятельности подразделений МВД России – главных администраторов (администраторов) доходов бюджетов (по линии Госавтоинспекции, по линии миграции и др.) как одних

из участников бюджетного процесса, пополняющих доходную часть государства при оказании государственных услуг.

Кроме того, подразделения системы МВД России обладают соответствующими бюджетными полномочиями в части осуществления финансового планирования и исполнения бюджета (доходной и расходной частей) с использованием современных цифровых технологий, что требует всестороннего усиления роли руководителей подразделений Министерства в части повышения эффективности указанного направления деятельности.

Список литературы:

1. *Артюхин Р. Е.* Национальные проекты – качественно новый уровень ответственности государства // Государственная служба. 2020. № 1 (123).
2. *Белова С. Н.* Актуальные вопросы формирования проекта федерального бюджета МВД России в ГИИС «Электронный бюджет» // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020.
3. *Белова С. Н.* Сущность понятия администрирования доходов бюджетов органами внутренних дел // Бизнес в законе. 2011. № 1.
4. *Белова С. Н, Владимирова О. Н., Гришмановский Д. Ю.* Электронный бюджет в системе стратегического планирования и обеспечения экономической безопасности // Экономическая безопасность. 2023. Т. 6. № 3.
5. *Глазунова О. В., Глазунова В. С.* Цифровизация в сфере управления общественными финансами // Вестник Волгоградского государственного университета. Экономика. 2020. № 1.

Виктория Александровна Бецкова
магистрант факультета
информационной безопасности
Московский государственный
лингвистический университет
E-mail: vikabeckova@mail.ru

УДК 004.01.07.3

Организация процессов и информатизация деятельности кадровых подразделений с применением АИС

Аннотация

Статья посвящена актуализации внедрения современных информационных технологий в деятельность социальных структур государственного сектора. Автор акцентирует внимание на деятельности кадровых подразделений, опираясь на эмпирический опыт МИД России. В статье обозначены повышенные разрешающие возможности информационных систем, обладающие возможностью обработки информации по прохождению службы. Должное внимание уделено обеспечению информационной безопасности при решении задач.

Ключевые слова и словосочетания: *информатизация; цифровизация; цифровая трансформация; информационные технологии; автоматизированные информационные системы; технологии искусственного интеллекта; динамика обращений граждан; электронный документооборот; информатизация деятельности кадровых подразделений; информационная безопасность.*

На сегодняшний день одним из самых актуальных направлений в развитии научно-технического прогресса является информатизация, цифровизация общества, а также цифровая трансформация, воздействующая на организационную структуру многих социальных систем. Информационные технологии (далее – ИТ) являются неотъемлемой частью при решении задач в госучреждениях Российской Федерации [2].

Так, именно развитие и интеграция ИТ становятся ключевым вектором развития деятельности кадровых подразделений. Автоматизированные информационные системы (далее – АИС) явля-

ются неотъемлемой частью в функционировании и поддержании работы государственных учреждений. Основными преимуществами использования рассматриваемых технологий являются:

– автоматизация рутинной деятельности;

– снижение вероятности ошибок за счет минимизации влияния человеческого фактора;

– сокращение времени выполнения отдельных задач за счет машинной обработки больших данных;

– расширение видов операций обработки документов на основе расширенных возможностей технологий искусственного интеллекта;

– возможность интеграции информационного пространства и автоматизированная подготовка проекта управленческого решения.

Примером, свидетельствующим о непрерывном росте и информатизации государственных учреждений, является статистическая информация (рис. 1). За последние года значительно увеличивается прием обращений от граждан через электронную почту на примере МИД России. Это связано с более высокой эффективностью и скоростью обработки заявок посредством специализированного ПО.

Рис. 1. Динамика количества обращений граждан в МИД России

Важной частью в функционировании государственных учреждений являются кадровые подразделения. Кадровые подразделения государственных учреждений занимаются управлением персоналом в этих учреждениях. Они отвечают за набор, оценку и развитие сотрудников, решение вопросов, связанных с оплатой труда и социальными льготами, а также за соблюдение трудового законодательства. Задачи кадровых подразделений государственных учреждений могут включать: разработку штатного расписания; определение численности и структуры персонала; проведение конкурсных отборов

на вакантные должности; разработку и внедрение политики в области защиты прав и интересов сотрудников; учет и управление кадровым потенциалом учреждения; проведение подготовки и повышения квалификации сотрудников и др.

Как видно, рассматриваемые подразделения выполняют целое множество сложных и рутинных задач, связанных с управлением персоналом. Из-за этого может наблюдаться наличие множества ошибок при выполнении задач, что связано с возможностью влияния человеческого фактора. Решение данной проблемы может быть достигнуто в результате интеграции АИС в деятельность кадровых подразделений. Примерами подобных решений являются VipNet, АСЭДО-МЭДО, АИС «СпринтСофт» и АИС «Отдел кадров».

АСЭДО-МЭДО – автоматизированная система электронного документооборота, которая используется в кадровых подразделениях государственных учреждений. Она позволяет эффективно управлять документами, обеспечивает их целостность и сохранность, а также повышает эффективность работы сотрудников. АИС «СпринтСофт» – АИС, которая используется в кадровых подразделениях государственных учреждений. Она позволяет управлять информацией о сотрудниках, их трудовых отношениях, расчетах заработной платы и других аспектах кадрового учета. АИС «Отдел кадров» – автоматизированная информационная система, используемая в кадровых подразделениях государственных учреждений. Она позволяет управлять всей информацией о сотрудниках, отслеживать изменения в их карьере, вести учет кадрового состава и обеспечивать своевременное выполнение кадровых процедур [3].

Каждая из данных систем может использоваться независимо друг от друга. При этом наиболее эффективным и включающим в себя большее число преимуществ и возможностей применительно к рассматриваемой задаче является АСЭДО-МЭДО. Доказательством этого является то, что данная автоматизированная система уже используется Администрацией Президента Российской Федерации, аппаратом Правительства Российской Федерации, федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации, а также иными государственными органами и государственными организациями. Однако важным вопросом остается защита информации и обеспечение информационной безопасности АИС. Для решения данных проблем актуально использование инструмента VipNet.

VipNet – система защиты информации, которая применяется в кадровых подразделениях государственных учреждений. Она представляет собой комплекс технических и программных средств,

который обеспечивает конфиденциальность, целостность и доступность информации при передаче и хранении. VipNet обладает высокой степенью защиты данных и основан на криптографических протоколах. Он шифрует информацию и обеспечивает ее безопасную передачу по каналам связи. Также VipNet имеет механизм контроля целостности данных, что позволяет обнаруживать любые попытки несанкционированного изменения информации.

VipNet используется для защиты персональных данных сотрудников, а также конфиденциальных документов и иных материалов, которыми занимается отдел кадров [1]. С помощью VipNet можно безопасно обмениваться информацией как внутри учреждения, так и с другими государственными организациями. Использование VipNet позволяет снизить риск утечки и несанкционированного доступа к данным. Это обеспечивает надежную защиту информации, сохранение ее целостности и конфиденциальности, а также соответствие требованиям законодательства в сфере защиты персональных данных.

Таким образом, в результате выполненной работы был актуализирован вопрос и подтверждена необходимость информатизации деятельности кадровых подразделений с применением АИС. Автором представлены примеры информационных инструментов, способных значительно повысить качество и эффективность выполняемых процессов, наиболее подходящим из которых была выбрана система АСЭДО-МЭДО. Отдельно был рассмотрен вопрос обеспечения защиты информации, с котором позволяет справиться интеграция инструмента VipNet.

Список литературы:

1. О персональных данных [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «Консультант-плюс».

2. Об информации, информационных технологиях и защите информации [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Об организации предоставления государственных и муниципальных услуг [Электронный ресурс]: Федер. закон от 27 июля 2010 г. № 210-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Данил Вячеславович Будко,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: danilbudko8@dbudko.ru

УДК 343.97

Искусственный интеллект как фактор криминологического риска

Аннотация

В данной работе обозначена важнейшая роль как в настоящем, так и в будущем технологий искусственного интеллекта как основного детерминанта развития общества. Представлены приоритетные направления в дальнейшем развитии искусственного интеллекта, а также определен широкий комплекс его перспективных возможностей. Но эти возможности, в свою очередь, обусловливают большие криминологические риски.

Актуальность статьи обоснована запросом от государства на разработку комплекса мер по минимизации негативных рисков развития и внедрения искусственного интеллекта. Главной формой реализации технологий искусственного интеллекта среди массового населения выступают искусственные нейронные сети. Такие особенности в их функционировании, как открытость, обусловливающая собой неограниченный доступ любому пользователю, автономность функционирования, простота в их использовании, не требующая специальных технических знаний, позволяет совершать преступную деятельность в области информационно-телекоммуникационных технологий на совершенно новом уровне.

В целях предупреждения негативного проявления возможностей технологий искусственного интеллекта, сведения к минимуму угрозы для граждан в данной сфере автором предлагается применить криминологический инструментарий, позволяющий комплексно рассмотреть детерминанты, обусловливающие криминогенные риски. Выделены и охарактеризованы основные направления научного исследования, представляющие собой различные уровни предупредительно-профилактической деятельности.

Ключевые слова и словосочетания: *искусственный интеллект; криминологический риск; искусственные нейронные сети; бесконтрольное развитие; меры криминологического предупреждения преступлений.*

Искусственный интеллект (далее – ИИ) – технология настоящего и будущего, основа развития общественных процессов в недалеком будущем. Многие научные деятели и мировые политики отзываются подобным образом о данных технологиях. Высказываются даже небезосновательные мнения о том, что уровень развития в области технологий может заменить показатели ВВП, ведь ИИ напрямую влияет на экономические возможности целых государств. Вследствие этого темпы развития данных технологий превышают все возможно представляемые ориентиры.

Ряд тезисов, подтверждающих его дальнейшее активное развитие и в частых случаях бесконтрольное внедрение, был обосновано представлен на VIII конференции по развитию ИИ АIJ «Путешествие в мир искусственного интеллекта» (далее-Конференция) [1]. Технологиям ИИ, как уже было отмечено выше, выделяют особое место среди информационных технологий, например, высказывается мнение, что следующая производственная революция 5.0 будет характеризоваться дальнейшими открытиями в области ИИ, и все «передовые» страны это безусловно признают. Человечество стоит на пороге эпохи, когда расширение горизонтов использования искусственного интеллекта развязывает новую промышленную революцию [4, с. 106].

Также на вышеупомянутой Конференции подчеркивалась его особая значимость и даже утверждалось, что ИИ послужит основным драйвером научного мира и будет лежать в основе других технических разработок. Данные технологии часто характеризуются как «сквозные» и обладают универсальностью, не привязанностью к одной из конкретной сфер и функционированием во всех областях человеческой жизнедеятельности.

Как отметил глава нашего государства В. В. Путин: «генеративный ИИ – это новая глава существования человечества, новый партнер для человека». Но Президентом Российской Федерации также были затронуты острые вопросы, касающиеся опасности его дальнейшего бесконтрольного развития, а именно определены дальнейшие важнейшие направления в его развитии с целью минимизации рисков его незаконного проявления. Президентом Российской Федерации было отмечено, что необходимо определить границы развития ИИ; разработать соответствующие этические, социальные и нравственные нормы при его использовании; обеспечить безопасность и разумность при его дальнейшем развитии; необходимо свести к минимуму угрозы для граждан.

Закрывать глаза на проблему рисков неразумно. В первую очередь это может сказаться (и сказывается!) на качестве решения

задач предупреждения преступлений: картина криминальной детерминации оказывается неполной, ее оценка неточной, и, следовательно, профилактическая система лишается некоторых важных предпосылок повышения эффективности своих практических усилий. Не говоря уже о том, что риски, не взятые под контроль, оставленные на свободе, быстро разрастаются и превращаются в масштабные угрозы безопасности граждан, общества, государства [3]. При этом, по мнению А.В. Аносова, нейтрализация цифровых детерминант преступности возможна путем создания соответствующих условий реализации заложенных в них преимуществ [2].

Впервые этический вопрос и попытку урегулировать отношения между человеком и робототехникой предложил Айзек Азимов, описав в рассказе «Runaround», вышедшем в свет в 1942 г. В нем содержались три правила по нивелированию возможных конфликтов, вызываемых развитием цифровых отношений, а именно: 1) искусственно созданный робот не может причинить вред человеку ни действием, ни бездействием; 2) робот должен подчиняться человеку (если это не противоречит первому правилу); 3) он не может причинить вред самому себе (если это не противоречит предыдущим правилам).

При всех его возможных положительных аспектах научное сообщество и передовые государства единодушно приходят к общему консенсусу и признают, что дальнейшее бесконтрольное развитие ИИ пророчит большие криминогенные риски. Как отметил Президент Российской Федерации: «Будущее не за запретами!», что позволяет сделать вывод о необходимости рационального, поэтапного выстраивания системы внедрения ИИ и разумного оценивания рисков его развития с целью минимизации опасности для граждан.

В частности, разработкой Концепции по безопасному интегрированию технологий ИИ, их оптимизации и повышению эффективности в оперативно-служебных подразделениях МВД России занимается коллектив Академии управления МВД России, разрабатывая концептуальные основы по его рациональному применению [5].

Понятийный аппарат и общие признаки технологии ИИ весьма подробно раскрываются в Указе Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», который утверждает Национальную стратегию развития искусственного интеллекта на период до 2030 г. (далее – Национальная стратегия)[1].

[1] Национальная стратегия развития искусственного интеллекта на период до 2030 года [Электронный ресурс]: утверждена указом Президента Рос. Федерации

Искусственный интеллект – это комплекс технологических решений который включает в себя: информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе использующее методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Технологии ИИ раскрываются посредствам следующего аппаратно-программного комплекса: компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальная поддержка принятия решений и перспективные методы искусственного интеллекта.

ИИ обладает специфическими характеристиками в сравнении с иными цифровыми продуктами, а именно: позволяет имитировать когнитивные функции человека (большие языковые модели – генеративные искусственные нейросети); при выполнении конкретных задач результаты сопоставимы, как минимум, с результатами интеллектуальной деятельности человека.

Основной формой реализации технологий ИИ выступают большие языковые генеративные модели – искусственные нейронные сети (далее – ИНС). Именно их архитектурный тип взят за основу построения так называемых чат-ботов.

Данная технология конструктивно представлена в виде входного (первичной обработки запроса пользователя) и выходного слоя (собирательного элемента, отражающего общий результат), промежуток между которыми сформирован различным множеством искусственных нейронов и связей между ними. Сам генеративный цифровой процесс выработки конечного результата выглядит следующим образом: отправляется запрос пользователя в чат, в дальнейшем информация обрабатывается входным слоем и проходит через все промежуточные слои (искусственные нейроны), выдавая результат посредством выходного слоя. Одной из основных проблем вследствие получаемых результатов на выходе именуется «проблема черного ящика». Характеризуется она тем, что на данный момент никто из разработчиков не может дать четкого ответа и описать процесс выработки финального решения, что порождает довольно-таки часто непредвиденные результаты, носящие в себе порою «негативные» подтексты.

Примером может послужить функционирование ИИ на основе ИНС, создающей новостные заголовки по запросам пользователя. Отсутствие критериев ценза привело к тому, что любой желающий

от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «Консультант-Плюс».

мог создать новостную повестку, носящую в себе явно экстремистский подтекст [6].

Данная техническая уязвимость также представляет собой прямую опасность для жизни и здоровья человека. В мире уже зафиксирован случай доведения лица до самоубийства вследствие контакта с ИНС, выступавшей в роли психотерапевта [8].

В силу своей публичности и общедоступности ИНС используются в совершенно разных целях человеческого промысла. Также данные технологи не обошли и криминальный мир, были им приняты и используются в своих интересах.

В настоящее время в мировой практике зарегистрированы случаи использования открытых (категория «открытости» раскрывается посредством их общедоступности и безграничного использования) ИНС для совершения таких противоправных деяний, как мошенничество; компрометация или вымогательство путем замены ИНС человеческого лица на цифровом изображении или синтеза голоса; разработка вредоносных компьютерных программ; доведение до самоубийства человека вследствие контакта с ИНС, выступавшей в роли психотерапевта; разработка и массовое применение новых методов социальной инженерии с целью получения пользовательских паролей и иных личных данных и др.

Одним из первых преступлений, совершенных с помощью технологий ИИ, а именно ИНС DeepFake, в 2019 г. стало хищение крупной денежной суммы. Мошенники применили метод синтеза и генерации голоса директора банковской компании, тем самым создав убедительную звуковую модель копии голоса. Представившись директором данной компании, мошенники дали поручения перевести определенную сумму денег на банковский счет в течение часа, что не вызвало подозрений у сотрудников, так как голос был идентичен оригиналу его носителя.

Ключевыми особенностями открытых ИНС, создающих криминологическую угрозу, являются следующие характеристики: общедоступность их использования, приводящая к бесконтрольному и неограниченному доступу любого желающего для реализации своих целей; способность автономного функционирования без участия лица, осуществляющего постоянный контроль и мониторинг за их действиями; возможность прямого воздействия через сеть Интернет на различные ресурсы, в том числе критически важные объекты инфраструктуры по запросу пользователя; отсутствие индикаторов, свидетельствующих об использовании ИНС в межсетевом обмене или применении результатов деятельности ИИ в криминальных целях; возможность обойти установленные ограничения путем гра-

мотного составления цепочки запросов и возможности переубедить ИИ в полезности достигаемых целей.

Хотелось бы выделить одну из важнейших мыслей: не сами технологии ИИ как таковые представляют опасность, а именно человеческое проявление посредством данных высоких мультипликативных технологий выражает главные криминологические риски. Ни одно из технических изобретений не может причинить вред обществу, если не поступит соответствующий запрос от пользователя.

Внедряя новую технологию, необходимо определять новый класс ответственности и прогнозировать возможные риски, возникающие с ее развитием. Аналогию можно привести с таким витком технического прогресса, как внедрение «BigData», а именно новое цифровое направление в техническом развитии, способствующее появлению новых методов обработки информации колоссальных объемов, удешевлению хранения данных, а также возникающих в связи с этим больших рисков их утечки, что создало потребность в нормативно-правовом регулировании данной сферы и выразилось в принятии Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] и урегулировании данной сферы главой 28 Уголовного Кодекса Российской Федерации.

Что же касается ИИ, то на данный момент не существует нормативных актов, регулирующих данную сферу отношений. На законодательном уровне закреплены документы лишь общего характера, ориентирующие дальнейшее общее стратегическое направление развитие технологий ИИ.

Так, с целью сведения к минимизации рисков для граждан и необходимости установления дальнейших перспектив развития ИИ, выдвигая во главу угла принцип безопасности, закрепленный п. 19, и учитывая п. 51 Национальной стратегии, а также используя криминологический инструментарий по предупреждению преступлений, предлагаются следующие направления научной разработки.

В рамках общесоциального уровня предупреждения преступности предполагается дальнейшее усовершенствование положений «Кодекса этики в сфере ИИ» и закрепление в нем следующих приоритетных направлений: данный документ является общеобя-

[1] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «Консультант-Плюс».

зательным для ознакомления и точного соблюдения всеми разработчиками технологии ИИ; перед использованием технологий ИИ обычным пользователям необходимо обязательное ознакомление с положениями «Кодекса этики в сфере ИИ» и их принятие, при этом возлагая на себя ответственность в случае нарушения положений, закрепленных в нем [7]. В силу этого необходимо разработать комплекс санкционных мер в случае использования технологий ИИ против человека, т. е. действий, направленных на причинение какого-либо вреда.

В рамках специально-криминологического предупреждение необходимо:

– разработать маркировку продукции, получаемой в результате использования ИИ, с целью ее отличия от иной информации, генерируемой в цифровом пространстве;

– формирование специального реестра ИНС и регистрация всех пользователей с целью их учета;

– выявление подозрительных запросов (экстремистского, националистического, дискредитирующего и т. п. характера) и попыток обойти цензурный барьер, запрещающих подобные запросы, и своевременное направление цифровых данных о пользователе, запрашивающем подобную информацию, в соответствующие правоохранительные органы;

– разработка отдельных индикаторов применения ИНС в механизме совершения преступления с целью систематизации знаний и разработки методологических основ по выявлению и предупреждению преступлений, в которых технологии ИИ использовались как средство или орудие совершения преступного деяния.

Виктимологическую профилактику осуществлять по следующим направлениям:

– информирование физических и юридических лиц, государственных органов, в частности сотрудников правоохранительных органов, о новых методах и способах совершения преступлений, в которых были использованы технологий ИИ;

– своевременное выявления новых методов социальной инженерии и доведение до граждан способов противодействия им.

Подводя итог вышеизложенному, необходимо признать, что технологии ИИ являются нашим неотъемлемым будущим. Но в силу их быстрого развития и бесконтрольного внедрения, детерминирующее собой большие криминологические риски, возникают различного рода опасности для окружающих. Дальнейшее прогнозирование и контроль со стороны государственных органов позволит наиболее безопасно и рационально осуществлять процесс их использования и интеграции.

Особая роль отводится комплексной разработке методологической основы по минимизации рисков со стороны негативного проявления ИИ, позволяющей без ущерба для страны, подойти к разработке мер по предупреждению преступлений, совершаемых с помощью ИИ. Она предполагает не наличие каких-либо жестких запретов, а гибкий инструментарий криминологических мер, позволяющих выявить причины и условия возникновения криминогенных рисков и эффективным образом оказать на них своевременное воздействие, с целью недопущения их возрастания и нейтрализации детерминирующих факторов, оказывающих разрушающее воздействие.

Список литературы:

1. AI Journey 2023. Международная конференция Сбера по искусственному интеллекту. URL: https:// aij.ru/?yscklid=ls3jvl458p761321830 (дата обращения: 20.01.2024).

2. *Аносов А. В.* Цифровые детерминанты коррупционной преступности // Труды Академии управления МВД России. 2023. № 1 (65).

3. *Бабаев М. М., Пудовочкин Ю. Е.* Феномен риска в контексте профилактической политики (криминальная рискология) // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10. № 1.

4. *Бегишев И. Р.* Уголовно-правовая охрана общественных отношений, связанных с робототехникой: дисс. на соискание ученой степени д-ра юрид. наук: специальность 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Казань, 2022.

5. *Бецков А. В., Лукашов Н. В.* О разработке проекта концепции использования технологий искусственного интеллекта в системе МВД России // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020.

6. *Калашников Н. А., Козлова О. Е.* Анализ и выявление экстремистских рисков в работе нейросетей // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции / под ред. И. Р. Бегишева [и др.]. Казань: Познание, 2022.

7. Кодекс этики в сфере ИИ. URL: https://ethics.a-ai.ru (дата обращения: 22.01.2024).

8. СМИ: бельгиец покончил с собой после общения с искусственным интеллектом. URL: https://ria.ru/20230329/ii1861467723.html?ysclid=lsxkz96hjy329716266 (дата обращения: 01.02.2024).

Андрей Игоревич Власов,
кандидат технических наук, доцент,
заместитель заведующего кафедрой
по научной работе ИУ-4
«Проектирование и технология производства
электронной аппаратуры»
МГТУ имени Н. Э. Баумана

Тимур Маратович Фатхутдинов,
студент кафедры ИУ-4
«Проектирование и технология производства
электронной аппаратуры»
МГТУ имени Н. Э. Баумана

УДК: 159.93

Проблемы автоматического распознавания эмоций в рамках предиктивной аналитики психоэмоционального состояния непрерывного потока людей

Аннотация

С каждым днем увеличивается количество средств видеофиксации в помещениях и окружающем пространстве. Применение камер видеофиксации призвано снизить возможные противоправные проявления непосредственно своим наличием, а также предоставлять возможность оператору (системе) предиктивный анализ событий. В случае, если противоправное действие произошло, то средства видеофиксации являются эффективным инструментом для осуществления оперативно-розыскной деятельности.

Ключевые слова и словосочетания: *аппаратно-программные комплексы; идентификация эмоций; когнитивные искажения; нейронные сверточные сети.*

Одним из перспективных направлений предиктивной аналитики поведенческих аспектов потока людей или отдельных индивидуумов в потоке является распознавание эмоционального состояния человека с использованием аппаратно-программных комплексов (АПК), использующих алгоритмы машинного обучения [3; 10]. В типовой АПК автоматической идентификации лиц целесообразно интегрировать предиктивную аналитическую систему определения психоэмоционального

состояния объекта и/или потока людей с возможностью регистрации и предсказания событий с учетом модели «эффекта толпы» (психологии толпы) (стихийная толпа, ведомая толпа, организованная толпа, агрессивная толпа, паническая толпа, стяжающая толпа и т. п.) [6; 8–9].

В АПК эмоционального детектирования в качестве идентифицирующих объектов для установления эмоционального состояния объекта используются методы фрагментации видеопотока с выделением фигуры человека, черт лица и т. п. Среди разнообразия возможностей по выделению из видеопотока образов отдельных личностей наиболее привлекательным объектом является изображение лица, которое можно фиксировать с помощью камеры видеофиксации без каких-либо дооснащения их специализированными средствами. Однако во времена глобальной пандемии, когда ношение маски, закрывающей рот и нос, широко поощряется обществом, а в некоторых случаях даже предписано законодательством, распознавание эмоционального состояния может быть затруднено [5]. К тому же личности, представляющие оперативный интерес, могут целенаправленно скрывать свои лица медицинскими масками и другими специальными средствами. Кроме этого, идентификация эмоций может быть ограничена фактором проявления индивидуумом когнитивных искажений, когда ожидаемая реакция на внешнее эмоциональное или психофизическое воздействие не соответствует реакции индивидуума [2; 4].

Идентификация эмоций на фоне когнитивных искажений является одной из значимых проблем автоматического детектирования эмоций по лицу [4]: оценка адекватности мимической реакции (эмоции) на внешнее возмущающее воздействие (рис. 1). При этом наличие когнитивного искажения определяется не группой выявленных эмоций, а несоответствием мимической реакции внешним (побуждающим) условиям.

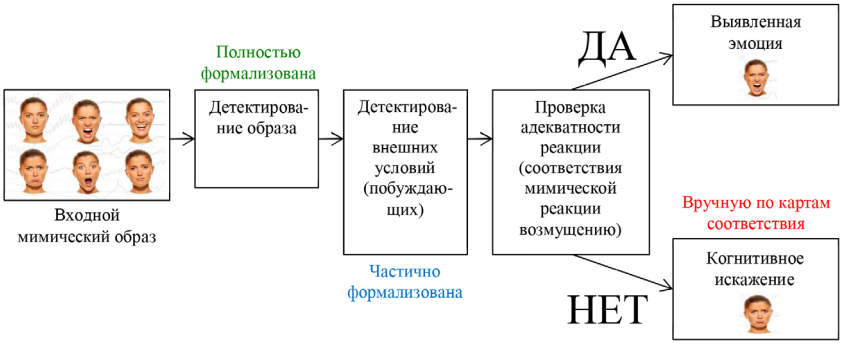

Рис. 1. Проблема детектирования эмоций на фоне когнитивных искажений

Когнитивные искажения напрямую соотносятся с эмоциональными состояниями, которые детектируются посредством предобученной модели, поэтому по точности детектирования эмоционального состояния можно судить о точности детектирования когнитивного искажения. Для оценки качества дискретных результатов модели в качестве метрики целесообразно использовать MAP критерий (Mean Average Precision).

MAP – среднее значение метрики оценки точности детекторов объектов. MAP включает в себя компромисс между точностью и откликом и учитывает как ложные срабатывания (FP), так и ложные отрицания (FN). Это свойство делает MAP подходящей метрикой для большинства приложений детектирования. Однако эти метрики по отдельности не могут являться полностью достоверными. Например, когда модель имеет высокий отклик, но низкую точность, модель правильно классифицирует большинство положительных образцов, но имеет много ложных срабатываний (т. е. классифицирует многие отрицательные образцы как положительные), или же, когда модель имеет высокую точность, но низкий отклик, то модель является точной, когда она классифицирует образ как положительный, но она может классифицировать только некоторые из положительных образцов. MAP зарекомендовала себя как эталонная метрика, используемая в области компьютерного зрения для оценки надежности моделей обнаружения объектов. Средняя точность реализует компромисс между точностью и откликом и максимизирует эффект обеих метрик оценки.Предлагаемое решение оценки эмоционального состояния с учетом возможных когнитивных искажений позволяет провести анализ состояния объекта исследования и сформировать комплексную оценку. Это актуально для оценки психоэмоционального состояния как отдельного индивидуума, так и группы людей, в том числе и «толпы». Также это актуально для управлениями переговорами в различных сферах деятельности людей, для операторов технических систем, военных, спортсменов, кадровых служб и служб безопасности.

В данной работе основное внимание уделено проблемам по выявлению эмоционального состояния человека в условиях недостаточного изображения лица путем ограничения размеченного набора данных посредством нейронных сверточных сетей [1].

В случае наличия лицевой маски она фактически скрывает область рта и носа (нижнюю треть головы), которые имеют базовое значение в распознавании эмоций по лицу. Это затрудняет интерпретацию эмоциональных проявлений. Исследования показывают,

что лицевые маски оказывают сильное негативное влияние на распознавание эмоций [5; 7].

Для уменьшения негативного влияния в первую очередь возможно упростить задачу путем объединения нескольких схожих эмоций и получить пять категорий: «Гнев – Отвращение», «Страх – Удивление», «Счастье», «Печаль» и «Нейтральность», а также в исключении эмоцию «Презрение» из общего перечня [3]. Переклассификация оправдана сходством некоторых особенностей верхней части лица в выражениях лица, связанных с чувствами «Гнева – Отвращения» и «Страха – Сюрприза». В частности, в случае гнева и отвращения брови опускаются вниз, а в случае страха и удивления брови поднимаются вверх. Исключение категории презрения оправдано двумя причинами: первая – это не ключевая эмоция в общении; вторая – это эмоция, в которой выразительность сосредоточена в области рта и поэтому не обнаруживается, если на лице субъекта надета маска. Этот процесс объединения также приносит пользу с точки зрения частичной балансировки набора данных [7]. Поскольку конкретная задача, поставленная в данной работе, заключается в определении эмоций в присутствии маски на лице.

Далее необходимо воссоздать подходящий набор данных, в котором ограничен рот. Сделать это можно несколькими способами. В первом способе накладывается маска к каждому изображенному субъекту, во втором случае оставляем только те части лица, по которым возможно определить эмоции [7].

Предложенный подход, основанный на обучении глубоких нейронных сетей [3; 4] для детектирования эмоций с учетом возможных когнитивных искажений и в условиях ограниченного набора признаков (состоящего из восьми эмоций: счастья, отвращения, гнева, страха, удивления, печали, презрения, нейтральности), позволяет устойчиво классифицировать пять основных классов эмоций (гнев – отвращение, страх – удивление, счастье, печаль, нейтральность).

Список литературы:

1. *Аверьянихин А. Е., Власов А. И., Евдокимова Е. В.* Иерархическая пирамидальная субдискретизация в глубоких сверточных сетях для распознавания визуальных образов // Нейрокомпьютеры: разработка, применение. 2021. Т. 23. № 1.

2. *Власов А.И., Конькова А.Ф.* Медико-диагностические экспертные системы для оценки адекватности адаптивной реакции

организма на воздействие экстремальных факторов // Конверсия. 1995. № 9–10.

3. *Власов А. И., Ларионов И. Т., Орехов А. Н., Тетик Л. В.* Система автоматического распознавания эмоционального состояния человека // Нейрокомпьютеры: разработка, применение. 2021. Т. 23. № 5.

4. *Кожаринов А.С. [и др.].* Методы анализа когнитивных искажений и концепция автоматизированной интеллектуальной системы их детектирования // Нейрокомпьютеры: разработка, применение. 2022. Т. 24. № 4.

5. *Косулин К. Э., Карпов А. А.* Методы аудиовизуального распознавания людей в масках // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22. № 3.

6. *Крысько В. Г.* Социальная психология: Схемы и комментарии. Москва: ВЛАДОС-ПРЕСС, 2001.

7. *Кухарев Г. А., Рюмина Е. В., Шульгин Н. А.* Метод генерации масок на изображениях лиц и системы их распознавания // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22. № 3.

8. *Подлиняев О. Л., Каримов А. А.* Психологические особенности поведения людей в толпе и их учет сотрудниками право охранительных органов при проведении массовых мероприятий // Психопедагогика в правоохранительных органах. 2018. № 3 (74).

9. *Подлиняев О. Л.* Психология толпы и специфика ее разновидностей // Вестник Восточно-Сибирского института МВД России. 2017. № 2 (81).

10. *Старков И. И., Власов А. И.* Применение методов машинного обучения в системах выявления плагиата с целью решения проблемы узкоспециализированных понятий // Нейрокомпьютеры: разработка, применение. 2022. Т. 24. № 6.

Дмитрий Владимирович Голиков,
старший преподаватель кафедры
информационных технологий
Академия управления МВД России
E-mail: dgolikov17@mvd.ru

УДК: 623.746.-519

Возможности комплекса беспилотной авиационной системы подъема аппаратуры в рамках деятельности органов внутренних дел

Аннотация

В данной статье рассматривается актуальность применения нового направления развития беспилотных летательных аппаратов – комплексов беспилотной авиационной системы подъема аппаратуры или как их называют иначе – привязные дроны. Рассматриваются как плюсы, так и минусы данной системы в целом. Определяется актуальность данной технологии в рамках использования в подразделениях МВД России для эффективного выполнения функций и задачи по охране общественного порядка и обеспечению общественной безопасности.

Ключевые слова и словосочетания: *беспилотные летательные аппараты; правоохранительные органы; комплексы беспилотной авиационной системы подъема аппаратуры; инновационные технологии; охрана общественного порядка; обеспечение общественной безопасности; оперативно-розыскная деятельность.*

В настоящее время наметилась стойкая тенденция использования беспилотных летательных аппаратов (БПЛА) во многих сферах современного общества: от безобидной развлекательной игрушки до смертоносного оружия.

Не стали исключением из этого процесса и правоохранительный органы. Ведь одним из принципов работы полиции в Российской Федерации, декларируемых в Главе 2 ст. 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» является использование достижений науки и техники, современных технологий

инновационных и информационных систем[1]. И это, несомненно, верный путь, ведь совершенно очевидно, что повышение эффективности работы правоохранительных органов в настоящее время всецело зависит от использования новейших современных технологий, которые способны оказать неоценимую помощь в деятельности правоохранителей как по обеспечению общественного порядка и профилактики правонарушений, так и непосредственно в борьбе с преступностью.

В целом в ряде подразделений МВД России беспилотные летательные аппараты различного типа используются уже более десяти лет. Применение беспилотных летательных средств в работе правоохранительных органов до недавнего времени рекомендовано при выполнении задач, при которых не требуется транспортирование людей и грузов, а также в случаях проведения оперативно-розыскных операций и спецопераций. Исходя из этого, можно определить свод задач, решаемых в интересах органов внутренних дел, которые можно возложить на системы и комплексы с БПЛА с учетом перспектив их развития [2].

Однако в последнее время запросы на использование БПЛА при охране общественного порядка значительно возрастают. Соответственно, будет расти и требование к количеству операторов данных устройств. И тут возникает еще одна проблема: качество подготовки пилотов БПЛА. Зачастую аварии БПЛА происходят из-за технических или человеческих ошибок. Не должным образом подготовленный сотрудник может одним неаккуратным движением руки превратить дорогостоящую технику в кучу бесполезных обломков. Однако во многих случаях во время охраны общественного порядка нет необходимости выполнять маневрирование беспилотными аппаратами, например, съемку с воздуха общественного мероприятия с массовым скоплением граждан. В таких случаях вполне возможно использовать так называемые «привязные дорны», или как еще их называют **комплексы беспилотной авиационной системы подъема аппаратуры.** Привязные дроны значительно сокращают количество аварий в полете, так как их перемещение ограничено и вероятность столкновения с другими пользователями воздушного пространства минимальна.

Привязной БПЛА имеет небольшую зону действия, в которой он может летать. Из-за ограничений полета, создаваемых кабелем питания, меньшего контроля над БПЛА для их работы не требуется

[1] О полиции: Федер. закон от 7 февраля 2011 г. № 3-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_110165 (дата обращения: 28.01.2024).

обученный пилот. Также существуют модели, не требующие GPS-навигации, что значительно снижает количество технических ошибок, которые приводят к сбоям БПЛА [3].

Также к преимуществам такого подхода можно отнести вертикальный взлет и посадку, которые не требуют взлетно-посадочной полосы или каких-то ухищрений типа пусковой установки или захвата при посадке. В отличие от привязного же аэростата или воздушного змея, мультикоптер устойчив в воздухе даже в условиях свежего или крепкого, порывистого и меняющегося по направлению ветра.

Вместе с этим появляется возможность исключить самую тяжелую его часть – полноразмерную батарею питания, ограничившись небольшой «аварийной» батареей, необходимой для экстренной посадки при обрыве кабеля управления. Вместо батареи, правда, появляется кабель питания, который нагружает беспилотник, существенно ограничивая возможности его перемещения, однако в результате все равно получается подъем какого-либо дополнительного полезного груза (например, камеры с оптикой, имеющей лучшие характеристики) по сравнению с точно таким же свободнолетающим БПЛА.

Вместе с этим привязной БПЛА подключается к наземному терминалу с источником питания и получает энергию от мощного аккумулятора, который слишком тяжел для беспилотного средства. Такой беспилотник, как правило, не летает куда-либо, а остается над точкой, где находится его провод питания и управления.

Зато у нас появляется продолжительность полета – вот, где они преуспевают. Привязные дроны имеют более продолжительное время полета по сравнению со свободно летающими дронами с аккумуляторами различных типов. Среднее время полета беспилотных летательных аппаратов на одной полной зарядке составляет 20–40 мин. Большинство же привязных дронов имеют неограниченное время полета и могут оставаться в воздухе до тех пор, пока не возникнет проблема с каким-либо из агрегатов, например, отказ двигателя или пропеллера.

Еще одним преимущество привязанных дронов – изображение без помех, так как видеосвязь может передаваться по кабелю. По этой же причине система не подвержена действию системы радиоэлектронной борьбы, что может быть весьма немаловажно для силовых структур.

Как ранее уже отмечалось, свободно летающие БПЛА требуют большого мастерства и многих часов практики для эффективной работы. Здесь же из-за ограниченного движения привязного дрона

оператору нужны только начальные навыки пилотирования, и он может в основном сосредоточиться на своих задачах, не отвлекаясь на управление [1].

Теперь затронем возможность применение дронов привязного типа. Такие системы отлично подходят для ситуаций, когда летать на большие расстояния не нужно, а достаточно оставаться на месте в состоянии зависания и работать над точкой, где расположен блок питания. Привязные БПЛА мобильны, быстро развертываются на местности и эффективно решают широкий спектр задач. Например, при наличии таких аппаратов упрощается:

– видеонаблюдение с использованием бортовых камер;
– работа пунктов охраны;
– организация сотового покрытия;
– создание систем связи в сложных условиях и чрезвычайных ситуациях;
– обеспечение телетрансляции;
– создание локальных навигационных сетей;
– эффективное обследование объектов и территорий.

Чем же могут быть полезны данные системы в деятельности подразделений МВД России? Самое очевидное применение – это использование в качестве подъемной платформы для видеоаппаратуры с учетом того, что установленная камера может работать в оптическом и в инфракрасном диапазоне и обладать способностью снимать с хорошей разрешающей способностью. В данном виде привязной БПЛА вполне может быть использован для наблюдения и фиксации происходящего на массовых мероприятиях как санкционированных, так и стихийных незапланированных. Мобильная установка (например, в виде автотранспорта) с БПЛА оперативно может быть направлена в заданную точку, где будет находиться за оцеплением и снимать происходящее с защищенной территории неограниченное количество времени. При необходимости возможно оперативное перемещение установки. Если же во время применения возникнут какие-то технические неполадки или произойдет ошибка в пилотировании, то будет исключена возможность падения БПЛА на граждан.

Те же самые функции возможно выполнять во время стихийных бедствий или техногенных катастроф.

Еще одно применение системы можно найти в сфере телекоммуникаций. Привязной БМЛА может выполнять функции быстро разворачиваемой подъемной антенны вместо, например, мобильной телескопической вышки с установленным на ней ретранслятором или базовой станцией сотовой связи, которая позволит сотрудникам

правоохранительных органов вести сеанс связи даже в ситуациях, когда с поверхности земли этого сделать не получается по каким-то причинам (кроме того, не везде физически возможно поставить данную вышку, потому что, как правило, устанавливают ее на большегрузных автомобилях). Благодаря этому способоу возможно обеспечить сотовое покрытие там, где сеть сотовой связи полностью вышла из строя из-за стихийного бедствия или техногенной катастрофы или данной сети попросту нет, как это бывает на отдаленных территориях, где, например, идет поиск пропавшего человека или скрывающихся преступников.

Вполне возможна перспектива использования небольших привязных БПЛА обычным нарядом полиции, ведь для этого нужны лишь начальные навыки работы с беспилотником. Практически уже будет вполне возможно оперативно посмотреть со стороны улицы в квартиру на высоких этажах через окна, если входную дверь невозможно быстро открыть и нет понимания, что происходит внутри. При этом сотрудникам полиции не нужно лазить по балконам на высоких этажах или вызывать автовышку. Такие возможности будут далеко не лишние в практическом плане: автору за время службы приходилось иметь дело с подобными происшествиями.

В целом можно отметить, что данное направление развития беспилотных летательных аппаратов будет безусловно полезно для практической деятельности органов внутренних дел и несомненно займет достойное место в арсенале технических средств.

Список литературы:

1. Беспилотная авиационная система. Справочник по терминологии в оборонной сфере. URL: https://dictionary.mil.ru/dictionary (дата обращения: 08.01.2024).

2. Беспилотники для правоохранительных органов. URL: https://aeromotus.ru/dji-drone-for-law-enforcement/ (дата обращения: 28.01.2024).

3. *Каштанов В. В., Немтинов В. А.* Анализ организации связи с применением беспилотных летательных аппаратов малой дальности. URL: http://vestnik.tstu.ru/rus/t_28/pdf/28_4_008.pdf (дата обращения: 28.01.2024).

Андрей Александрович Долгов,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: andaleks78@mail.ru

УДК. 005.2

Методика моделирования и формирования организационно-управленческого механизма учета рисков при решении задач ресурсного обеспечения

Аннотация

Предложена новая методика управления рисками при решении задач ресурсного обеспечения, которая объединяет математическое моделирование с организационно-управленческими механизмами. Использован поэтапный подход, включающий идентификацию рисков, математическое моделирование, разработку стратегий управления рисками и реализацию организационно-управленческого механизма. Предложена новая методика, которая позволяет более точно предсказывать потенциальные риски и более эффективно разрабатывать стратегии для их смягчения. Продемонстрировано применение методики в различных отраслях, таких как производство, финансы и ресурсное обеспечение силовых структур.

Новая методика успешно достигает своих целей и предлагает значительные улучшения по сравнению с традиционными подходами. Однако ее эффективность может быть ограничена факторами, такими как доступность данных и вычислительные возможности. Дополнительное исследование может помочь определить способы преодоления этих ограничений.

Ключевые слова и словосочетания: *методика управления; риск; ресурсное обеспечение; оценка; эффективность; управление рисками; механизм управления; моделирование.*

Важными аспектами в области управления проектами и операциями при решении задач ресурсного обеспечения являются исследования математических моделей и формирование организационно-управленческого механизма учета рисков. Такие методики находят применение в различных отраслях, включая производство, финансы, логистику и другие направления.

Целью данной работы является разработка новой методики, которая позволит более эффективно управлять рисками при решении задач ресурсного обеспечения. Задачи включают в себя идентификацию потенциальных рисков, разработку стратегий для их смягчения и определение подходящих мер ответа.

Существует множество методик управления рисками, включая квалификационный и количественный анализ риска, а также различные подходы к моделированию риска. Однако эти методики часто ограничены своей способностью учитывать сложные взаимосвязи между различными видами рисков [6].

Исследование математических моделей и формирование организационно-управленческого механизма учета рисков при решении задач ресурсного обеспечения — это сложная и многогранная задача. Она включает в себя несколько ключевых аспектов (рис. 1).

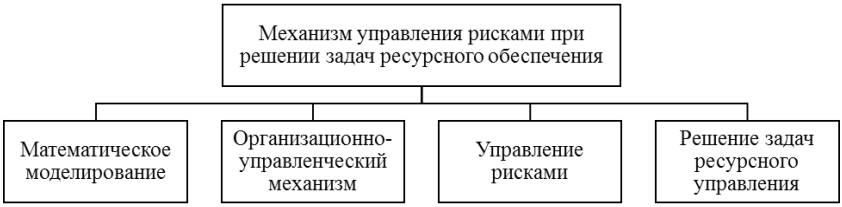

Рис. 1. Аспекты механизма управления рисками

1. Математическое моделирование. Это процесс использования математических структур и концепций для представления и анализа реальных систем. Математические модели могут быть использованы для предсказания поведения системы в различных условиях, что может быть особенно полезно при управлении рисками, особенно при прогнозировании.

2. Организационно-управленческий механизм. Данная структура или система определяет, как будут приниматься решения, кто будет принимать эти решения и как они будут реализованы. В контексте управления рисками она может включать процедуры оценки риска, стратегии смягчения риска и планы ответа на инциденты [5].

3. Управление рисками. Представляется как процесс идентификации, оценки и контроля рисков, которые могут повлиять на достижение целей, что в контексте ресурсного обеспечения может включать риски, связанные с доступностью и стоимостью ресурсов, а также с возможными препятствиями для их использования.

4. Решение задач ресурсного обеспечения. Здесь необходимо рассматривать процесс определения того, какие ресурсы необходимы для достижения определенных целей, а также планирования и координации их приобретения, доставки и использования [1].

Все эти аспекты тесно связаны, и успех в одном из них может значительно повлиять на успех в других. Поэтому важно подходить к этой задаче с глубоким пониманием всех ее составляющих и стремиться к интегрированному подходу.

Новая методика предлагает такой подход к управлению рисками, который объединяет математическое моделирование с организационно-управленческими механизмами, что позволяет более точно предсказывать потенциальные риски и более эффективно разрабатывать стратегии для их смягчения.

Объединение этих элементов в одну систему может быть достигнуто поэтапно, как показано на рис. 2.

Рис. 2. Интегрированный подход к решению задачи

1. Идентификация рисков. Сначала необходимо определить потенциальные риски, которые могут возникнуть при решении задач ресурсного обеспечения и включать в себя анализ текущей ситуации, прогнозирование возможных изменений и оценку их вероятного влияния.

2. Математическое моделирование. Здесь можно использовать математические модели для представления этих рисков и их потенциального влияния на систему, которые могут включать в себя использование статистических методов, методов машинного обучения или других подходов к моделированию.

3. Разработка стратегий управления рисками. На основе результатов моделирования можно разработать стратегии для управления каждым из идентифицированных рисков, которые могут включать в себя выбор подходящих мер смягчения риска, разработку планов ответа на инциденты и определение процедур мониторинга и контроля [2].

4. Реализация организационно-управленческого механизма. Все элементы должны быть интегрированы в организационно-управленческий механизм, который определяет, как будут приниматься и реализовываться решения по управлению рисками [7].

Важно отметить, что все эти шаги должны зависеть друг от друга и постоянно адаптироваться к изменяющимся условиям; они требуют глубокого понимания всех нюансов выстроенной системы и способности быстро и эффективно реагировать на новую информацию.

Эта методика может быть применена в любой отрасли, где требуется управление рисками при решении задач ресурсного обеспечения. Сюда можно включать не только производство, где требуется балансировка между доступностью ресурсов и потребностями производства, но и финансы, где необходимо управлять рисками, связанными с государственными закупками, а также ресурсное обеспечение силовых структур.Возникает необходимость привести несколько примеров, которые могут иллюстрировать применение новой методики управления рисками.

Возникает необходимость привести несколько примеров, которые могут иллюстрировать применение новой методики управления рисками.

В частности, предложенная методика может быть использована для управления рисками, связанными с невыполнением плана перевозок из-за неблагоприятных внутренних или внешних обстоятельств. И если обратиться к математическому моделированию, то получится рассчитать, как различные факторы могут повлиять на процесс доставки ресурсов, а организационно-управленческий механизм может помочь разработать стратегии для смягчения этих рисков.

В области управления персоналом применение такой методики возможно для управления рисками, связанными с подбором персо-

нала, который не отвечает целям организации, потерей ключевых сотрудников и утечкой информации. Здесь математическое моделирование может помочь предсказать, как различные стратегии найма и увольнения могут повлиять на производительность и психологию персонала [3].

В финансовой сфере такая методика может использоваться для управления рисками, связанными с неосуществлением организацией своих финансовых обязательств из-за задолженностей, инфляции, изменения курса валют или по каким-либо другим причинам. Математическое моделирование, в свою очередь, сможет прогнозировать, как различные экономические условия повлияют на финансовую стабильность организации [4].

Рассмотренный интегрированный подход к решению задач по управлению рисками предлагает значительные преимущества при сравнении с традиционными подходами, узко или точечно рассматривающими возникающие проблемы. Можно предполагать возможность более точного прогнозирования рисков и более эффективного управления ими.

В целом новая методика успешно достигает своих целей. Однако ее эффективность может быть ограничена факторами, такими как доступность данных и вычислительные возможности. Дополнительное исследование может помочь определить способы преодоления этих ограничений.

Список литературы:

1. *Волчков Д. А., Топоров А. В.* Военно-экономическое обоснование процессов достижения ресурсного компромисса в обеспеченности вещевым имуществом военных потребителей // Экономический вектор. 2020. № 2 (21).

2. *Джамай Е. В., Зинченко А. С.* Разработка адаптивной многокомпонентной системы управления риском высокотехнологичных предприятий // Вестник МГОУ. Серия: Экономика. 2022. № 2.

3. *Ермолаев М. Б., Хомякова А. А., Белова А. Д., Серкова Ю. А.* Разработка алгоритма интеллектуальной поддержки принятия решений на базе системного подхода // Известия ВУЗов ЭФиУП. 2022. № 1 (51).

4. *Иванов В. В., Саркисьянц Ю. К.* Ситуационное моделирование принятия решений в международных контрактных операциях // Российский внешнеэкономический вестник. 2019. № 9.

5. *Ларионова Р. А., Кривогина Д. Н., Харитонов В. А.* Механизм управления структурой медицинского учреждения как организаци-

онной системой массового обслуживания в условиях нестационарного потока // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2023. № 1.

6. *Ткалич С. А.* Гибридная методика практической реализации системы принятия решений по приоритетному регулированию // Известия ЮФУ. Технические науки. 2021. № 7 (224).

7. *Яровова В. В.* Стратегическое управление предприятием в условиях ограничений и неопределенности // Гуманитарные, социально-экономические и общественные науки. 2023. № 4.

Андрей Александрович Жирнов
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: aumskw@yandex.ru

УДК 005.8:004

Об инструменте управления проектами противодействия криминальным угрозам

Аннотация

В статье определена необходимость использования специальных инструментов при управлении проектной деятельностью в организационной системе. Отмечено, что для управления деятельностью подразделений уголовного розыска в рамках разрабатываемой методологии проектного управления в сфере противодействия криминальным угрозам требуется разработка советующего задачам и специфике такой деятельности инструмента управления проектами в виде информационной системы. В качестве основного инструмента управления проектами предложена перспективная информационно-аналитическая система поддержки принятия решений при управлении проектами ПКУ. Определены ее цель, задачи, структура и некоторые принципы построения. Полученные результаты могут быть использованы на последующих этапах разработки рассматриваемого инструмента управления проектами.

Ключевые слова и словосочетания: *проект противодействия криминальным угрозам; проектный подход; проектное управление; информационно-аналитическая система; инструмент управления проектом.*

В настоящее время, характеризующееся стремительным развитием информационных технологий, увеличением объема передаваемой информации (к 2021 г. объем передаваемой информации по отношению к аналогичным показателям 2011 г. вырос в 300 раз [7]) и широким распространением технологий искусственного интеллекта, т. е. в условиях глобальной информатизации и цифровой трансформации, в том числе в сфере правоохранительной деятельности [1; 2], невозможно представить эффективное управление организационной системой (далее – ОС), которое бы осуществля-

лось без использования инструментов управления, реализованных в некоторой программной среде и позволяющих руководителям ОС получать актуальную информацию о процессах функционирования таких ОС и принимать на ее основе оптимальные управленческие решения.

Полагаем, что необходимость применения таких инструментов управления для достижения высоких показателей эффективности еще в большей степени актуализируется для ОС, в которых применяются методы и модели проектного управления. Дело в том, что реализовать основные преимущества проектного управления (достижение целей проекта в рамках временных и ресурсных ограничений) можно только при точном и быстром решении различных расчетно-аналитических задач, возникающих на этапах планирования и оперативного управления проектом. Такие задачи можно решить только с использованием инструментов управления, позволяющих автоматизировать процессы сбора, хранения, обработки и анализа информации, необходимой для принятия управленческих решений. Как правило, такие инструменты управления представлены в виде информационных систем, состоящих из совокупности аппаратных и программных средств.

Эффективность реализации проектов противодействия криминальным угрозам (далее – проектов ПКУ) в рамках разрабатываемой нами методологии управления проектами в сфере противодействия криминальным угрозам в подразделении уголовного розыска (далее – подразделении УР) в значительной степени будет определяться степенью автоматизации процессов управления проектами ПКУ и уровнем информационной поддержки при принятии управленческих решений. В связи с чем, по нашему мнению, требуется разработка общих требований к функциональным возможностям и архитектуре инструмента управления проектами ПКУ.

Таким образом, требуется определить цель, задачи и структуру основного инструмента управления проектами ПКУ. Исходя из общей постановки задачи, в дальнейшем будем его назвать информационно-аналитической системой поддержки принятия решений при управлении проектами ПКУ (далее – ИАС ППР ПКУ).

Полагаем, что ИАС ППР ПКУ должна представлять собой единую информационную среду, в которой была бы интегрирована информация обо всех аспектах проектной деятельности в подразделении УР, обращаясь к которой, заинтересованные стороны проекта ПКУ могли получить информацию, необходимую для принятия оптимальных решений.

Цель ИАС ППР ПКУ – обеспечение эффективного управления проектами ПКУ путем предоставления информационной поддержки: команде управления проектом, позволяющей ее членам принимать более обоснованные и точные управленческие решения при планировании проектов, оперативном управлении проектами и оценке результатов проектов; всем заинтересованным сторонам проекта ПКУ оперативно получать, отправлять, обрабатывать, анализировать информацию в соответствии с их проектными ролями и зонами ответственности, а также осуществлять коммуникацию между ними.

Тогда, используя метод «дерева целей», главную цель ИАС ППР ПКУ можно разложить на задачи, способствующие ее достижению, а проанализировав данные задачи, можно сформулировать функциональные требования, предъявляемые к ИАС ППР ПКУ.

Были сформулированы следующие основные *задачи* и функциональные требования к ИАС ППР ПКУ:

1. *Планирование проекта ПКУ*. ИАС ППР ПКУ должна позволять осуществлять планирование проекта ПКУ: формировать расписание проекта; рассчитывать оценочные сроки выполнения работ проекта; определять количество ресурсов, требуемое для успешной реализации проекта; рассчитывать риски, связанные с реализацией проекта.

2. *Оперативное управление проектом ПКУ*. ИАС ППР ПКУ должна позволять: отслеживать ход выполнения работ проекта ПКУ; управлять содержанием работ; управлять трудовыми ресурсами проекта, в том числе назначать исполнителей проекта на выполнение работ проекта; отслеживать относительную нагрузку на исполнителя проекта; контролировать доступность и использование в работах в соответствии с планом проекта возобновляемых и невозобновляемых ресурсов проекта; идентифицировать риски проекта и осуществлять реагирование на возникшие рисковые события с целью снижения их негативных последствий.

3. *Оценка результатов проекта ПКУ*. ИАС ППР ПКУ должна позволять оценивать по различным параметрам результаты проекта (например, по степени достижения цели проекта или отклонению фактических затраченных на достижение цели проекта времени и ресурсов); осуществлять анализ результатов проектов с целью выявления и устранения негативных факторов (допущенных ошибок, временных задержек), а также учета и распространения позитивных факторов (новых методик, подходов и практик, показавших свою эффективность), повлиявших на ход реализации проекта.

4. Коммуникация и обмен информацией. ИАС ППР ПКУ должна обеспечивать эффективную коммуникацию между заинтересованными сторонами проекта ПКУ, включая: возможность удаленного общения членов команды проекта друг с другом по различным каналам связи; автоматизацию процесса назначения исполнителей на выполнение работ проекта; электронный документооборот; инструменты совместной работы; доступ к проектной документации и отчетам о результатах проектной деятельности.

5. Накопление, обработка и анализ информации. ИАС ППР ПКУ должна обеспечивать возможность накопления информации обо всех аспектах проектной деятельности, осуществляемой ранее в подразделении УР, в том числе включая информацию о членах команды проектов ПКУ, их компетенциях и опыте работы. Кроме того, в ИАС ППР ПКУ должны быть реализованы механизмы структурирования и обработки накапливаемой информации, позволяющие формировать различные виды статистических и аналитических отчетов.

С позиции системного подхода, цели и задачи системы определяют ее структуру. Под структурой информационной системы принято понимать описание взаимосвязи элементов данной системы. Кроме того, в ряде случаев, дополнительно описываются принципы построения структуры информационной системы.

Для выявления наиболее эффективных принципов построения информационных систем, осуществляющих поддержку в принятии решений при управлении проектами, которые можно было бы использовать и в ИАС ППР ПКУ.

Был проведен анализ функциональных возможностей структуры, компонентов некоторых отечественных и зарубежных информационно-аналитических систем (Spider Project [4], Advanta [5], ProjectLibre [6], Microsoft Project [3], Oracle Primavera [8]), в результате которого были сделаны следующие выводы:

1. Большинство из рассмотренных нами информационно-аналитических систем имеют модульный принцип построения, предусматривающий разделение информационной системы на независимые (способные работать автономно), но взаимосвязанные модули (подсистемы). По нашему мнению, это связано со следующими преимуществами модульного принципа построения: во-первых, обеспечение большей гибкости информационной системы, при которой внесение изменений или замена отдельных модулей системы не оказывает влияния на работу всей системы; во-вторых, обеспечение надежности информационной системы, т. е. благодаря разделению информационной системы на подсистемы упрощаются процессы ее

проектирования и тестирования – каждый модуль может быть тщательно протестирован, отлажен и интегрирован отдельно.

2. Современные информационно-аналитические системы построены на облачных технологиях (под которыми понимается модель предоставления вычислительных ресурсов и программного обеспечения посредством сети Интернет). Как показал проведенный нами анализ, в своем развитии информационно-аналитические системы прошли путь от «локальных», установленных на одном рабочем месте, к «клиент-серверным», обеспечивающих подключение нескольких различных рабочих мест к единому серверу и соединение различных серверов между собой, а далее – до «облачных» информационных систем с подключением пользователей посредством сети Интернет и удаленным размещением серверов, обслуживаемых командой высококвалифицированных специалистов (рис. 1).

Рис. 1. Условное представление различных моделей предоставления вычислительных ресурсов и программного обеспечения

Облачные технологии позволяют сократить расходы на закупку, настройку и обслуживание собственного серверного оборудования. Кроме того, при такой модели предоставления вычислительных ресурсов и программного обеспечения с возможностью подключения пользователей и размещения серверов данных без привязки к конкретному местоположению (т. е. в любом месте, где доступно подключение к сети Интернет) достигается большая гибкость и масштабируемость информационной системы, что более удобно как для пользователей, так и для специалистов, обслуживающих такие системы.

В связи с чем полагаем, что перспективная ИАС ППР ПКУ также должна быть выполнена:

Во-первых, в виде единого программного комплекса с модульной структурой, что обеспечит гибкость ее конфигурации и обновления, а также возможность ее масштабирования с поэтапным наращиванием необходимых функций в отдельных программных модулях, где разделение ИАС ППР ПКУ на модули может осуществляться в соответствии с ее основными задачами, перечисленными выше.

Во-вторых, построена на облачных технологиях. По нашему мнению, ИАС ППР ПКУ может быть интегрирована в развернутую ИСОД МВД России, в основе которой лежит модель предоставления вычислительных ресурсов и программного обеспечения посредством внутриведомственной локальной вычислительной сети. При таком подходе можно использовать имеющуюся аппаратную и сетевую инфраструктуру (с добавлением требуемых серверных мощностей) и сделать акцент на разработке программной части ИАС ППР ПКУ.

В качестве основных модулей ИАС ППР ПКУ можно предложить следующие: модуль управления параметрами проекта ПКУ; планирования проекта ПКУ; контроля и мониторинга проекта ПКУ; оценки результатов проекта ПКУ; коммуникации и электронного документооборота; накопления и анализа информации.

Тогда структуру ИАС ППР ПКУ, состоящей из вышеперечисленных модулей, можно представить в следующем виде (рис. 2).

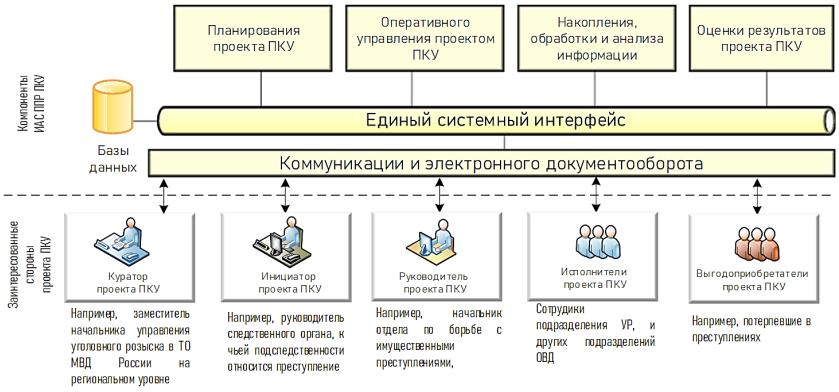

Рис. 2. Структура ИАС ППР ПКУ

В современных условиях цифровизации при переходе на новые подходы к управлению ОС, в том числе на проектный подход, осо-

бое внимание должно уделяться инструментам управления, позволяющим автоматизировать процессы сбора, хранения, обработки и анализа информации, необходимой для принятия оптимальных управленческих решений.

Полагаем, что в качестве такого инструмента применительно к разрабатываемой нами методологии управления проектами в сфере ПКУ может быть рассмотрена ИАС ППР ПКУ. Нами были определены ее цель, задачи, структура и некоторые принципы построения (модульность; предоставление ресурсов с использованием облачных технологий). Полученные результаты в дальнейшем могут быть использованы при непосредственной разработке ИАС ППР ПКУ и подобных систем.

Список литературы:

1. *Горошко И. В.* Правоохранительная деятельность: возможное изменение парадигмы в эпоху цифровизации // Елецкий государственный университет имени И. А. Бунина. 2022.

2. *Горошко И. В., Бондаренко Ю. В.* Современные вызовы информатизации и правоохранительная деятельность // Институт проблем управления имени В. А. Трапезникова. 2019.

3. ПО для управления проектами | Microsoft Project. URL: https://www.microsoft.com/ru-ru/microsoft-365/project/project-management-software (дата обращения: 21.02.2024).

4. Спайдер Проджект. Публикации. URL: http://www.spiderproject.ru/ru2/index.php/publications (дата обращения: 21.02.2024).

5. ADVANTA – система управления проектами для бизнеса. URL: https://www.advanta-group.ru/ (дата обращения: 21.01.2024).

6. Alternative to Microsoft Project Open Source | Projectlibre. URL: https://www.projectlibre.com/ (дата обращения: 21.01.2024).

7. Ericsson Mobility Report November 2021 // Tenth anniversary of the Ericsson Mobility Report is packed with stats from a decade of mobile data traffic. URL: https://www.ericsson.com/en/press-releases/2021/11/ericsson-mobility-report-mobile-data-traffic-increased-almost-300-fold-over-10-years (дата обращения: 06.10.2023).

8. Oracle Primavera P6 EPPM User and Integration Documentation Version 22. URL: https://docs.oracle.com/cd/F51301_01/index.htm (дата обращения: 21.02.2024).

Александр Иванович Иванов,
доктор технических наук, профессор,
научный консультант
АО «Пензенский научно-исследовательский
электротехнический институт»
E-mail: bio.ivan.penza@mail.ru

Людмила Антоновна Лекарь,
кандидат технических наук,
доцент кафедры информационных технологий
Академия управления МВД России
E-mail: antonna47@bk.ru

УДК: 004.852

Необходимость отечественного стандарта на тестирование качества нейросетевого распознавания лиц людей

Аннотация

Доверенное тестирование приложений искусственного интеллекта должно быть выполнено доверенной испытательной лабораторией на доверенной базе тестовых биометрических образов. Когда речь идет о распознавании образов лиц людей, должны использоваться реальные базы, полученные не в идеальных социальных сетях, а с реально работающих видеокамер охранной системы или близрасположенных систем наблюдения с видеофиксацией. Нужен открытый код тестирования, соответствующий требованиям отечественных стандартов.

Какие образы лиц, какого качества, каких людей, в каких условиях они получены, каковы их объемы – это все прерогатива силовых структур, решающих проблемы защиты прав законопослушных граждан. Любой коммерсант России хочет поставлять свои продукты органам Госвласти. Вопрос в том, насколько тот или иной коммерческий продукт является качественным. Ведущие зарубежные университеты и испытательная лаборатория NIST (National Institute of Standards and Technology) США готовы выполнить тестирование нейронных сетей, распознающих лица людей. Однако сегодня испытательным лабораториям недружественных стран доверять уже нельзя. Необходимы свои отечественные средства тестирования качества и распознавания лиц, обеспечиваемые тем или иным коммерческим продуктом.

Ключевые слова и словосочетания: *отечественный стандарт; тестирование; нейросети; распознавания лиц людей; биометрия; системы наблюдения с видеофиксацией; правоохранительная деятельность; обеспечение общественного порядка.*

Распознавание лиц с использованием многослойных сетей искусственных нейронов давно уже является промышленной технологией широкого применения. Одним из отечественных лидеров этой технологии является фирма NtehLab, которая в декабре 2021 г. прошла тестирование в испытательной лаборатории NIST (США) и, видимо, имеет на свой продукт 2021 г. зарубежный сертификат.

Насколько потребитель из России может доверять сертификату NIST – вопрос открытый. Основой доверия к результатам тестирования является доверие не только к тестору, но и к базам биометрических образов, на которых было выполнено тестирование. Испытательная лаборатория NIST и испытательные лаборатории иных зарубежных университетов не предоставляют доступ к своим тестовым базам. Какие у них тестовые базы никто не знает.

Если тестовые базы имеют изображения «хорошего» качества, то и результат тестирования улучшится. Верно и обратное: рост в тестовой базе «плохих» изображений должен приводить к ухудшению определяемых вероятностных характеристик.

Вывод напрашивается сам собой: «спасение утопающих – дело рук самих утопающих». Нет смысла ждать милости от NIST и испытательных лабораторий других зарубежных университетов. Целесообразно привлекать к созданию испытательных лабораторий отечественные университеты, которым доверяет тот или иной потребитель технологии нейросетевого распознавания лиц.

Задача создания открытого программного обеспечения под тестирование не является сложной. Она вполне посильна кооперации промышленных организаций, которые договорились о протоколах тестирования. Национальный стандарт (например, стандарт технического комитета № 164 «Искусственный интеллект») как раз и является некоторым компромиссом и чередой взаимных уступок производителей. Главное, чтобы код средства тестирования был открытым (общедоступным).

Поясним сказанное рис. 1. Обычно программный продукт того или иного производителя строится на поиске лиц в видеокадре. В левой части рисунка приводится найденное в кадре лицо. Обнаруженный фрагмент с лицом приводится, например, к изображению 64x64 пикселя. Каждый пиксель является вектором входных дан-

ных для сверточной многослойной нейронной сети [1; 4]. Условная сверточная нейросеть отображена в правой части рис. 1.

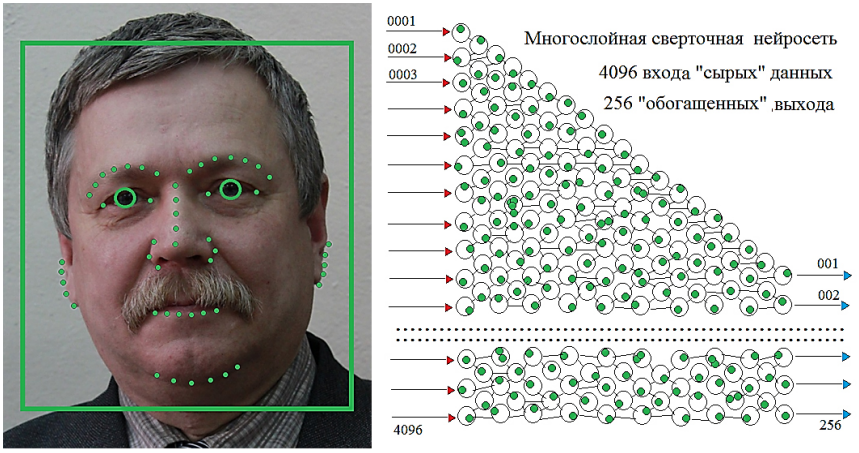

Рис. 1. Основа технологии применения многослойных нейронных сетей, заранее обученных свертывать длинный вектор входных «сырых» данных в вектор меньшей размерности, «обогащенный» выходными данными

Основная задача любых нейронных нейронных сетей – это «обогащение» входных «сырых» данных. Нейросеть правой части рис. 1 заранее обучена свертывать вектор «сырых» входных биометрических данных длинной в 4096 (пикселей) в более короткий вектор из 256 биометрических параметров лица человека.

Обучение нейросети выполняется примерно на 16 примерах образа «Свой» (16 разных изображений лица одного и того же человека). На 16 примерах удается вычислить математическое ожидание каждого из 256 контролируемых биометрических параметра, а также их стандартное отклонение.

В этих условиях как решающее правило для каждого примера может быть использовано расстояние Евклида:

$$\mathrm{R_j} = \sum_{i=1}^{256} \frac{(x_{i,j} - E(x_i))^2}{256 \cdot (\sigma(x_i))^2} \quad (1),$$

где E (.) – оператор вычисления математического; σ(.) – оператор вычисления стандартного отклонения; j – номер примера в обучающей выборке.

Само решающее правило сводится к выбору допустимых порогов изменения расстояний (1). Обычно пороги выбирают таким образом, чтобы все примеры в обучающей выборке «Свой» принимались.

Описанная выше технология не является экзотикой – это фрагмент «машинного обучения». Под задачу оценки качества «машинного обучения» уже существует международный стандарт, который в ближайшее время будет гармонизован и введен в действие на территории России[1].

Решение проблемы обеспечения конфиденциальности содержания «рабочих» и «тестовых» баз биометрических образов

Отметим, что открытый код средства тестирования связан с тестируемым коммерческим продуктом только через длину вектора выходных данных сверточной нейросети, т. е. от создателя коммерческого продукта потребуется добавить в тестируемую версию его продукта несколько дополнительных строк кода. Эти строки должны формировать для средства тестирования файл со значениями выходных векторов для 20 примеров образа лица человека. Доработка программного обеспечения под внешнее независимое тестирование минимальна. Для тестирования продукта его исходный код не нужен (полностью сохраняются авторские права производителя на код его продукта), если сертификация касается только обеспечиваемых приложением вероятностей ошибок первого и второго рода.

При наличии тестового программного обеспечения с открытым кодом сама тестовая база может быть любой: потребитель имеет возможность формировать ее сам, одновременно обеспечивая ее конфиденциальность. Разработчики открытого кода тестового программного обеспечения должны пользоваться своей тестовой базой, с которой они вольны поступать, как угодно. Разработчики могут как сохранить, так и уничтожить после отладки продукта собственную отладочную базу лиц.

При такой постановке задачи потребитель программного продукта получает возможность выполнять самостоятельно тестирование на качество всех предлагаемых ему коммерческих решений. При этом он сможет использовать свои собственные «рабо-

[1] ПНСТ 835–2023 (ISO/IEC TS 4213:2022). Гармонизованный проект национального стандарта ТК 164. «Искусственный интеллект. Оценка эффективности моделей и алгоритмов машинного обучения в задаче классификации».

чие» базы, по которым в будущем должен будет выполняться поиск того или иного биометрического образа. Нет необходимости передавать уже имеющие у потребителя «рабочие» базы сторонним тесторам. В ряде случаев обеспечение конфиденциальности биометрических образов является принципиально важным. Например, принципиально важным является сохранение конфиденциальности базы лиц людей, уже когда-то преступивших закон, уже когда-то находившихся под следствием и уже отбывших наказание за содеянное.

Уже стандартизованное в России решение проблемы увеличения объема тестовых баз морфингом дополнительных образов

Обычно стремятся к тому, чтобы объем тестовой базы был примерно в 30 раз больше, чем ожидаемая вероятностная характеристика ошибок второго рода (ложное принятие образа «Чужой» как образа «Свой»). Например, если для некоторого коммерческого продукта заявлена вероятность ошибок второго рода $P_2 \approx 0.005$ (доверительная вероятность – 0.995), то для проверки этого заявления потребуется тестовая база лиц «Чужой» объемом не менее 60 000 тестовых биометрических образов[1].

Очевидно, что NIST (опираясь на госбюджетное финансирование США) всегда сможет заранее сформировать тестовую базу любого объема под заявленные достаточно высокие вероятностные характеристики коммерческих продуктов. Проблема высокой стоимости формирования больших тестовых баз биометрических образов известна давно. Именно она останавливает руководство обычных университетов от создания собственных испытательных лабораторий качества коммерческих продуктов нейросетевого распознавания образов.

Такая проблема стоит для всех зарубежных университетов, кроме российских и белорусских. В 2010 г. принят национальный стандарт России ГОСТ Р 52633.2[2], регламентирующий формирование синтетических векторов образов–потомков, полученных из векторов реальных образов–родителей.

Общий подход к расширению тестовой базы иллюстрируется рис. 2.

---

[1] ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура».

[2] ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

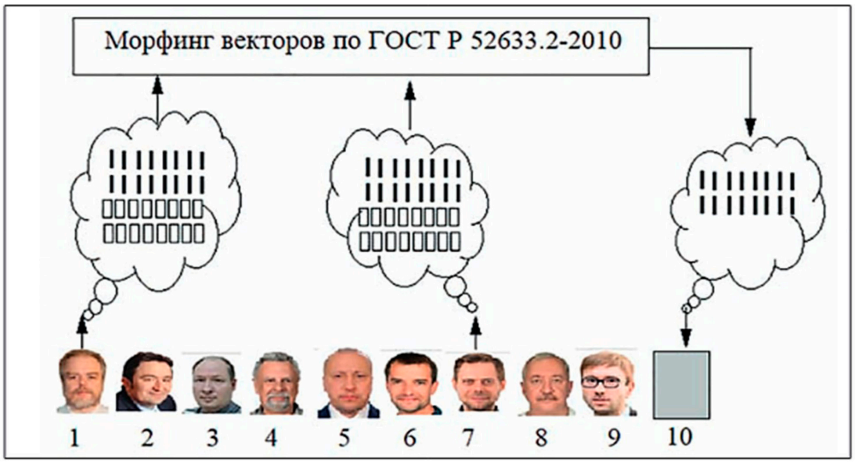

Рис. 2. Морфинг-размножение реальных биометрических образов лиц людей (образов–родителей) синтетическими биометрическими образами–потомков

Если руководствоваться требованиями отечественного стандарта[1] по формированию баз биометрических образов, то каждый образ должен быть представлен 16 и более примерами. Это требование обусловлено тем, что на каждом образе тестовой базы мы должны иметь возможность обучить свою нейросеть, например, опираясь на расстояние Евклида (1). Как результат, вместо одного изображения лица человека в тестовой базе появляется 16 изображений обучающей выборки. На рис. 2 эта ситуация поясняется для лица–1 и лица–7 в форме двух облаков над ними, отображающих нестабильность (размытость) каждого биометрического образа.

Очевидным также является то, что каждому примеру образа «Свой» сверточная нейронная сеть будет ставить в соответствие 16 коротких векторов обогащенных данных. При организации поиска и тестирования на компьютере нет смысла хранить реальные примеры изображений лица. Вместо них удобнее хранить их короткие вектора уже обогащенных биометрических данных. Это обеспечивает существенное снижение требуемой память и, соответственно, ускорение тестирования [2; 3].

Следует отметить, что морфинг двух лиц – это давно используемая вычислительная процедура. Обычно ее используют худож-

[1] ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

ники. Для этой цели художник вручную задает одинаковые точки на лицах, а далее компьютер создает промежуточные расстояния между двумя лицами. Формально каждый программный продукт при поиске лиц на изображении выделяет некоторые точки на лице (см. рис. 1), опираясь на которые, может быть построен морфинг промежуточных вариантов между двумя связываемыми между собой лицами.

В рассматриваемом нами случае нет необходимости в обычном морфинге, так как мы имеем короткие вектора обогащенных данных. В соответствии с ГОСТ Р 52633.2[1] для скрещивания двух векторов от двух изображений двух разных лиц и получения векторов одного образа–потомка достаточно выполнить операцию усреднения одинаковых параметров. Последнее отображено третьим облаком векторов на рис. 2, для которого можно восстановить примеры, однако в этом нет необходимости.

Создать первоначальную тестовую базу из 1000 лиц студентов посильно для любого университета. Если процедура получения синтетических векторов будет построена на получение одного образа–потомка от двух образов–родителей, то удастся увеличить тестовую базу до полумиллиона образов. При получении от двух образов–родителей двух образов–потомков мы увеличиваем объем тестовой базы до одного миллиона образов лиц людей. Этого вполне достаточно для организации при любом отечественном университете испытательной лаборатории. При этом испытательная лаборатория университета может встать в позицию NIST, не предоставляя доступ сторонним пользователям к его тестовой базе.

Перспектива устранения произвола почти полного отсутствия информации о статистиках тестовых баз

Позволить себе почти ничего не сообщать о статистиках используемой тестовых баз реальных биометрических образов могут далеко не все. То, что позволено NIST, никому иному не дозволено. Если развитие тестирования пойдет по пути создания множества испытательных лабораторий разных университетов, то университетам придется сообщать о статистических характеристиках своих тестовых баз. Не вдаваясь в содержание статистик, рискнем назвать только некоторые их параметры.

[1] ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

1. Число естественных биометрических образов, собранных по ГОСТ Р 52633.1[1];

2. Число добавленных синтетических образов, созданных по ГОСТ Р 52633.2[2];

3. Средняя вероятность ошибок второго рода – Р2 для среднестатистического образа лица по базе естественных образов;

4. Вероятность ошибок второго рода для наихудших по стойкости 3 % лиц по базе естественных биометрических образов;

5. Вероятность ошибок второго рода для наилучших по стойкости 3 % лиц по базе естественных биометрических образов.

Необходимость в опубликовании такого типа статистик позволяет заказчику тестирования ориентироваться в собранных в той или иной базе тестовых образов. Подобные характеристики несложны; формально они должны быть заложены в открытом коде тестирования (если таковой будет создан).

По крайней мере опубликование даже этих статистических характеристик должно существенно ограничить возможные манипуляции со стороны испытательных лабораторий.

Почему необходим не только контроль за коммерческими продуктами проверки качества работы нейросетевых приложений, но и за испытательными лабораториями? Ответ на этот вопрос прост. Необходимо исключить возможность злоупотреблений (субъективности) со стороны испытательных лабораторий. Если испытательная лаборатория ничего не говорит о статистиках ее тестовых баз и не предоставляет эти базы испытуемому, то возможны злоупотребления. Если испытательная лаборатория хочет улучшить статистики проверяемого продукта, то ей достаточно ухудшить стабильность биометрических характеристик тестовых баз. Верно и обратное: повышение стабильности биометрических параметров среднестатистического биометрического образа будет обязательно приводить к улучшению вероятностных характеристик проверяемого продукта.

Авторы данной статьи уверены в том, что создание открытого кода для тестирования качества работы нейросетевых приложений является вполне посильной задачей для отечественной промышленности, однако параллельно с этим нужен отечественный

[1] ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

[2] ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

стандарт. В свою очередь, появление подобного программного обеспечения даст реальную возможность любой отечественной структуре развернуть под своим контролем испытательные лаборатории без компрометации реально используемых тестовых баз лиц реальных людей или иных образов.

Задача разработки нейросетевых приложений искусственного интеллекта, включая его предварительное тестирование и задача самостоятельного тестирования качества заказчиком работы того или иного коммерческого продукта должны быть разделены. При этом размер используемых тестовых баз реальных образов лиц не является технической проблемой. По крайней мере это относится к России и Белоруссии, где действует стандарт ГОСТ Р 52633.2-2010[1].

Список литературы:

1. *Аггарвал Чару*. Нейронные сети и глубокое обучение // Санкт-Петербург, 2020.

2. *Иванов А. И.* Искусственный интеллект высокого доверия Ускорение вычислений и экономия памяти при тестировании больших сетей искусственных нейронов на малых выборках // Системы безопасности. 2020. № 5.

3. *Майоров А. В., Сомкин С. А., Юнин А. П., Акмаев А. Ж.* Оценка стойкости защищенных нейросетевых преобразователей биометрия-код с использованием больших баз синтетических биометрических образов // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 4 (48).

4. *Николенко С., Кудрин А., Архангельская Е.* Глубокое обучение. Погружение в мир нейронных сетей. Санкт-Петербург, 2018.

[1] ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

Никита Сергеевич Карнаухов,
адъюнкт факультета подготовки
научных и научно-педагогических кадров
Академия управления МВД России
Email: wingspan@list.ru

УДК: 004.832.22

Цифровое фенотипирование: перспективы и вызовы

Аннотация

Цифровое фенотипирование является современным исследовательским подходом, который объединяет генетику и фенотипическую информацию с целью понимания связи между генотипом и фенотипом. В данной статье будут рассмотрены основные принципы цифрового фенотипирования, методы получения данных о геноме и фенотипе, а также перспективы и вызовы в области исследования генетических вариаций и их влияния на фенотип.

Ключевые слова и словосочетания: *цифровое фенотипирование; секвенирование; ДНК; анализ геномной информации.*

Цифровое фенотипирование представляет собой мощный инструмент для исследования сложных связей между генотипом и фенотипом. С течением времени методы цифрового фенотипирования становятся все более доступными и дешевыми, что приводит к увеличению возможностей для проведения исследований в этой области.

Необходимость обработки больших объемов данных и сложность их анализа являются одними из главных вызовов цифрового фенотипирования. Это требует развития современных вычислительных инструментов и подходов к обработке данных [4]. Кроме того, этические и правовые вопросы, связанные с хранением и использованием геномных данных, требуют серьезного внимания и обсуждения.

Также следует учитывать, что цифровое фенотипирование может столкнуться с ограничениями в понимании сложных взаимодействий между генотипом и фенотипом. Многофакторная природа фенотипических характеристик и их зависимость от внешних факторов делают сложной задачу полного и точного предсказания фенотипа на основе генетической информации [1].

Цифровое фенотипирование стало неотъемлемой частью расследования преступлений в современном правосудии. С появлени-

ем высокопроизводительных методов секвенирования ДНК и развитием биоинформатических технологий возможности использования генетических данных для выявления и идентификации преступников значительно увеличились [5].

Цифровое фенотипирование при расследовании преступлений основано на изучении уникальных генетических характеристик каждого индивида, которые передаются по наследству. Геном – это полный набор генетической информации, хранящейся в ДНК. Анализ генома позволяет определить уникальные генетические маркеры, такие как полиморфизмы однонуклеотидных полиморфизмов (SNP), короткие тандемные повторы (STR) и др. [7].

При расследовании преступлений останки преступника или следы ДНК на месте преступления могут быть подвергнуты геномному анализу и последующему фенотипированию. На основе этих данных можно сравнить геном преступника с генетическими данными, хранящимися в генетических базах данных, таких как национальные и международные базы данных ДНК. Это позволяет выявить потенциальных подозреваемых и установить связи между различными преступлениями и преступниками.

Цифровое фенотипирование также может использоваться для идентификации жертв преступлений. Если обнаружены останки неопознанной жертвы, генетическая информация может быть сопоставлена с данными пропавших людей и их ближайших родственников, чтобы установить их личность.

Одним из подходов к цифровому фенотипированию является анализ ассоциации генетических вариаций с фенотипическими характеристиками. Это позволяет исследователям определить, какие гены могут быть связаны с конкретными фенотипическими проявлениями. Другой подход – функциональное цифровое фенотипирование. Он заключается в исследовании изменений, вызванных генетическими вариациями, на уровне клеточных и молекулярных систем. Это может помочь в понимании механизмов, лежащих в основе определенных фенотипических проявлений [6].

Основные методы цифрового фенотипирования:

1. Секвенирование ДНК. Современные методы секвенирования ДНК позволяют исследователям определить последовательность нуклеотидов, из которых состоит геном. Это открывает двери для анализа генетических вариаций и их связи с фенотипическими характеристиками. Такие технологии, как секвенирование следующего поколения, позволяют собирать огромные объемы данных о геноме, что расширяет возможности исследования.

Рис. 1. Секвенирование ДНК

Это простая схема, которая показывает основные этапы секвенирования ДНК. Первоначально происходит превращение и изоляция ДНК. Затем полученные фрагменты ДНК маркируются. После этого происходит само секвенирование фрагментов ДНК, а затем результаты секвенирования считываются и анализируются.

2. Анализ экспрессии генов. Этот метод позволяет исследовать активность и множественность экспрессии генов. Анализ экспрессии генов может помочь исследователям понять, какие гены активны и какие влияют на определенные фенотипические проявления. Это особенно полезно для исследования генов, связанных с развитием заболеваний или ответом на терапию.

3. Метаболомное фенотипирование. Этот подход направлен на изучение небольших органических молекул, известных как метаболиты, в клетках или тканях организма. Изменение профиля метаболитов может свидетельствовать о наличии определенных генетических вариаций и может служить индикатором различных фенотипических изменений.

4. Генотипирование связанных с фенотипом маркеров. Исследователям интересно определить специфические генетические маркеры, которые могут быть связаны с определенными фенотипическими характеристиками. Такие маркеры, как однонуклеотидные полиморфизмы (ОНП), могут служить индикаторами для различных фенотипических проявлений, включая предрасположенность к различным заболеваниям.

Использование формул и рисунков в статье поможет визуализировать концепции и результаты исследований, а также облегчить понимание сложных математических и статистических моделей, используемых в анализе данных.

1. Формула для расчета генетической связи между генотипом и фенотипом:

$$P = G + E$$

В этой формуле P обозначает фенотип, G – генотип, а E – окружающую среду. Формула предполагает, что фенотип определяется как сумма генетической составляющей (генотип) и внешних факторов (окружающая среда).

2. Формула для вычисления скорости реакции амплификации полимеразы (PCR):

$$V = (Vmax * c) / (Km + c)$$

Здесь V обозначает скорость реакции, Vmax – максимальную скорость реакции амплификации полимеразы, c – концентрацию матрицы ДНК, а Km – константу Михаэлиса, которая представляет собой меру аффинности фермента к матрице.

3. Формула для расчета генетической дисперсии:

$$Vg = (\sigma g^2) / (\sigma p^2)$$

Здесь Vg обозначает генетическую дисперсию, σg^2 – генетическую дисперсию, а σp^2 – общую дисперсию. Генетическая дисперсия представляет собой часть общей дисперсии фенотипа, которая объясняется генетическими различиями.

4. Формула для вычисления генетического расстояния между двумя локусами:

$$D = (r * 0.5) / (1 - r)$$

Здесь D обозначает генетическое расстояние, а r – коэффициент сцепленности между двумя локусами. Формула основана на законе Харди-Вайнберга и позволяет оценить генетическое расстояние на основе известного коэффициента сцепленности.

В заключение цифровое фенотипирование представляет собой возможность глубже понять соотношение генотипа и фенотипа. Современные методы и подходы развиваются быстрыми темпами [3], что открывает новые перспективы в исследовании генома и его влияния на фенотип. Однако необходимо продолжать работу над развитием технологий и улучшением методов обработки данных [2], а также активно обсуждать этические вопросы, связанные с цифровым фенотипированием.

Список литературы:

1. *Дворянкин О. А.* Биометрия в интернете – информационные технологии современности // Eastern European Scientific Journal. 2022. № 27.

2. *Дворянкин О. А.* Герои нашего информационного времени // Национальная Ассоциация Ученых. 2021. № 36-4 (63).

3. *Дворянкин О. А.* Информационная война в сети интернет // Молодой ученый. 2021. № 6 (348).

4. *Дворянкин О. А.* По ту сторону Введенских ворот. Кибержизнь. «Мизер» или «Игра теней». Берегите себя // ИПЦ Маска. 2024.

5. *Винс Буффало.* Навыки работы с биоинформатическими данными. 2015.

6. *Поляничева Т. Д.* Биоинформатика и средства информационных технологий для хранения и эффективного анализа биологических данных: сборник статей Международной научно-практической конференции. Петрозаводск, 2023.

7. *Цветков В. Я.* Даталогия и биоинформатика // Славянский форум. 2022. № 2 (36).

Андрей Викторович Кокорев,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
Email: majjor77@rambler.ru

УДК: 007.621.391

О нормативно-правовом регулировании авиационного обеспечения Министерства внутренних дел Российской Федерации

Аннотация

В статье представлен анализ норм права по использованию средств беспилотной авиации органами внутренних дел в интересах решения правоохранительных задач. Рассмотрена современная структура авиационного обеспечения Министерства внутренних дел Российской Федерации.

Ключевые слова и словосочетания: *нормативно-правовое регулирование авиационного обеспечения; структура авиационного обеспечения; аэромобильные комплексы.*

Территория нашей страны занимает на карте мира одну шестую часть суши. Эти огромные пространства не всегда позволяют органам внутренних дел Российской Федерации (далее — ОВД), не обладающим достаточной мобильностью, оперативно и эффективно выполнять возложенные на них обязанности [1].

В XXI веке на фоне стремительно проходящего научно-технического прогресса, благодаря совершенствованию технических характеристик и наличию некоторых объективных условий деятельности правоохранительной системы, появилась потребность в высокомобильной возможности мониторинга оперативной обстановки и быстрой транспортировки сотрудников на место совершения правонарушения. Так, в 2003 г. было принято решение о создании в составе Министерства внутренних дел Российской Федерации (далее — МВД России) собственной авиации ОВД. Напомним, что в отличии от ОВД Советского Союза, сформировавшиеся после его распада правоохранительные органы Российской Федерации не могли похвастаться наличием такой необходимой составляющей. В СССР была возможность задей-

ствовать авиационную технику (самолеты, вертолеты) у Министерства гражданской авиации СССР вместе с летным и техническим персоналом. Благодаря уникальным авиационным возможностям повышалась эффективность деятельности ОВД особенно на удаленных расстояниях, сложных рельефах местности, в том числе в акваториях [2].

В самом начале XXI века пристальное внимание было уделено обоснованию возможности повышения эффективности деятельности органов и подразделений МВД России по решению правоохранительных задач, учитывая уникальные разрешительные возможности аэромобильных комплексов [3]. В результате углубленного исследования данного вопроса по задействованию разнородных технических комплексов было принято решение федерального уровня о формировании системы авиационных отрядов специального назначения МВД России.

Постановление Правительства Российской Федерации от 2 сентября 2003 г. № 542 «Об авиации органов внутренних дел Российской Федерации»[1] и принятое на его основе Положение об авиации ОВД, утвержденное приказом МВД России от 1 октября 2003 г. № 763 «О мерах по реализации Постановления Правительства Российской Федерации от 2 сентября 2003 года № 542»[2] дали широкие возможности по использованию собственной авиационной техники и персонала, состоящего из сотрудников ОВД [6]. Началось создание авиационных отрядов специального назначения, задействующих летательную и воздухоплавательную технику, оснащенных самолетами, вертолетами, беспилотными летательными и воздухоплавательными аппаратами различных типов как отечественного, так и иностранного производства [4; 5].

В условия длящейся реформы правоохранительной системы авиационные отряды специального назначения покинули систему МВД России. Указ Президента Российской Федерации от 5 апреля 2016 г. № 157 «Вопросы Федеральной службы войск

[1] Об авиации органов внутренних дел Российской Федерации: Постановление Правительства Российской Федерации от 2 сентября 2003 г. № 542. URL: https://base.garant.ru/1353227/ (дата обращения: 20.10.2023).

[2] О мерах по реализации Постановления Правительства Российской Федерации от 2 сентября 2003 года № 542: Положение об авиации органов внутренних дел Российской Федерации от 1 октября 2003 г. № 763. URL: https://base.garant.ru/1353227/#block_1000 (дата обращения: 20.10.2023).

национальной гвардии Российской Федерации»[1] вновь лишил МВД России авиационной составляющей. Авиационная техника и обслуживающий персонал были переданы в новую силовую структуру.

Однако польза от применения авиации в работе ОВД была понятна как руководству страны, так и Министерству. Поручения Президента Российской Федерации от 30 декабря 2022 г. № Пр-2548[2], а также обновления, вносимые в Федеральный закон от 19 марта 1997 г. № 60-ФЗ «Воздушный кодекс Российской Федерации»[3], позволили рассмотреть и положительно разрешить вопрос о возвращении авиационных подразделений в состав МВД России, восстановить авиационное обеспечение в деятельности органов и подразделений МВД России, пока только с использованием беспилотных воздушных судов и беспилотных авиационных систем.

Поэтому Федеральным законом от 4 августа 2023 г. № 440 «Внесение изменений в отдельные законодательные акты Российской Федерации»[4] в ст.ст. 11 и 13 Федерального закона от 7 февраля 2011 г. № 3 «О полиции»[5] были внесены дополнения по использованию беспилотных воздушных аппаратов (далее – БВС [БАС]). На основании этих изменений была выстроена четкая структура руководства и управления авиационным обеспечением МВД России, определены подразделения по организации, подготовке и выполнению задач авиационной поддержки ОВД (рис. 1).

---

[1] Вопросы Федеральной службы войск национальной гвардии Российской Федерации: Указ Президента Рос. Федерации от 5 апреля 2016 г. № 157. URL: https://base.garant.ru/71368610/?ysclid=ltyidlrwb3779660737 (дата обращения: 20.10.2023).

[2] Перечень поручений по вопросам развития беспилотных авиационных систем: утв. Президентом Рос. Федерации 30 декабря 2022 г. № Пр-2548. URL: https://www.garant.ru/products/ipo/prime/doc/405967211/?ysclid=ltyigmobll798403766 (дата обращения: 20.10.2023).

[3] Воздушный кодекс Российской Федерации: Федер. закон от 19 марта 1997 г. № 60-ФЗ. URL: https://base.garant.ru/10200300/?ysclid=ltyiinoqa6732696914 (дата обращения: 20.10.2023).

[4] О внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон от 4 августа 2023 г. № 440-ФЗ. URL: http://publication.pravo.gov.ru/document/0001202308040025?ysclid=ltyilpu7kf134942277 (дата обращения: 20.10.2023).

[5] О полиции: Федер. закон от 7 февраля 2011 г. №3-ФЗ. URL: https://base.garant.ru/12182530/?ysclid=ltyint4qwg707110597 (дата обращения: 20.10.2023).

Рис. 1. Структура авиационного обеспечения МВД России

Ведущую роль в организации, планировании и контроле авиационного обеспечения выполняет отдел робототехники и беспилотных летательных аппаратов управления связи ДИТСиЗИ МВД России. По его рекомендации на основании приказа от 18 января 2019 г. производится закупка современных беспилотных летательных аппаратов предпочтительно отечественного производства.

Согласно приказу МВД России от 29 декабря 2022 г. № 1111 «Об утверждении Курса поддержания летной натренированности авиационного персонала МВД России на беспилотных воздушных

судах»[1] в Учебном методическом центре Федерального казенного учреждения «Научно-производственное объединение «Специальная техника и связь МВД России» и других учебных центрах идет теоретическая и практическая подготовка летного персонала по управлению и обслуживанию БВС (БАС).

Утверждение приказа МВД России от 13 июля 2022 г. № 516 «О некоторых вопросах подразделений информационных технологий, связи и защиты информации территориальных органов МВД России»[2] позволило сформировать группы, отделения и отделы по применению и эксплуатации робототехнических комплексов и беспилотных воздушных судов Центра информационных технологий, связи и защиты информации МВД России территориальных органов.

Список литературы:

1. *Бецков А. В.* Применение аэромобильных комплексов МВД России при противодействии преступности: методические рекомендации. Москва, 2015.

2. *Бецков А. В.* Теоретические и организационные основы формирования аэромобильных комплексов МВД России. Москва: ТЭИС, 2009. 198 с.

3. *Бецков А. В.* Формирование и функционирование аэромобильных комплексов МВД России (теоретические, правовые и организационные основы). Москва: ТЭИС, 2010. 238 с.

4. Воздушная поддержка безопасности // Еженедельная газета «Петровка, 38». № 19 (9325).

5. Использование вертолетов в полицейских службах. URL: https://helico-russia.ru/blog/ispolzovanie-vertoletov-v-politseyskikh-sluzhbakh/ (дата обращения: 20.10.2023).

6. *Павлов Д. В., Павлова Л. Р.* Использование авиации в органах внутренних дел // Закон и право. 2020. № 11.

[1] Об утверждении Курса поддержания летной натренированности авиационного персонала МВД России на беспилотных воздушных судах: приказ МВД России от 29 декабря 2022 г. № 111.

[2] О некоторых вопросах подразделений информационных технологий, связи и защиты информации территориальных органов МВД России: приказ МВД России от 13 июля 2022 г. № 516.

Александр Федотович Крячко,
полковник запаса, доктор технических наук, профессор,
заведующий кафедрой радиотехнических
и оптоэлектронных комплексов
Санкт-Петербургский государственный
университет аэрокосмического приборостроения
Email: alex_k34.ru@mail.ru

Сергей Алексеевич Майоров,
кандидат технических наук,
доцент кафедры
Московский государственный технический
университет имени Н. Э. Баумана
Email: msa21051982@mail.ru

УДК 004.056.55

Повышение эффективности стеганографического метода с множественным доступом на основе технологии MC-CDMA

Аннотация

В современных условиях на практике возрастает частота использования при организации стеганографического канала связи потоковых контейнеров, в частности цифрового видео (что обязательно должно учитываться при разработках современных криптостеганографических систем), хотя на сегодня, как свидетельствуют открытые источники, ощущается значительная нехватка соответствующих стеганометодов, что обусловлено в первую очередь сложностью задачи, ориентированностью (для обеспечения определенных свойств стеганосообщения) математических базисов методов в основном на области преобразования контейнеров, что имеет негативные последствия: подобные преобразования (сингулярное разложение, дискретное косинусное преобразование, вейвлет-преобразование и др.) характеризуются значительной вычислительной сложностью, увеличением ошибок округления, из-за которых возможны искажения защищаемой информации, а также снижением вероятности обеспечения надежности восприятия стеганосообщения за счет непредсказуемости амплитуды изменений в пространственной области при воздействии на блоки цифрового изображения или кадра цифрового видео в пространстве преобразований.

Ключевые слова и словосочетания: *канал связи; стеганография; передача информации; преобразование Уолша-Адамара; код Хаффмана; встраиваемая информация; схема уплотнения каналов; разбалланс; теорема Шеннона.*

Большинство современных стеганографических методов позволяют организовать скрытый стеганографический канал только между парой абонентов. При этом для решения ряда практических задач возникает необходимость организации множественного доступа к скрытому каналу, что допускает одновременную работу множества авторизованных пользователей при обеспечении эффективного сокрытия самого факта передачи информации.

Сегодня известны [3–4; 10] методы организации скрытого стеганографического канала передачи информации с множественным доступом, которые основаны на технологии MC-CDMA [6] с использованием преобразования Уолша-Адамара.

Однако как показывают исследования, имеющиеся методы обладают рядом недостатков, среди которых является тот факт, что число абонентов является строго регламентированным и должно равняться $N = 2^k = 2, 4, 8, 16, \ldots$, а также дополнительная информация от каждого из абонентов должна встраиваться одновременно. Существенным недостатком использования технологии MC-CDMA является и дезинтегрированность разделения каналов с применяемым стеганографическим методом, т. е. технология MC-CDMA не показывает, как конкретно должно происходить встраивание и извлечение дополнительной информации.

Целью статьи является разработка методики обеспечения множественного доступа к стеганографическому каналу, обеспечивающей высокую надежность восприятия и гибкость распределения ресурсов.

Одним из эффективных способов организации множественного доступа в стеганоканале является использование технологии кодового распределения каналов MC-CDMA [6] на основе преобразования Уолша-Адамара. Технология MC-CDMA [6–7; 11] предоставляет значительную гибкость распределения ресурсов стеганоканала между пользователями. Так, для некоторых более приоритетных пользователей может быть выделено несколько каналов связи, что приведет к кратному увеличению пропускной способности стеганоканала для данных пользователей.

Однако несмотря на высокую эффективность и перспективность использования технологии кодового распределения в стеганоканалах, этот вопрос остается достаточно малоисследованным.

В литературе [4; 10] представлены лишь данные об организации отдельных случаев стеганосистем на основе технологии кодового распределения каналов MC-CDMA с числом абонентов N=4, и только на основе кодов Хаффмана, при этом фундаментальные параметры кодирования группового сигнала так же, как и вопросы оптимизации выбора числа каналов N с точки зрения минимизации значения среднего числа двоичных разрядов для представления элемента группового сигнала остаются безответными, что ставит задачу дальнейшего исследования и совершенствования этого стеганографического метода.

Рассмотрим особенности функционирования технологии MC-CDMA для организации множественного доступа в стеганоканале. Выберем для организации кодового распределения каналов ортогональное преобразование Уолша-Адамара. Несомненным преимуществом преобразования Уолша-Адамара является то, что элементы его базисных векторов принимают лишь значения бинарного алфавита $\{\pm 1\}$, что соответствует бинарной природе встраиваемой информации. Это обстоятельство вместе с простотой правил построения матриц преобразования Уолша-Адамара позволяет значительно упростить как программную, так и аппаратную реализацию алгоритмов встраивания и извлечения дополнительной информации.

Рассмотрим подробнее принципы технологии MC-CDMA, которые применяются в стеганографических системах с множественным доступом (рис. 1). Так, биты исходных данных d_i, поступающие по каждому каналу, изменяют знак одной из ортогональных функций W_i. Далее происходит умножение на некоторую константу g_i (чаще всего принимают g_i=1) и суммирование. Полученный сигнал представляет собой дополнительную информацию, которая должна быть в дальнейшем встроена в стеганосообщение [6].

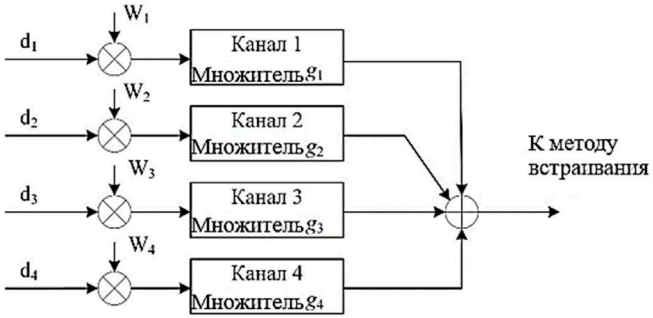

Рис. 1. Схема уплотнения каналов по технологии MC-CDMA

Рассмотрим конкретный пример. Пусть d_1=[1, 1], d_2=[-1, -1], d_3=[-1, 1], d_4=[1, -1], тогда как в качестве системы ортогональных функций выбраны функции Уолша длины $N=2^k$, упорядоченные по Адамару [3]:

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \tag{1}$$

где H_1=1.

Для нашего случая k=4. Таким образом, имеем систему функций:

$$\begin{bmatrix} W_1 = +1,+1,+1,+1; \\ W_2 = +1,-1,+1,-1; \\ W_3 = +1,+1,-1,-1; \\ W_4 = +1,-1,-1,+1. \end{bmatrix} \tag{2}$$

Выполняя преобразование (рис. 1), получаем результирующий сигнал, который подается на вход стеганографического метода для дальнейшего встраивания:

$$\begin{array}{cccccccc} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \\ \hline 0 & 0 & 0 & 4 & 0 & 4 & 0 & 0 \end{array} \tag{3}$$

Каждый пользователь, получив последовательность S=[0, 0, 0, 4, 0, 0], после извлечения из стеганосообщения на приемной стороне может выделить сообщение, которое предназначено конкретно ему в соответствии с формулой [6]:

$$d_a = \frac{\sum_{i=0}^{N} S \cdot W_a}{g_a N} \tag{4}$$

Например, можем выделить исходное сообщение, переданное по второму каналу:

$$\begin{array}{cccc} 0 & 0 & 0 & 4 \\ \times\ +1 & -1 & +1 & -1 \\ \hline 0 & 0 & 0 & -4 \end{array} \quad \times \quad \begin{array}{cccc} 0 & 4 & 0 & 0 \\ +1 & -1 & +1 & -1 \\ \hline 0 & -4 & 0 & 0 \end{array} \qquad (5)$$

Вычисляя сумму, и разделив ее на g_2N, получаем выходной сигнал d_2=[-1, -1]. В общем схема стеганосистемы с множественным доступом с использованием технологии MC-CDMA имеет вид, изображенный на рис. 2 [10].

Рассмотрим подробнее принципы функционирования устройства уплотнения каналов. В соответствии с технологией MC-CDMA биты входных данных d_i, поступающие по каждому каналу, изменяют знак одной из ортогональных функций W_i.

Исходя из выбранного вида ортогонального преобразования для построения матриц Уолша-Адамара порядка $N=2^k$, строки (столбцы) которых являются указанными функциями Уолша, будем использовать конструкцию Сильвестра [10].

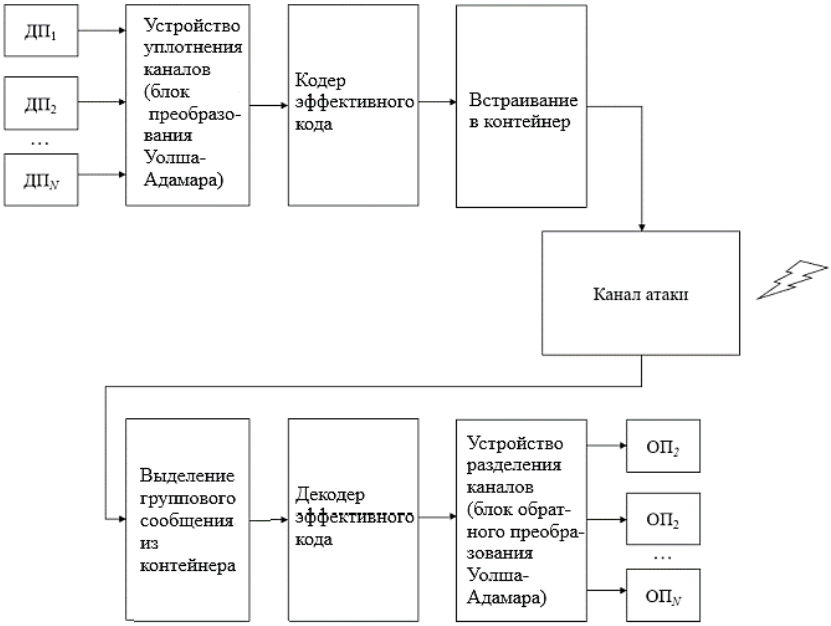

Рис. 2. Структурная схема стеганосистемы с множественным доступом с использованием технологии MC-CDMA

Таким образом, групповой сигнал, который должен быть встроен в контейнер в стеганосистемах с кодовым распределением каналов на основе технологии MC-CDMA, фактически является последовательностью коэффициентов преобразования Уолша-Адамара вектора данных от каждого из пользователей $\{d_i\}$ [8].

Это обстоятельство ведет к необходимости применения эффективного кодирования коэффициентов преобразования Уолша-Адамара для обеспечения удобства дальнейшего встраивания.

В работе [10] для осуществления операции эффективного кодирования коэффициентов преобразования Уолша-Адамара предложено использовать эффективные коды Хаффмана [2; 5], требующие предварительного сбора статистики появления символов кодируемого алфавита.

В соответствии с теорией кодирования весом Хэмминга w_1 бинарной последовательности называется количество символов «-1» в ней. Разбалансом бинарной последовательности Δ называется разность числа ее символов «+1» и «-1»:

$$\Delta = K^+ - K^- \tag{6}$$

где K^+ и K^- – число символов «+1» и «-1», соответственно, содержащихся в бинарной последовательности. Тогда множество значений {0, ±2, ..., ±*N*}, которые может принимать разбаланс Δ двоичных последовательностей, составляет множество возможных значений коэффициентов преобразования Уолша-Адамара.

Таким образом, каждый коэффициент преобразования Уолша-Адамара является разбалансом поэлементного произведения исходного кодового слова на соответствующую функцию Уолша-Адамара. Учитывая, что длина последовательности равна *N*, а все ее элементы $t_i \in \{\pm 1\}$, то разбаланс последовательности веса w_1 равен:

$$\Delta = \left(N - w_t\right) - w_t = N - 2w_t \,. \tag{7}$$

Учитывая, что возможные значения веса $w_t \in \{0,1,...,N\}$, приходим выводу, что значения разбаланса принадлежат множеству $\Delta \in \{0, \pm 2, ..., \pm N\}$.

Вероятность появления коэффициента преобразования Уолша-Адамара с заданным значением определяется как:

$$p(\omega_i) = p(-\omega_i) = \frac{C_N^{0.5(N-\omega_i)}}{2^N} \cdot \tag{8}$$

Возможные значения коэффициентов преобразования Уолша-Адамара равны значениям разбаланса последовательности Т и при-

надлежат множеству $\omega_i \in \{0, \pm 2, ..., \pm N\}$. Следовательно, количество значений первого коэффициента преобразования Уолша-Адамара равно количеству последовательностей с заданным разбалансом $J(\omega_i) = C_N^{0.5(N-\omega_i)}$.

Покажем, что это правильно для любого коэффициента преобразования Уолша-Адамара. Рассмотрим полный бинарный код мощности $J=2^N$, каждое кодовое слово которого имеет длину N:

$$\begin{matrix} [+1\ +1\ ...\ +1] \\ [+1\ +1\ ...\ -1] \\ \vdots\ \ \vdots\ \ \ \ \vdots \\ [-1\ -1\ ...\ -1] \end{matrix} \qquad (9)$$

Оставшиеся коэффициенты преобразования Уолша-Адамара находятся как значения разбалансов произведений соответствующих функций Уолша (столбца матрицы Уолша-Адамара) на последовательности из полного кода:

$$\begin{matrix} [h_N\ \ h_{N-1}\ ...\ +h_1] \\ \times\ \ \times\ \ \ \ \ \ \times \\ [+1\ \ +1\ ...\ \ +1] \\ [+1\ \ +1\ ...\ \ -1] \\ \vdots\ \ \ \vdots\ \ \ \ \ \ \vdots \\ [-1\ -1\ ...\ \ -1] \end{matrix}. \qquad (10)$$

Очевидно, что эта операция (известная в теории сигналов как построение производной системы сигналов [1]), примененная к полному коду, сохранит все его кодовые слова с точностью до их последовательности. Это обстоятельство обусловлено отсутствием столбцов полного кода, которые являются инверсией друг друга, что ведет к тому, что любое знаковое кодирование столбцов полного кода сохраняет все его кодовые слова.

Следовательно, неизменным останется и количество кодовых слов полного кода, которые имеют заданное значение разбаланса и, соответственно, частоты появления того или другого значения

коэффициентов преобразования Уолша-Адамара w_i. Учитывая, что общее количество коэффициентов преобразования Уолша-Адамара в одном векторе составляет N, то частота появления того или иного значения коэффициента преобразования Уолша-Адамара составляет $J(\omega_i) = NC_N^{0.5(N-\omega_i)}$. Следовательно, вероятность появления того или иного коэффициента преобразования Уолша-Адамара будет равна отношению частот появления данного коэффициента к общему количеству коэффициентов преобразования Уолша-Адамара полного кода:

$$p(\omega_i) = \frac{NC_N^{0.5(N-\omega_i)}}{N2^N} = \frac{C_N^{0.5(N-\omega_i)}}{2^N}.$$

Отметим также, что свойство равенства вероятностей появления равных по амплитуде, но противоположных по знаку коэффициентов преобразования Уолша-Адамара $p(\omega_i) = p(-\omega_i)$ легко доказать, раскрыв число сочетаний в числителе формулы (7):

$$p(\omega_i) = \frac{C_N^{0.5(N-\omega_i)}}{2^N} = 2^{-N} \frac{N!}{\left(\frac{N-\omega_i}{2}\right)!\left(N-\frac{N-\omega_i}{2}\right)!} = 2^{-N} \frac{N!}{\left(\frac{N-\omega_i}{2}\right)!\left(\frac{N+\omega_i}{2}\right)!}$$

и с другой стороны:

$$p(-\omega_i) = \frac{C_N^{0.5(N+\omega_i)}}{2^N} = 2^{-N} \frac{N!}{\left(\frac{N+\omega_i}{2}\right)!\left(N-\frac{N+\omega_i}{2}\right)!} = 2^{-N} \frac{N!}{\left(\frac{N+\omega_i}{2}\right)!\left(\frac{N-\omega_i}{2}\right)!}.$$

При N =16 и w_i=*2* получаем, что возможность появления данного коэффициента равна $p(2) = \frac{C_{16}^{0.5(16-2)}}{2^{16}} = \frac{C_{16}^{7}}{2^{16}} = 0.1746$, что соответствует фактически полученному результату. В соответствии с (8) вычислим остальные вероятности появления коэффициентов преобразования Уолша-Адамара для значения N=16, для каждого из которых построим кодовые слова кода Хаффмана (табл. 1).

Таблица 1

Код Хаффмана для коэффициентов преобразования Уолша-Адамара N =16

Символ	Вероятность появления	Код	Длина кодового слова
ω_0	0,1964	11	2
ω_1	0,1746	001	3
ω_2	0,1746	000	3
ω_3	0,1222	100	3
ω_4	0,1222	011	3
ω_5	0,0667	0101	4
ω_6	0,0667	0100	4
ω_7	0,0278	10100	5
ω_8	0,0278	1011	4
ω_9	0,0085	1010100	7
ω_{10}	0,0085	101011	6
ω_{11}	0,0018	101010100	9
ω_{12}	0,0018	10101011	8
ω_{13}	0,0002	10101010100	11
ω_{14}	0,0002	1010101011	10
ω_{15}	0,0000153	101010101011	12
ω_{16}	0,0000153	101010101010	12

Анализ представленных в табл. 1 данных приводит к выводу, что средняя длина кодового слова, необходимого для передачи одного коэффициента преобразования Уолша-Адамара, при количестве разделяемых каналов N=16, составляет l_{av} = 3.1041.

Нетрудно рассчитать l_{av} и для других значений N. Тем не менее зависит от особенностей кода Хаффмана. Согласно теореме Шеннона о кодировании источника [9] средняя длина кодового слова,

необходимая для кодирования символа его алфавита, не превышает информационную энтропию данного алфавита $l_{av} \geq H\left(\{\omega_i\}\right)$:

$$H\left(\{\omega_i\}\right)_N = -\sum_{i=0}^{N} p\left(\omega_i\right)\log_2 p\left(\omega_i\right). \qquad (11)$$

Таким образом, при произвольном значении N имеем следующее неравенство:

$$l_{av} \geq -\sum_{i=0}^{N} \frac{C_N^{0.5(N-\omega_i)}}{2^N}\log_2 \frac{C_N^{0.5(N-\omega_i)}}{2^N}, \quad \omega_i = 0, \pm 2, ..., \pm N - 1 \qquad (12)$$

При заданном N правая часть выражения (12) составляет нижнюю границу количества двоичных разрядов, необходимых для кодирования одного коэффициента преобразования Уолша-Адамара.

Для наглядности на рис. 3 построен график зависимости средней длины кодового слова Хаффмана, необходимый для кодирования одного коэффициента преобразования Уолша-Адамара, а также информационной энтропии (12) от количества разделяемых каналов N.

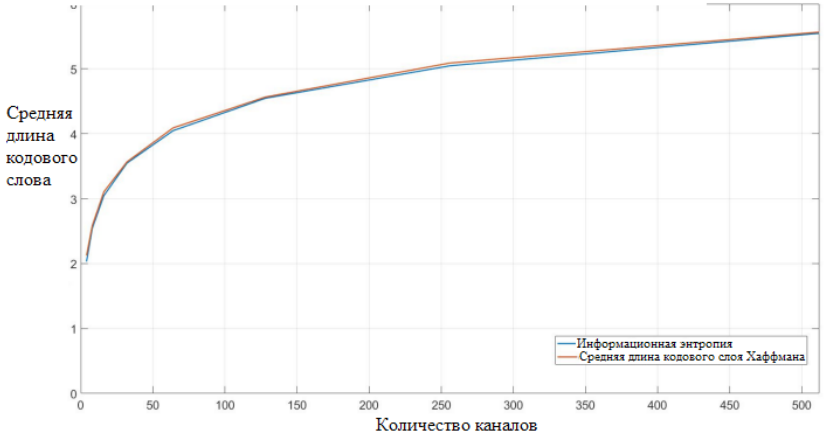

Рис. 3. График зависимости средней длины кодового слова от количества разделяемых каналов

Анализ данных рис. 3 свидетельствует о нарастании средней длины кодового слова при возрастании количества N разделяемых каналов, что говорит о возрастании избыточности в представлении передаваемой информации при увеличении числа разделяемых каналов с помощью технологии MCCDMA.

Проведенные исследования позволили установить, что при значении количества разделяемых каналов N=4, применение эффективного кода Хаффмана не является наиболее эффективным способом кодирования коэффициентов преобразования Уолша-Адамара. Установлено, что для повышения эффективности кодирования коэффициентов преобразования Уолша-Адамара может быть использован специальный класс совершенных алгебраических конструкций – бент-последовательностей.

Бинарная последовательность $B = [b_0, b_1, \ldots b_i, \ldots b_{N-1}]$, где $b_i \in \{\pm 1\}$ – коэффициенты, парной длины $N=2^k$, $i=0,1,\ldots,N-1$, N – порядок матрицы Уолша-Адамара, называется бент-последовательностью (БП), если она имеет равномерный по модулю спектр Уолша-Адамара $W_B(w)$, который представим в матричной форме:

$$S_B(\varpi) = BH, \ \varpi = 0,1,\ldots,N-1, \tag{13}$$

где H – матрица Уолша-Адамара порядка N.

Исходя из определения, каждый коэффициент преобразования Уолша-Адамара бент-последовательности $S_B(\varpi = 0), S_B(\varpi = 1), \ldots, S_B(\varpi = N-1)$ принимает значения из множества $\{\pm\sqrt{N}\}$. Таким образом, вектор коэффициентов преобразования Уолша-Адамара бент-последовательности является, по своей сути, бинарной последовательностью, отображенной на алфавит $\{\pm\sqrt{N}\}$, так как каждый его элемент приобретает лишь одно из двух возможных значений, отличающихся знаком. Понятно, что коэффициенты преобразования Уолша-Адамара бент-последовательности являются исключительно удобными для встраивания информации в контейнер. Тем не менее бент-последовательности являются крайне непредсказуемыми и сложными математическими объектами из-за своей максимально возможной нелинейности.

В случае N=4 имеем уникальную ситуацию, когда половина всех последовательностей являются бент-последовательностями, т. е. удовлетворяют условиям (13). Данный факт может быть использован для увеличения количества информации, встраиваемой в контейнер в стеганосистемах с кодовым распределением каналов при N=4 следующим образом: групповой сигнал может быть подвергнут преобразованию с помощью C-кода еще до нахождения его коэффи-

циентов преобразования Уолша-Адамара. *С*-кодом называется код, каждое кодовое слово которого имеет заданное (обычно минимально возможное) значение пик-фактора κ, который определяется как:

$$\kappa = \frac{P_{\max}}{P_{av}} = N^{-1} \max_{t} \left\{ \left| S_c(t) \right|^2 \right\}, \qquad (14)$$

где $P_{\max}$ – максимальная мощность сигнала $S_c(t)$, P_{av} – средняя мощность сигнала $S_c(t)$. С-коды могут успешно использоваться в стеганографических системах, основанных на технологии MC-CDMA.

Таким образом, схема стеганосистемы с распределением каналов с использованием технологии MC-CDMA (рис. 2) приобретает вид, показанный на рис. 4.

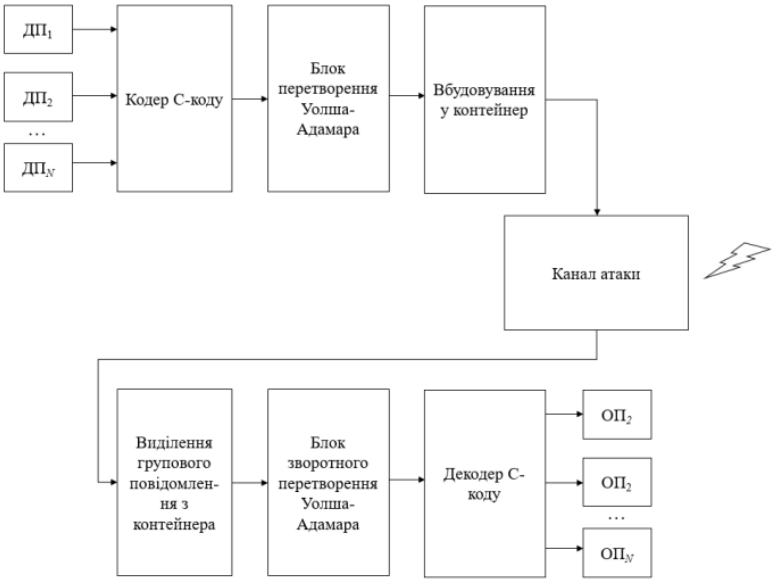

Рис. 4. Схема стеганосистемы с использованием технологии MC-CDMA и С-кода с использованием С-кода

Таким образом, по сравнению с использованием кода Хаффмана для кодирования коэффициентов преобразования Уолша-Адамара предложенный код позволяет упаковывать коэффициенты Уолша-Адамара на 6,25 % эффективнее. В отличие от случая использования кода Хаффмана для кодирования коэффициентов

преобразования Уолша-Адамара, предложенный код позволяет детектировать как минимум одну ошибку, что подтверждает целостность встроенной информации.

Список литературы:

1. *Горбенко И. Д. [и др.].* Метод синтеза производных систем сигналов на основе криптографических дискретных последовательностей символов // Радиотехника. 2017.
2. *Мазурков М. И.* Основы теории передачи информации. Одесса: Наука и Техника, 2005.
3. *Цветков К. Ю., Федосеев В. Е., Коровин В. М., Абазина Е. С.* Модель кодера скрытого канала с кодовым уплотнением с использованием сигнальных последовательностей Франка-Уолша, Франка-Крестенсона // Труды Научно-исследовательского института радио. 2015. № 1.
4. *Amirtharajan R., Rayappan J.* B. B. Covered CDMA multi-user writing on spatially divided image. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011.
5. *Mc Eliece R.* The theory of information and coding // Cambridge University Press, 2002.
6. *Paterson K. G.* On codes with low peak-to-average power ratio for multicode CDMA. HP LaboratoriesTechnicalReport HPL. 2001
7. *Paterson K. G.* Sequences for OFDM and Multi-code CDMA: two problems in algebraic coding theory, Sequences and their applications // Proc. Berlin: Springer, 2002.
8. *Schmidt K.* Quaternary Constant-Amplitude Codes for Multicode CDMA, IEEE International Symposium on Information Theory. Nice, 2007.
9. *Shannon C. E.* A Mathematical Theory of Cryptography. USA: Bell System Technical Memo, 1945.
10. *Sheidaeian H., Zolfaghari B., Zobeiri M.* An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. V. 2.
11. *Wada T., Yamazato T., Katayama M., Ogawa A.* A constant amplitude coding for orthogonal multi-code CDMA systems. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences. 1997. V. 80.

Игорь Анатольевич Кубасов,
доктор технических наук, доцент,
профессор кафедры информационных технологий
Академия управления МВД России
E-mail: igorak@list.ru

УДК: 004.838.2

Роль инновационных информационных технологий в цифровой трансформации МВД России

Аннотация

Актуальность определения роли и места инновационных информационных технологий в современной цифровой трансформации МВД России как никогда важна и обусловлена социальными, технологическими и организационными факторами. Рассмотрено применение инновационных информационных технологий, обеспечивающих подразделениям МВД России возможность адаптироваться к меняющимся условиям и эффективно выполнять свои функции и задачи по охране общественного порядка и обеспечению общественной безопасности. Обоснован вывод о ключевой роли инновационных информационных технологий в успешной реализации цифровой трансформации МВД России.

Ключевые слова и словосочетания: *искусственный интеллект; цифровая трансформация; инновационные технологии; охрана общественного порядка; обеспечение общественной безопасности.*

Актуальность определения роли и места инновационных информационных технологий[1] в современной цифровой трансформации МВД России как никогда важна и обусловлена различными факторами. Эти факторы можно разделить на три основные категории: социальные, технологические и организационные.

С социальной точки зрения актуальность определения роли и места инновационных информационных технологий в успешной реализации цифровой трансформации МВД России можно оценить

[1] Примеры инновационных информационных технологий: большие данные; нейротехнологии и искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; промышленный интернет; компоненты робототехники и сенсорика; технологии беспроводной связи; технологии виртуальной и дополненной реальностей.

с учетом меняющихся потребностей и ожиданий граждан. Реализация цифровой трансформации может помочь оправдать эти ожидания, а ведомству предоставлять эффективные и ориентированные на граждан государственные услуги, в том числе цифровые.

Кроме того, цифровая трансформация может повысить прозрачность и подотчетность деятельности подразделений МВД России. Оцифровывая процессы и внедряя передовые технологии, министерство может обеспечить лучший доступ к информации для граждан, способствовать открытому управлению и обеспечить более прозрачную и подотчетную систему, что укрепляет доверие к органам внутренних дел и их деятельности.

С технологической точки зрения актуальность определения роли и места инновационных информационных технологий можно оценить, исследовав современные технологические достижения и их потенциал для повышения эффективности оперативно-служебной деятельности подразделений МВД России. Такие технологии, как искусственный интеллект, анализ больших данных, робототехника, облачные вычисления и многие другие могут позволить оперативно обрабатывать и анализировать огромные объемы данных, принимать решения на основе данных и существенно повышать эффективность правоохранительной деятельности.

Более того, успешная реализация цифровой трансформации обеспечит повышение уровня технологической независимости ведомственной информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств, повышение уровня кибербезопасности. Поскольку киберугрозы продолжают развиваться и становиться все более изощренными в современных условиях, для ведомства крайне важно инвестировать в передовые технологии и системы для защиты конфиденциальных данных и инфраструктуры.

С организационной точки зрения актуальность внедрения и развития инновационных информационных технологий можно определить с учетом текущих оперативных задач, стоящих перед подразделениями МВД России. Например, имеются устаревшие информационные системы, неэффективные и дорогостоящие в обслуживании. Реализация цифровой трансформации обеспечит модернизацию этих систем, оптимизацию процессов и повышение операционной эффективности.

Кроме того, цифровая трансформация МВД России позволит улучшить взаимодействие между его различными подразделениями и другими ведомствами. Внедряя цифровые платформы и инструменты, министерство может облегчить обмен информацией, опти-

мизировать рабочие процессы и улучшить процессы принятия решений, что в конечном итоге существенно повысит эффективность оперативно-служебной деятельности.

Повышая удовлетворенность граждан государственными услугами, в том числе цифровыми, снижая издержки государственного управления, повышая уровень надежности и безопасности информационных систем, уровень технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств, внедрение и развитие инновационных информационных технологий обеспечат адекватное противодействие современной преступности [9].

Следует отметить, что внедрение и развитие инновационных информационных технологий направлено на существенное повышение эффективности деятельности подразделений МВД России по предотвращению преступности и обеспечению общественного правопорядка. Эти технологии включают в себя широкий спектр инструментов и систем, которые позволяют собирать, анализировать и использовать данные способами, которые ранее были невообразимы [2].

Далее рассмотрим основные инновационные информационные технологии, которые произвели революционное преобразование в деятельности подразделений МВД России.

1. Большие данные – технология, применяемая для прогнозирования тенденций преступности и оптимального распределения сил и средств. Анализируя статистические данные о преступности, демографическую информацию, погодные условия и другие соответствующие факторы, органы внутренних дел могут определять районы и времена повышенного риска, что позволяет выявлять закономерности, тенденции и аномалии, разрабатывать упреждающие стратегии полиции, раскрывать и расследовать преступления [6; 10]. Например, мониторинг и анализ социальных сетей помогает органам внутренних дел выявлять потенциальные угрозы и оперативно их купировать [5].

2. Технология геоинформационных систем (ГИС) позволяет создавать карты преступности в режиме реального времени, на которых отображаются горячие точки и тенденции преступности. Этот инструмент помогает органам внутренних оперативно реагировать на инциденты.

3. Технологии искусственного интеллекта поддерживают процессы расследования, улучшают процесс принятия решений и оптимизируют распределение ресурсов. Так, например, техноло-

гия распознавания лиц помогает органам выявлять подозреваемых, определять местонахождение пропавших без вести лиц и повышать безопасность на публичных мероприятиях. Технология обработки естественного языка помогает идентифицировать подозреваемых, анализировать улики и извлекать информацию из различных источников. Эти технологии существенно ускоряют процессы расследования и расширяют возможности принятия решений [4; 8–9; 11].

4. Интернет вещей – технология, позволяющая интегрировать такие устройства, как камеры наблюдения и датчики, эффективно контролировать общественные места. Сбор и анализ данных в режиме реального времени способствуют повышению общественной безопасности и реагированию на чрезвычайные ситуации [3].

5. Блокчейн – технология, обеспечивающая безопасное хранение данных и аутентификацию, повышая прозрачность и целостность различных операций с данными.

6. Технологии виртуальной реальности и дополненной реальности используют для обучения и совершенствования навыков, повышения ситуационной осведомленности сотрудников при решении оперативно-служебных задач [1].

7. Мобильные технологии предоставляют сотрудникам полиции возможность получать оперативно удаленный доступ к информации, взаимодействовать в режиме реального времени.

8. Облачные вычисления – технология, обеспечивающая хранение данных, обмен между собой и с другими правоохранительными органами.

9. Робототехника применяется для наблюдения, поисково-спасательных операций, управления дорожным движением и мониторинга крупных событий. Беспилотные летательные аппараты повышают осведомленность о ситуации, сокращают время реагирования и оказывают ценную поддержку в критических ситуациях [7; 12].

10. Технологии расследования киберпреступлений применяются как специализированные инструменты для цифровой криминалистики, сетевого анализа и анализа киберугроз.

Следовательно, можно заключить, что инновационные информационные технологии играют ключевую роль в цифровой трансформации МВД России, давая органам внутренних дел возможность адаптироваться к меняющимся условиям, эффективно выполняя свои функции и задачи по охране общественного порядка и обеспечению общественной безопасности.

Инновационные информационные технологии обеспечивают существенные преимущества органам внутренних дел, революционизируя их оперативную эффективность. Дальнейшее развитие

и интеграция инновационных информационных технологий имеют огромный потенциал для повышения оперативных возможностей подразделений МВД России.

Список литературы:

1. *Кубасов И. А.* Виртуальная и дополненная реальность: технологии, революционизирующие методы работы предприятий // Первая миля. 2023. № 5 (113).

2. *Кубасов И. А.* Искусственный интеллект как драйвер цифровой трансформации МВД России // Криминологический журнал. 2023. № 2.

3. *Кубасов И. А.* Промышленный Интернет вещей как революционный скачок развития // Надежность и качество сложных систем. 2023. № 2 (42).

4. *Кубасов И. А.* Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений // Вестник Воронежского института МВД России. 2022. № 2.

5. *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).

6. *Кубасов И. А., Лекарь Л. А.* Поиск и анализ больших данных в социальных сетях и Интернете для информационно-аналитического обеспечения оперативно-розыскной деятельности // Оперативно-розыскной портал: право и технологии. 2022. № 2 (2).

7. *Кубасов И. А., Пучков Г. Ю.* Анализ технических решений в области организации оперативной радиосвязи и особенности использования беспилотных летательных аппаратов в интересах органов внутренних дел Российской Федерации // Известия ЮФУ. Технические науки. 2012. № 3 (128).

8. *Кубасов И. А., Стрельников Ф. И., Лунев Ю. С.* Вопросы повышения эффективности использования автоматизированных дактилоскопических учетов при раскрытии и расследовании преступлений // Вестник Воронежского института МВД России. 2020. № 2.

9. *Кубасов И. А., Щетников А. В.* О реализации федерального проекта «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации» в сфере внутренних дел / под ред. И. Г. Чистобородова // Цифровая трансформация системы МВД России: сборник научных статей по материалам

Международного форума. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2022.

10. *Кубасов И. А., Лекарь Л. А., Кондрущенков О. М.* Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-розыскной деятельности: сборник статей Международной научно-практической конференции / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. 2020.

11. *Кубасов И. А., Ливанский А. Г., Пучков Г. Ю.* К вопросу о внедрении средств интеллектуального видеонаблюдения в деятельность органов внутренних дел Российской Федерации. Вестник МВД России. 2022. № 5.

12. *Кубасов И. А., Сушков В. И.* Применение технологий искусственного интеллекта в робототехнических комплексах специального назначения в целях обеспечения правоохранительной деятельности // Вестник Воронежского института ФСИН России. 2022. № 3.

Игорь Анатольевич Кубасов,
доктор технических наук, доцент,
профессор кафедры информационных технологий
Академия управления МВД России
E-mail: igorak@list.ru

Артем Викторович Кирюхин,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: nokia26340@mail.ru

УДК 004.832.2

Искусственный интеллект на службе органов внутренних дел Российской Федерации

Аннотация

В статье идет речь о современных возможностях и перспективах использования искусственного интеллекта в деятельности органов внутренних дел Российской Федерации, акцентируя внимание на его применении для обеспечения общественной безопасности.

Ключевые слова и словосочетания: *искусственный интеллект; органы внутренних дел.*

Органы внутренних дел Российской Федерации несут ответственность за обеспечение общественной безопасности и должны направлять усилия на ее обеспечение. Чтобы продолжать эффективное обеспечение общественной безопасности, органы внутренних дел Российской Федерации (далее – ОВД) активно внедряют современные достижения науки и техники в свою деятельность. Технический прогресс позволяет сотрудникам ОВД использовать беспрецедентные информационные технологии в оперативно-служебной деятельности. Существует множество сфер деятельности, в которых сотрудники ОВД могут положиться на информационные технологии [1; 3]. Также прорывным информационным технологиям в деятельности ОВД уделяется огромное внимание как со стороны руководства МВД России, так и со стороны руководства РФ.

Использование искусственного интеллекта (далее – ИИ) становится все более важными аспектом для деятельности ОВД. Крайне

эффективно использование ИИ в области предотвращения и прогнозирования преступности, что следует из отчетов правоохранительных органов некоторых стран[1]. Предиктивная деятельность является лишь одним из результатов этого сдвига.

Использование систем видеонаблюдения стало важным аспектом в области раскрытия преступлений[2]. Даже при низком качестве записей с систем видеонаблюдения ИИ способен выявлять личность преступников и пропавших без вести лиц, обрабатывая при этом значительные объемы данных, на обработку которых человеком понадобилось бы больше времени. В тоже время ИИ может распознать лиц, которых люди обычно не могут обнаружить, например, найти лицо в толпе на стадионе.

Однако применение ИИ не ограничивается только распознаванием лиц. Эта технология также может использоваться для распознавания объектов и анализом сложных сценариев, таких как автомобильные аварии, появление оружия, закладка наркотических средств и т. д. Распознавание объектов особенно важно для ОВД, например, во время проведения массовых мероприятий. ИИ может подать сигнал тревоги в центр принятия решений, если кто-то в районе проведения мероприятия имеет потенциальную угрозу. Кроме того, ИИ может эффективно работать с данными, получаемыми с камер беспилотных летательных аппаратов, позволяя ОВД осуществлять мониторинг больших территорий.

ИИ может играть ключевую роль в прогнозировании преступлений для ОВД, предсказывая потенциальные преступления. ИИ может осуществлять детальный анализ, учитывая большое число критериев, криминальной активности по различным районам, создавая карты зон с высоким уровнем преступности. ИИ также сможет определять, кто рискует совершить преступление, а кто, скорее всего, совершит повторное преступление после выхода из тюрьмы, на основе собранных данных и анализа закономерностей. Это даст возможность более эффективно распределить силы и средства ОВД РФ [2].

Кроме того, ИИ может быть использован в расследовании ненасильственных преступлений. Анализируя финансовые операции на предмет аномалий и необычных паттернов, ИИ поможет выявить подозрительные транзакции. Его способность идентифициро-

---

[1] URL: https://www.soundthinking.com/law-enforcement/resource-deployment-resourcerouter/ (дата обращения: 01.03.2024).

[2] URL: https://alrf.ru/news/sistema-videonablyudeniya-pomogaet-raskryvat-bolee-60-prestupleniy-mintsifry/ (дата обращения: 01.03.2024).

вать поддельные товары и денежные банкноты, обращая внимание на детали, которые могут ускользнуть от человеческого взгляда.

ИИ может внедряться для выявления фальсификации документов. Обучение на массиве данных, содержащем подлинные и фальшивые документы, позволят ИИ обнаруживать малейшие отклонения и аномалии, которые недоступны для визуального восприятия человека. Сравнивая документы с эталонными образцами, ИИ сможет анализировать типографские особенности и качество бумаги, эффективно адаптируясь к новым методам фальсификации. Использование такого подхода сделает ИИ ценным инструментом в арсенале ОВД.

Благодаря расширенным возможностям визуализации, распознаванию объектов и лиц, а также адаптивности ИИ снижает потребность в трудоемких задачах и освобождает сотрудников ОВД для выполнения более сложных действий. ИИ также может выявить лиц, совершивших преступления, которым в противном случае это сошло бы с рук, и раскрывать преступления, которые в противном случае остались бы незамеченными. Однако важно позаботиться о том, чтобы алгоритм работы такой системы был рациональным и прозрачным. Многие исследователи придерживаются мнения, что на международном уровне необходимо создать комитет по регулированию использования ИИ. Еще один аспект, который необходимо решить, – это обеспечение прав граждан. Становится совершенно очевидным, что сотрудникам ОВД потребуется дополнительная помощь со стороны искусственного интеллекта, что особенно актуально в условиях кадрового дефицита.

Список литературы:

1. *Кубасов И. А.* Проблемные вопросы применения технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации // Вестник Воронежского института МВД России. 2021. № 3.

2. *Кубасов И. А.* Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений // Вестник Воронежского института МВД России. 2022. № 2.

3. *Овчинский В.* Искусственный интеллект для полиции: справедливость, преемственность, прозрачность, пропорциональность. URL: http://zavtra.ru/blogs/iskusstvennij_intellekt_dlya_politcii (дата обращения: 01.03.2024).

Игорь Анатольевич Кубасов,
доктор технических наук, доцент,
профессор кафедры информационных технологий
Академия управления МВД России
E-mail: igorak@list.ru

Виктор Андреевич Рогожкин,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: vrogozhkin@internet.ru

УДК 343.34

Геоданные и геоинформационные технологии в деятельности подразделений участковых уполномоченных полиции

Аннотация

В статье исследованы проблемные вопросы в деятельности подразделений участковых уполномоченных полиции и пути их решения в целях повышения эффективности оперативно-служебной деятельности. Обоснована целесообразность внедрения геоданных и геоинформационных технологий в оперативно-служебную деятельность подразделений участковых уполномоченных полиции. Определены перспективные способы наполнения сведений в электронный паспорт административного участка с использованием современных информационно-телекоммуникационных технологий. Выработаны предложения по совершенствованию модуля «Участковый» сервиса охраны общественного порядка ИСОД МВД России.

Ключевые слова и словосочетания: *геоданные; геоинформационные технологии; геоинформационные системы; участковый уполномоченный полиции; модуль «Участковый».*

На протяжении столетия служба участковых уполномоченных полиции (далее – УУП) является одной из основополагающих в системе МВД России. За весь период своего существования не только служба УУП претерпела изменения, но и формы и методы анализа, планирования и контроля за деятельностью этих подразделений. С быстрым развитием и применением информационно-теле-

коммуникационных технологий в обществе и органах государственной власти технический прогресс коснулся и службы УУП. Так, в соответствии с требованиями приказа МВД России от 31 декабря 2012 г. № 1166 участковый пункт полиции уже оснащался вычислительной и организационной техникой. Однако внесение сведений в паспорт административного участка, паспорт жилого дома и журнал учета приема граждан, их обращений и заявлений по-прежнему происходило в ручном режиме на бумажных носителях [3].

Новым этапом в совершенствовании отчетной документации УУП было введение в эксплуатацию модуля «Участковый» сервиса охраны общественного порядка ИСОД МВД России[1]. Появилась возможность накапливать информацию из физических носителей (бумажных журналов) в электронный паспорт административного участка. Объектами учета также остались профилактируемые лица шести категорий, несовершеннолетние, объекты недвижимости и жилые дома с их жильцами и др.

В целях совершенствования организации деятельности подразделений участковых уполномоченных полиции был принят приказ МВД России от 29 марта 2019 г. № 205, в соответствии с которым:

– участковый уполномоченный полиции обязан размещать результаты обхода административного участка, профилактической работы с подучетными и результаты рассмотрения обращений граждан в электронный паспорт административного участка;

– начальник подразделения УУП обязан ежеквартально контролировать полноту, регулярность и достоверность пополнения электронного паспорта административного участка с проставлением соответствующей отметки;

– упразднены журналы на бумажных носителях [2].

Переход от бумажных носителей результатов профилактической работы к электронным не только автоматизирует оперативно-служебную деятельность самого УУП, но и переводит в цифровое поле деятельность руководителя подразделения по контролю за его подчиненными.

---

[1] ИСОД МВД России – Единая система информационно-аналитического обеспечения деятельности МВД России.

[2] О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности (вместе с «Инструкцией по исполнению участковым уполномоченным полиции служебных обязанностей на обслуживаемом административном участке», «Наставлением по организации службы участковых уполномоченных полиции») [Электронный ресурс]: приказ МВД России от 29 марта 2019 г. № 205. Доступ из справ.-правовой системы «КонсультантПлюс».

В настоящий момент цифровым инструментом контроля руководителя подразделения участковых уполномоченных полиции в едином цифровом пространстве является СООП ИСОД МВД России.

С целью повышения эффективности основного инструмента оперативного контроля со стороны руководителя подразделений участковых уполномоченных полиции с применением современных информационно-телекоммуникационных технологий в данной статье рассмотрена перспектива широкого внедрения геоинформационных систем (далее – ГИС).

Будем рассматривать ГИС как аппаратно-программное обеспечение, позволяющее вести поиск, сбор, обобщение, пространственный анализ и преобразование цифровой информации о пространственных объектах в графическую [1].

Иными словами, руководителю подразделения участковых уполномоченных полиции предлагается предоставить аппаратно-программное обеспечение, позволяющее в реальном времени:

Во-первых, на базе системы позиционирования «ГЛОНАСС» контролировать исполнение служебных обязанностей на обслуживаемом административном участке участкового уполномоченного полиции, его фактическое нахождение на территории обслуживания; контролировать передвижение служебных транспортных средств.

Во-вторых, решать задачи самого оптимального маршрута обхода обслуживаемого административного участка участковым уполномоченным полиции. Специализированное программное обеспечение позволит рассчитать, к примеру, кратчайший маршрут посещения нескольких профилактируемых лиц участковым уполномоченным полиции. Сократится время, затрачиваемое на выполнения своих должностных обязанностей участковым уполномоченным полиции, а в случае эксплуатации служебных транспортных средств еще и экономится горюче-смазочные материалы.

В-третьих, получать сведения об объектах недвижимости, находящихся на территории обслуживания. Данный инструмент позволит осуществить выгрузку сведений об объектах органов государственной власти, коммерческих организаций, критической инфраструктуры и др. непосредственно в паспорт административного участка, их визуализация и в последующем использование полученной информации в оперативно-служебной деятельности.

В-четвертых, визуализировать всю имеющуюся оперативную информацию; расположить подвижные и стационарные объекты

на виртуальной карте и взаимодействовать с ними через автоматизированное рабочее место руководителя [4].

Перспективной задачей дальнейшего развития ИСОД МВД России является интеграция в нее геоинформационной системы для формирования банка геоданных, позволяющего использовать программное обеспечение как для создания самостоятельных решений, так и для ее интеграции в информационные системы единого информационного пространства [2].

Внедрение в модуль «Участковый» СООП ИСОД МВД России предложенных инструментов на базе ГИС позволит не только повысить эффективность контрольных функций руководителя подразделения УУП, но и всех функций управления УУП.

Список источников

1. *Зоткин С. А., Зайчик Е. М., Кубасов И. А.* О применении геоинформационных технологий в управлении войсками (силами) // Военная мысль. 1999. № 2.

2. *Кубасов И. А.* Проблемные вопросы и направления развития единой системы информационно-аналитического обеспечения деятельности МВД России // Охрана, безопасность, связь. 2020. № 5-3.

3. *Кубасов И. А.* Развитие и внедрение информационных технологий в деятельности органов внутренних дел: сборник научных статей Всероссийской научно-практической конференции // Информационные технологии в деятельности органов внутренних дел. Москва: Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя, 2023.

4. *Шапкин А. В., Кубасов И. А.* Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 годы. Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции / ответств. за вып. В. О. Лапин. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2019.

Иосиф Николаевич Кур,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: xviperrus@vk.com

УДК: 342.7, 343.3/.7

Правовое обеспечение оборота конфиденциальной информации как направление информационной безопасности

Аннотация

В настоящей статье автором исследуются вопросы правового обеспечения оборота конфиденциальной информации. Данная сфера правового регулирования рассматривается через призму информационной безопасности. Путем изучения действующего законодательства Российской Федерации в данной сфере выделяется авторская классификация видов информации, основанной по степени доступности, а также выделяются признаки конфиденциальной информации. Результатом является приведение авторского понятие последней. Кроме того, раскрывается содержание уголовно-правовой охраны сферы оборота конфиденциальной информации, затрагивающей широкий спектр охраняемых уголовным законом общественных отношений. В статье приводятся аргументы, акцентирующие внимание на проблемах в правовом обеспечении указанной сферы, неучтенность которых может привести к трудностям в правоприменительной деятельности. Такие трудности прямым образом оказывают влияние на состояние информационной безопасности в рассматриваемой сфере.

Ключевые слова и словосочетания: *конфиденциальная информация; правовое обеспечение; информационная безопасность; преступление; уголовный закон.*

Процессы информатизации и информационной интеграции в жизни личности, общества, государства играют существенную роль на сегодняшний день. В связи с чем актуализируется вопрос об обеспечении информационной безопасности организационными, техническими, а также правовыми средствами упомянутых выше субъектов.

Если не первостепенным, то немаловажным направлением информационной безопасности является обеспечение оборота конфиденциальной информации. Данный тезис подтверждается положением п. «ж» ст. 23 Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 (далее – Доктрина)[1]. В соответствии с данным положением обеспечение оборота конфиденциальной информации является одним из основных направлений информационной безопасности в области государственной и общественной безопасности.

Однако упомянутое положение Доктрины является лишь следствием многолетнего развития правового обеспечения оборота конфиденциальной информации как одного из направлений информационной безопасности. В связи с чем возникает необходимость в изучении данного направления деятельности общества и государства в контексте правового регулирования.

Необходимо сказать, что развитие правового регулирования в сфере обеспечения оборота конфиденциальной информации прямым образом обусловливается процессами цифровой трансформации в России. В связи с чем происходит осознание важности информации в жизни личности, общества, государства как следствия, которое находит свое отражение в закреплении ряда информационных положений в системе конституционного правового регулирования.

Общеизвестно, что Конституция Российской Федерации устанавливает пределы того правового пространства, в котором развивается правовая система Российской Федерации, система ее законодательства [13, с. 46.]. Анализ конституционных положений позволяет констатировать тот факт, что в Основном законе Российской Федерации содержится по крайней мере 10 статей информационного характера, среди которых 3 – имеют прямое отношение к вопросам оборота конфиденциальной информации. В свою очередь, изучение конституционно-правовых положений позволяют сделать вывод о том, что государством создана исходная правовая регламентация рассматриваемой сферы, на основе которой возникает соответствующее Основному закону Российской Федерации правовое обеспечение [12, с. 44–54.], направленное, с одной стороны, «охранять»

[1] Доктрина информационной безопасности Российской Федерации: утв. Указом Президента Рос. Федерации от 5 декабря 2016 г. № 646 // Российская газета: сайт. URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 22.03.2024).

информацию (в том числе конфиденциальную) от незаконных действий в ее отношении, с другой – охранять общество от негативных деяний с использованием информации, заключающихся, главным образом, в недопущении ее фальсификации.

Результатом конституционно-правового регулирования в сфере информации стало принятие в 1995 г. закона «Об информации, информатизации и защите информации»[1]. Названный документ, помимо понятия «информация» (ст. 2), категоризации видов информации по степени доступности (ст. 10), содержал категорию «конфиденциальная информация», под которой понималась только документированная информация, доступ к которой был ограничен в соответствии с законодательством Российской Федерации (п. 8 ст. 2). Однако с течением времени ввиду потребностей времени изменился и подход к правовому обеспечению информационной сферы, как следствие, сферы оборота конфиденциальной информации. В 2006 г. был принят Закон «Об информации, информационных технологиях и о защите информации» (далее – ФЗ Об информации)[2].

Вновь принятый закон дал иное понятие информации. Теперь под ней понимаются сведения (сообщения, данные) независимо от формы их представления (п. 1 ст. 2). Тем самым законодатель установил, что информация может быть не только документальной, но и, например, вербальной. Новый закон отказался от термина «конфиденциальная информация», указав на «конфиденциальность» информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ст. 2). Таким образом, законодатель сместил «центр тяжести» с сущности конфиденциальности на ее содержание, а именно на правила и особенности оборота такой информации, т. е. на его правовой режим.

В свою очередь, разнообразился подход законодателя к видам информации, регламентированных ФЗ Об информации. Согласно действующему закону информация подразделяется на 4 вида в зависимости от порядка ее предоставления или распространения: 1) информацию, свободно распространяемую; 2) информацию,

---

[1] Об информации, информатизации и защите информации: Федер. закон от 20 февраля 1995 г. № 24-ФЗ // СЗ РФ от 20 февраля 1995 г. № 8. Ст. 609 (утратил силу ФЗ от 27 июля 2006 г. № 149-ФЗ).

[2] Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 29.12.2022) // СЗ РФ от 31 июля 2006 г. № 31. Ч. I. Ст. 3448.

предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению; 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается (ч. 3 ст. 5). Учитывая названные новеллы в сфере оборота конфиденциальной информации (в частности, переход к конфиденциальности информации, выступающей в качестве правового режима), путем расширительного толкования *epistula legis* (от лат. «буквы закона») можно уловить *spiritus legis* (от лат. «дух закона») и на основании идеи, заложенной в ч. 3 ст. 5, ст. 9, ч. 6 и 7 ст. 10 ФЗ Об информации, подразделить информацию, распространение которой в Российской Федерации ограничивается или запрещается (п. 4 ч. 3 ст. 5 ФЗ Об информации) на несколько подвидов:

1. Запрещенная информация.

2. Информация ограниченного характера, подразделяемая на:

2.1. Иную информацию ограниченного характера;

2.2. Конфиденциальную информацию, которая подразделяется на несколько подвидов:

2.2.1. Сведения конфиденциального характера[1];

2.2.2. Государственная тайна[2].

Не вдаваясь в подробности деталей классификации, следует отметить, что последняя определяется по признаку «степени доступности информации», а также на основе анализа действующего законодательства Российской Федерации в сфере оборота конфиденциальной информации. Кроме того, в науке не существует единого подхода к классификации конфиденциальной информации [1, с. 3.]. В свою очередь, виды конфиденциальной информации, представленные выше, имея достаточно много общего, имеют совокупность признаков, по которым становится возможным их разграничение. Прежде всего по их предмету. Если предметом государственной тайны являются сведения, изложенные в ст. 5 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»

[1] Об утверждении Перечня сведений конфиденциального характера: утв. Указом Президента Рос. Федерации от 6 марта 1997 г. № 188 (последняя редакция) // Официальный сайт Президента Рос. Федерации: сайт. URL: http://www.kremlin.ru/acts/bank/10638 (дата обращения: 23.03.2024).

[2] О государственной тайне: Закон Рос. Федерации от 21 июля 1993 г. № 5485-I (последняя редакция) // Официальный интернет-портал правовой информации: сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102025035 (дата обращения: 23.03.2024).

(далее – Закон О государственной тайне)[1], то предметом сведений конфиденциального характера являются иные данные, отнесенные к конкретному виду конфиденциальной информации. Другим признаком разграничения являются интересы субъектов правоотношений. В частности, государственная тайна затрагивает прежде всего интересы безопасности Российской Федерации в политической, экономической и иных сферах. В свою очередь, сведения конфиденциального характера затрагивают отдельные интересы в различных по своему содержанию и виду сферах и прежде всего отдельных субъектов, а не государственной безопасности в целом. Третьим признаком разграничения представленных выше категорий является ущерб, причиняемый в результате посягательства на охраняемый интерес. Если разглашением (т. е. нарушением правового режима ее оборота) государственной тайны причиняется существенный ущерб ее безопасности, выражаемой как в материальном, так и в нематериальном эквиваленте, то при нарушении порядка оборота сведений конфиденциального характера причиняется либо материальный, либо иной ущерб.

В связи с вышесказанным стоит раскрыть сущность и содержание конфиденциальной информации через призму «тайны».

Следует отметить, что с момента утраты своей юридической силы Закона «Об информации, информатизации и защите информации»[2] отечественное законодательство не имеет правовой дефиниции «конфиденциальная информация». Кроме того, не существует и правовой дефиниции, раскрывающей содержание правовой категории «тайна», хотя законодатель при регулировании общественных отношений в сфере оборота конфиденциальной информации, разграничивая виды последней, использует данную формулировку [4; 8].

В свою очередь, научным сообществом выработано несколько позиций, характеризующих содержание тайны [2, с. 7; 5, с. 119; 6, с. 233; 7, с. 8; 9, с. 41; 10, с. 5]. Среди изученных характеристик «тайны» наиболее верной являются позиции, определяющие тайну посредством конфиденциальности информации, т. е. через призму его правового режима [2, с. 7; 9, с. 41].

---

[1] О государственной тайне: Закон Рос. Федерации от 21 июля 1993 г. № 5485-I (последняя редакция) // Официальный интернет-портал правовой информации: сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102025035 (дата обращения: 23.03.2024).

[2] Об информации, информатизации и защите информации: Федер. закон от 20 февраля 1995 г. № 24-ФЗ // СЗ РФ от 20 февраля 1995 г. № 8.Ст. 609 (утратил силу ФЗ от 27 июля 2006 г. № 149-ФЗ).

На основании изложенного стоит выделить признаки (элементы) конфиденциальной информации [11, с. 16]:

1. Категория сведений, относимых к определенному виду конфиденциальной информации.

2. Круг субъектов, владеющих такой информацией, либо обладающей правом на оборот указанных сведений.

3. Наличие ценности конфиденциальной информации (выражающейся в степени значимости для личности, общества либо государства).

4. Механизм обеспечения допуска и доступа к такой категории «тайной» информации.

5. Наличие юридической ответственности за нарушение правового режима конфиденциальности информации.

Таким образом, на основе действующего законодательства, существующих научных воззрений в данной сфере, можно сформулировать понятие конфиденциальной информации – это строго определенная (на основании закона либо подзаконного акта) совокупность сведений (данных), независимая от формы представления, правом на оборот которой обладает ограниченный круг лиц, сокрытая специальным образом с целью обеспечения законных интересов личности, общества, государства и имеющая особый правовой режим оборота, за нарушения требований которой наступает юридическая ответственность в соответствии с законом.

Говоря о правовом обеспечении оборота конфиденциальной информации, стоит отметить, что одни нормативные правовые акты устанавливают общественные отношения в рассматриваемой сфере, другие же – осуществляют ее охрану. В связи с чем такое обеспечение состоит из множества звеньев.

Одним из немаловажных звеньев, призванных охранять существующие и развивающиеся общественные отношения в сфере конфиденциальности, является Уголовный кодекс Российской Федерации (далее – УК РФ)[1]. Он выступает в качестве соответствующей правовой реакции общественности и государства на вызовы со стороны преступности, призванный охранять (а в случае нарушения – защищать) наиболее важные общественные отношения.

Уголовно-правовая охрана в сфере оборота конфиденциальной информации представляет собой одноименный институт [3, с. 12.]

[1] Уголовный кодекс Российской Федерации: Федер. закон от 13 июня 1996 г. № 63-ФЗ (последняя редакция) // Официальный интернет-портал правовой информации: сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (дата обращения: 23.03.2024).

(или подсистему), состоящий из 16 уголовно-правовых запретов, а именно: ст.ст. 137, 138, 138.1, 141, 147, 155, 183, 185.6, 276, 283, 283.1, 283.2, 284, 310, 311, 320 УК РФ. Представленные выше уголовно-правовые запреты имеют дуалистический характер, характеризующийся, с одной стороны, относимостью к одной сфере правового обеспечения (т. е. сферы оборота конфиденциальной информации), с другой – охраняющими разными по своему содержанию объектами уголовно-правовой охраны, изложенные в ст. 2 УК РФ.

В частности, рассматриваемым уголовно-правовым институтом затрагиваются следующие виды охраняемых уголовным законом общественных отношений: ст.ст. 137, 138, 138.1, 141, 147 УК РФ – конституционные права и свободы человека и гражданина; ст. 155 УК РФ – семья и несовершеннолетние; ст.ст. 183, 185.6 – сфера экономической деятельности; ст.ст. 276, 283, 283.1, 283.2, 284 УК РФ – основы конституционного строя и безопасности государства; ст.ст. 310, 311 УК РФ – правосудие; ст. 320 УК РФ – порядок управления.

В зависимости от тяжести преступления данный институт классифицируется следующим образом: ст.ст. 137, 138, 141, 147, 155, 183, 283.2, 284, 310, 311, 320 УК РФ – небольшой тяжести; ст.ст. 138.1, 185.6, 283, 283.1 УК РФ – средней тяжести; ст. 276 УК РФ – особо тяжкое.

В целом как правовое регулирование в целом, так и уголовно-правовое обеспечение оборота конфиденциальной информации имеет бланкетный характер. Правовые нормы, устанавливающие общественные отношения относят к более профильным нормативным-правовым актам, регулирующим вопросы оборота конкретного вида конфиденциальной информации.

Стоит отметить следующие выводы: во-первых, правовое обеспечение в сфере оборота конфиденциальной информации характеризуется бланкетным содержанием, отсылающим к «профильному» правовому регулированию, затрагивающего лишь отдельный вид конфиденциальной информации.

Во-вторых, ядром правовой основы в сфере конфиденциальности заложено аксиологическое основание, суть которого заключается в степени ценности конкретного вида сведений, данных, являющихся конфиденциальным. Они измеряются в зависимости от субъектов, предмета и ущерба (потенциального и реального).

В-третьих, правовое обеспечение расплывчатым образом определяет относимость информации к конкретному виду конфиденциальных сведений, в связи с чем возникают трудности при определении направления правового режима конфиденциальности. Для

нивелирования данной проблемы следует исходить из ценности предмета, а также ущерба, наносимого при нарушении правового режима конфиденциальности.

В-четвертых, считается сомнительным решение законодателя в отказе от правовой категории «конфиденциальная информация», что вносит определенные терминологические трудности в процессе законотворчества, т. е. отсутствует единая правовая категория, характеризующая все виды тайн. Вместе с тем является положительным появление правовой дефиниции «конфиденциальность информации», указывающей на ее правовой режим.

В-пятых, уголовно-правовая охрана оборота конфиденциальной информации представляет собой соответствующий правовой институт, имеющий дуалистический характер (охраняет одну сферу, при этом затрагивая множество разносторонних). При этом содержит в себе бланкетные уголовно-правовые запреты, которые отсылают к профильным нормативным правовым актам, устанавливающих общественные отношения в данной сфере. В связи с чем от точности правового регулирования и отсутствия правовых пробелов в последних зависит и степень эффективности такой уголовно-правовой охраны.

Список литературы:

1. *Братановский С. Н.* Сущность и виды специальных правовых режимов информации // Гражданин и право. 2012. № 9.

2. *Дворников А. А.* Уголовно-правовая охрана государственной и служебной тайны в органах внутренних дел: дис. ... канд. юрид. наук. Тюмень, 2007. 22 с.

3. *Жук М. С.* Институты российского уголовного права: понятие, система и перспективы развития: дис. ... д-ра юрид. наук. Краснодар, 2013. 62 с.

4. *Камалова Г. Г.* Вопросы систематизации информации ограниченного доступа // Вестник Удмуртского университета. Серия: «Экономика и право». 2016. № 2.

5. *Красавчикова Л. О.* Личная жизнь под охраной закона. Москва, 1983. 160 с.

6. *Ловцов Д. А.* Системология информационных правоотношений. Москва: Рос. Акад. Правосудия, 2008. 233 с.

7. *Паршин С. М.* Тайна в уголовном законодательстве (теоретико-прикладное исследование): дис. ... канд. юрид. наук. Нижний Новгород, 2006. 35 с.

8. *Пилипенко Ю. С.* К вопросу о классификации правовых тайн // Журнал российского права. 2009. № 9.

9. *Смолькова И.* Гласность и тайна в уголовном процессе // Законность. 1998. № 7.

10. *Фатьянов А. А.* Тайна и право (основные системы ограничения на доступ к информации в российском праве): монография. Москва: МИФИ, 1999.

11. *Фатьянов А. А.* Тайна и право (основные системы ограничения на доступ к информации в российском праве): монография. Москва: МИФИ, 1999. 288 с.

12. *Шахрай С. М.* Конституция России: стабильность и развитие // Актуальные проблемы российского права. 2018. № 10.

13. *Шульга С. В.* Соотношение основных принципов современного международного права и конституционного законодательства России: материалы Всерос. студ. юрид. форума / отв. ред. Т. А. Сошникова // Москва: Московский гуманитарный университет, 2019.

Игорь Олегович Лапшин,
кандидат технических наук,
заместитель начальника кафедры
специальных информационных технологий
Московский университет МВД России имени В. Я. Кикотя
E-mail: cosmos123@mail.ru;

Илья Сергеевич Стручков,
старший преподаватель кафедры
специальных информационных технологий
Московский университет МВД России имени В. Я. Кикотя
E-mail: pikia91@mail.ru

УДК: 004.838.2

Аналитическая работа в МВД России на современном этапе

Аннотация

Рассмотрены основные принципы аналитической работы в органах внутренних дел (ОВД), ее обеспеченность математическими моделями, методами и программно-техническими средствами, позволяющими изучать количественные и качественные характеристики исследуемых социально-правовых и криминологических процессов, а также формировать на этой основе варианты управленческих решений.

Ключевые слова и словосочетания: *аналитическая работа; МВД России; модели и методы; большие данные.*

Аналитическая деятельность в органах внутренних дел (ОВД) для повышения эффективности раскрытия и расследования преступлений и решения других оперативно-служебных задач всегда выступала приоритетной для правоохранительных органов.

В ходе реализации аналитической деятельности формируется информационное отображение события преступления – его криминологические, криминалистические и иные характеристики. Наиболее существенными при этом являются данные о субъекте расследуемого преступления, непосредственном объекте преступного посягательства, особенностях способа совершения преступления, в том числе особенностях используемых средств и орудий совершения преступления [9; 11].

Развиваются нормативные, организационные и технологические основы создания информационных массивов. Так, традиционные ручные картотеки применялись в правоохранительной деятельности, начиная с начала XX века. В 60-70-х годах по мере расширения возможностей компьютерной техники создавалась база для организации автоматизированных учетов. Автоматизированные системы оперативно-розыскного и профилактического назначения прошли несколько модификаций: «Зона-М», автоматизированный банк данных (АБД), интегрированный банк данных (ИБД), информационно-поисковые сервисы ИСОД МВД России.

В качестве основных функций информационно-аналитической и управленческой поддержки деятельности ОВД в самом общем виде выделяются [6]:

– накопление, обобщение, анализ, многократное и разноплановое использование данных, поступающих в ОВД из различных источников (официальных, неофициальных, общественных, реализованных на основе применения различных информационных технологий);

– организация социологических и криминологических исследований, прогнозирование криминогенной обстановки;

– подготовка для руководящего состава ОВД и различных инстанций информационно-аналитических и справочных материалов об основных результатах работы, оценках криминогенной обстановки на обслуживаемой территории;

– формирование справочно-информационного и аналитического фонда для обеспечения стратегической и тактической деятельности подразделений ОВД.

Информационную базу анализа и прогнозирования направлений функционирования ОВД составляет, главным образом, *статистическая информация* о состоянии преступности и результатах оперативно-служебной деятельности.

В то же врем уже давно ведутся дискуссии о недостатках традиционных статистических методов и подходов. Однако простота производимых расчетов, определенная их стереотипность и другие имеющиеся преимущества пока сдерживают развитие математической технологии в указанной сфере.

Однако с годами произошло и продолжает происходить значительное изменение многих факторов детерминации противоправных деяний, совершенствование методов их раскрытия и расследования на основе достижений науки и техники. Все это в совокупности привело к формированию новых требований к количественной поддержке принимаемых решений.

Нарастающая необходимость изменения существующего положения в указанной сфере приводит к новым подходам, технологиям, методам совершенствования информационно-аналитического обеспечения деятельности подразделений МВД России.

В связи со сказанным представляются важными следующие соображения:

1. Статистическое оценивание базируется, как правило, на *классических показателях представления информации*: абсолютные, относительные, средние значения, индексные величины – как основа расчетных преобразований математической статистики. При этом математическая статистика как система методов и практическая дисциплина обработки данных, располагая набором развитых алгоритмов, имеет определенные ограничения по их корректному применению.

Использование аппарата математической статистики в результате приводит к оперативному и наглядному получению итоговых данных, позволяющему проводить требуемые аналитические сравнения. Однако невыполнение ряда частных условий корректного применения методов статистики (например, при расчете средних значений при существенной неоднородности исходных данных) приводит к искаженным, а подчас и противоречивым результатам.

Отмеченные положения объясняют сложность создания на основе традиционных методов статистики надежных алгоритмов обработки, отражающих изменения в современных правовых явлениях, проверку исследовательских гипотез, прогнозов развития изучаемых криминологических процессов.

2. *Большие данные*. Масштаб информационных массивов, возможности их современной математической обработки привели к необходимости применения технологии больших данных. В работе [10] подчеркивается, что искусственный интеллект и большие данные определены как основные сквозные цифровые технологии. Это отмечено в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента России от 9 мая 2017 г. № 203[1].

Если говорить просто, то большие данные (англ. *Big Data*) – обозначение огромных объемов структурированных и неструктурированных данных, эффективно и оперативно обрабатываемых современными математическими методами и программными

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: Указ Президента Российской Федерации от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

инструментами. В широком смысле это социально-экономический феномен, отражающий появление технологических возможностей анализировать огромные массивы данных, а по существу – весь их мировой объем и вытекающие из этого трансформационные последствия для общества.

Для иллюстрации указанного феномена применительно к информационным системам МВД России приведем лишь один пример. Так, 23 года тому назад только за полгода информационными центрами ОВД поставлено на учеты более 35 млн объектов, представляющих оперативный интерес (общее число единиц, стоящих на учете в тот период, было почти в 10 раз больше). Сотрудники ОВД за те же полгода обратились к указанным системам с запросами около 60 млн раз [5]. Для сравнения – информационная система Национального центра криминальной информации (*NCIC*) ФБР США 23 года назад насчитывала около 40 млн единиц учета.

3. К важнейшим вопросам использования информационных ресурсов относится *обеспечение их актуализации*. Полнота и достоверность учетных документов основывается на постоянном контроле (логической, содержательной и иной проверки учтенных и новых вводимых данных) регистрируемой и корректируемой информации об объектах учетов.

Задачи и особенности актуализации данных необходимо рассматривать в ряду самостоятельных аспектов. Отметим два важнейших из них:

– различная степень актуализации данных по конкретным учетам сказывается и на других учетах, связанных с ними;

– отличающиеся форматы представления данных в различных базах приводят к отсутствию единого формата при создании информационных массивов для исследования криминогенной обстановки. По многим причинам разработать такой единый формат почти нереально, если учитывать различия хранилищ уголовно-правовой статистики, особенности специализированных автоматизированных учетов ОВД, неструктурированность информации из социальных сетей и многие другие факторы.

Современные тенденции информационного обеспечения правоохранительной деятельности указывают на постоянное расширение как перечней баз данных, так и технологических возможностей их обработки, а также подходов к автоматизированному управлению ими. В перспективе именно в гармоничном сочетании информационных сервисов, интеграции систем с разнородными данными видится эффективное решение информационно-аналитических и управленческих задач ОВД [4].

Существует множество причин (сбоев при обработке данных, технических ошибок, алгоритмического несоответствия, нечеткого выполнения регламентов ввода или корректировки исходных данных), определяющих появление ошибок в информационных базах. Ошибки приводят к следующим недоработкам в формировании статистических учетов, специализированных банков и баз данных ОВД: неполные данные, данные с ошибочными значениями, пропуски данных, несоответствие форматам данных, пустые ячейки и т. д.

Совокупность ошибок и неточностей делает некорректной обработку информационных массивов, а также приводит к подготовке недостаточно обоснованных и даже неверных управленческих решений. Этому, в частности, могут способствовать ошибки восприятия данных, которые оцениваются человеком или автоматизированными системами (например, при применении систем искусственного интеллекта).

4. При анализе особенностей и условий функционирования систем информационного обеспечения ОВД необходимо обратить внимание на их *динамичность* как системное свойство, а также на изменение содержания задач управления в данной сфере, характеризующегося проявлением в ней характеристик *сложных динамических систем* [6].

Обратимся к признакам таких систем. В первую очередь, они отличаются вариативностью, адаптивностью к изменениям окружающей среды, требующими наилучшие стратегию и тактику реагирования. Согласно этим важнейшим свойствам у системы управления имеется способность воспринимать управляющее воздействие, переходить в новое состояние в течение определенного переходного процесса. В результате обеспечивается возможность ее перестройки, которая требуется реально возникшими объективными обстоятельствами.

Эти положения относятся и к системам информационного обеспечения деятельности ОВД. При этом прослеживается устойчивая зависимость между раскрываемостью преступлений и информационной активностью сотрудников практических подразделений. В числе основных параметров информационной активности можно назвать: количество документов, поступающих в информационную систему за единицу времени; количество удаляемых документов; объем накопленных массивов [5].

Можно отметить и другие особенности, связанные с динамикой изменения информационных массивов, например:

– изменение представлений о выполняемой задаче, определяемых промежуточными результатами, новыми возникающими гипо-

тезами, более глубоким экспертным осмыслением ситуации. Это, как правило, влечет новую скорость и производительность проверки информационных массивов;

– вариация набора и последовательности оцениваемых параметров (структуры и форматов данных, степени их полноты, соответствия определенным правилам);

– возможные искажения из-за несовершенства алгоритмов ввода, удаления и корректировки данных.

Знание реальной динамики информационных массивов и ее прогноз позволяют достоверно определить характеристики персонала, способного на требуемом качественном уровне осуществлять управление системой информационного обеспечения деятельности ОВД.

Еще одной стороной рассматриваемого вопроса является *динамичность задач управления*. При этом выделяются такие свойства информационных систем, как их стабильность (способность сохранять свои качества), равновесие между динамичностью и стабильностью (обеспечение существования, функционирования, в конечном итоге – живучести), целевое поддержание равновесия (сохранение гомеостаза как противодействие разрушению и дезорганизации). В системах с перечисленными признаками обязательно наблюдаются процессы саморегуляции и самоорганизации.

Вся совокупность отмеченных системных свойств определяет непрерывное влияние и подверженность динамическим изменениям информационного обеспечения ОВД. Этому способствует информационный характер процессов раскрытия и расследования преступлений, проведения аналитической и иной деятельности ОВД.

В итоге оценка реальных процессов развития системы информационного обеспечения деятельности ОВД связана с динамичностью задач управления, возникновением классов новых подзадач. Данные обстоятельства накладывают на функционирование информационных систем правоохранительных органов и ОВД, в частности, требования поддержки динамического характера существования, обязательной реализации в программно-аппаратных средствах и приложениях возможностей по учету возникающих изменений.

5. Значимым фактором в развитии информационных систем и их методического обеспечения, поддерживающих эффективность информационно-аналитической и управленческой деятельности ОВД, следует считать учет *латентности преступлений*. Речь идет о скрытой преступности, которая по тем или иным причинам не стала известной правоохранительным органам.

Существуют различные методы косвенной оценки латентности правонарушений и преступлений. Например, часто обращаются

к результатам, полученным в работе [6]. Исследования почти в трех десятках стран мира показали, что значения показателей латентных преступников оцениваются в 5–6 % от общего числа населения в них.

Исходя из указанных результатов, при разработке математических моделей криминогенной обстановки следует учитывать фактор латентности во избежание серьезных ошибок в управленческих решениях ОВД.

В то же время методология традиционной статистической обработки информации о преступности не позволяет учесть и интерпретировать влияние латентности на состояние и динамику криминогенной обстановки, обеспечивать аналитическую деятельность в ОВД на современном уровне. Кроме того, в рамках традиционного анализа сложно ответить на многие вопросы о скрытых характеристиках криминогенной обстановки, обосновать на этой основе необходимые по масштабу, структуре и направлению управленческие решения по противодействию преступности.

В целом современные условия проведения информационно-аналитической работы в ОВД приводят к необходимости разработки и внедрения перспективных моделей, технологий и методов анализа данных.

Они должны развиваться в направлениях:

– предварительная системная подготовка (в том числе с применением методов искусственного интеллекта) информационных массивов, доведение их до требуемых форматов полноты, соответствия логике последующих преобразований в математических моделях;

– производительные алгоритмы обработки информации, по сути, приближающихся к технологии больших данных.

Технологии больших данных должны учитывать новые структурные, сервисные, аппаратно-программные, телекоммуникационные и иные принципы, подходы, ресурсы, что позволит достичь следующего качественного уровня развития информационно-аналитической и управленческой деятельности ОВД [1–3; 7–8].

Список литературы:

1. *Барсегян А. А. [и др.].* Анализ данных и процессов: учеб. пособие. Санкт-Петербург: БХВ-Петербург, 2009. 512 с.

2. *Барсегян А. А. [и др.].* Методы и модели анализа данных: OLAP и Data Mining. Санкт-Петербург: БХВ-Петербург, 2004. 336 с.

3. *Барсегян А. А. [и др.].* Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP. 2-е изд. Санкт-Петербург: БХВ-Петербург, 2007. 383 с.

4. *Бондарь К. М., Дунин В. С.* Пути интеграции геоинформационных систем для аналитического обеспечения раскрытия и расследования преступлений: сборник по материалам XXV Юбилейной Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Рязань, 2020.

5. *Бондарь К. М., Киселев В. И.* Автоматизированные банки данных и их использование в органах внутренних дел: учебное пособие. Хабаровск: ДВЮИ МВД России, 2000. 92 с.

6. *Бондарь К. М., Рыбак А. В., Скрипко П. Б.* Основы управления в органах внутренних дел: курс лекций. Хабаровск: Дальневосточный юридический институт МВД РФ, 2015. 180 с.

7. *Минаев В. А., Бондарь К. М., Рабчевский А. Н., Федорович В. Ю.* Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: монография / под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: ДВЮИ МВД России, 2023. 232 с.

8. *Минаев В. А., Бондарь К. М., Дунин В. С., Скрипко П. Б.* Математические модели анализа, оценки, прогнозирования и управления в органах внутренних дел: монография. Хабаровск: ДВЮИ МВД России, 2022. 308 с.

9. *Нестеров А. В.* Миграция населения и проблемы борьбы с организованной преступностью // Актуальные проблемы теории и практики борьбы с организованной преступностью. Москва, 1994.

10. *Овчинский В. С., Ларина Е. С.* Искусственный интеллект. Большие данные. Преступность. Москва: Книжный мир, 2018. 391 с.

11. *Полевой Н. С.* Криминалистическая кибернетика: теория информационных процессов и систем в криминалистике. Москва: МГУ, 1982. 208 с.

Игорь Олегович Лапшин,
кандидат технических наук,
заместитель начальника кафедры
специальных информационных технологий
Московский университет МВД России имени В. Я. Кикотя
E-mail: cosmos123@mail.ru;

Илья Сергеевич Стручков,
старший преподаватель кафедры
специальных информационных технологий
Московский университет МВД России имени В. Я. Кикотя
E-mail: pikia91@mail.ru

УДК: 004.838.2

Технология VIPNET для защиты информации в органах внутренних дел

Аннотация

Рассмотрены актуальные задачи защиты сетевой структуры органов внутренних дел с использованием технологии ViPNET. Раскрываются компоненты указанной технологии, архитектурная гибкость которой в сочетании с перспективными методами и средствами обеспечивает защиту от сетевых угроз.

Ключевые слова и словосочетания*: органы внутренних дел; вычислительная сеть; защита данных; технология ViPNET.*

При рассмотрении вопросов безопасности распределенных сетей недостаточно уделять внимание только незаконным внешним воздействиям, поскольку для злоумышленников, как правило, известны доступы к внутренней сети, во многих случаях выступающие более эффективными при осуществлении нарушений.

Для обеспечения безопасности коммуникаций и технических средств, а также защиты информационных ресурсов в территориально распределенной сети необходимо создать интегрированную защищенную среду в телекоммуникационной инфраструктуре, связанную с внешними техническими средствами и ресурсами.

В этой связи задачи, стоящие в части защиты сетевой структуры и передачи сетевого трафика, можно сформулировать следующим образом:

1. Обеспечение органов внутренних дел квалифицированными кадрами в области обеспечения информационной безопасности.

2. Совершенствование нормативного правового регулирования защищенного сетевого взаимодействия с другими ведомствами.

3. Оперативное реагирование на появление новых угроз информационной безопасности.

4. Расширение средств для всесторонней защиты от угроз в области информационной безопасности.

5. Сокращение расходов на содержание средств и систем защиты информации.

Указанные задачи отчасти решаются применением технологии ViPNet, которая объединяет целый ряд перспективных программных продуктов и сетевых решений:

1. Программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI).

2. Средства межсетевого экранирования и персональные сетевые экраны.

3. Средства шифрования данных.

4. Системы централизованного управления и мониторинга средств защиты информации (СЗИ).

5. Средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы документооборота, порталы и т. п.).

6. Программно-аппаратные комплексы (или самостоятельные сетевые устройства) обнаружения компьютерных атак ViPNet IDS.

Набор модулей технологии ViPNet может быть развернут на различных компьютерах в ведомственной сети независимо от их местоположения. Такой подход позволяет решить ряд указанных выше задач. При этом реализована возможность гибкого использования имеющегося оборудования – компьютеров, серверов, маршрутизаторов, коммутаторов, «брандмауэры» и других устройств в соответствии с существующей сетевой структурой без потери функциональности и удобства [2; 4].

В рамках технологии ViPNet выделяются три основных компонента: ViPNet–Клиент, ViPNet–Координатор, ViPNet–Администратор (рис. 1).

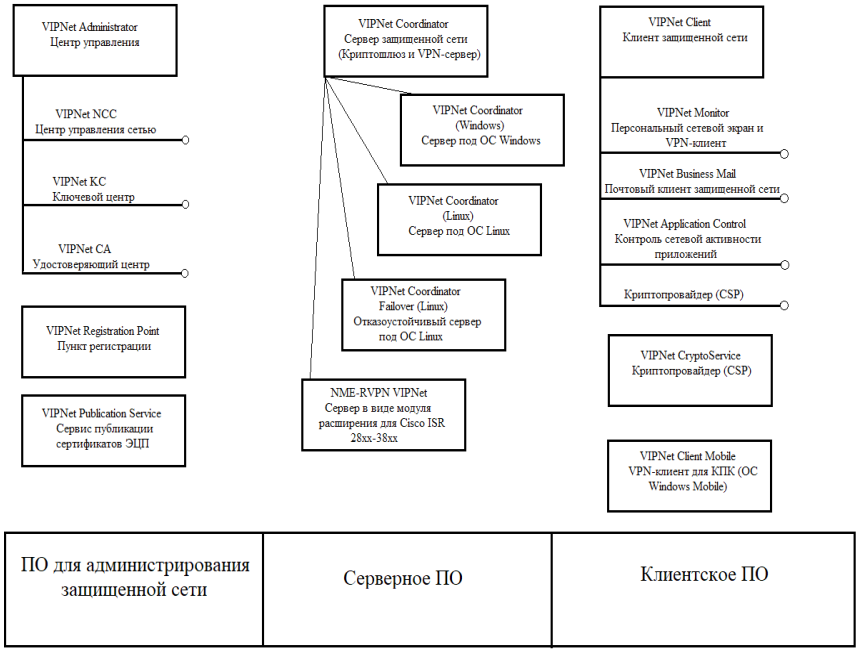

Рис. 1. Компоненты технологии ViPNet

ViPNet–Administrator является программным пакетом, состоящим из ViPNet УКЦ (Удостоверяющий и Ключевой Центр) и ViPNet ЦУС (Центр управления сетью). ViPNet ЦУС служит для настройки и эффективного управления защищенной виртуальной сетью ViPNet и решает задачи [1]:

– определения узлов защищенной сети, пользователей и допустимых связей между ними путем создания необходимых баз данных для работы УКЦ;

– определения политики безопасности на каждом узле и формирования списка прикладных задач, которые могут на данном узле решаться (шифрование трафика, ЭЦП, деловая почта и т. д.);

– поддержания автоматической рассылки справочной ключевой информации (справочников связей узлов, корневых и отозванных сертификатов, ключей шифрования, информации о связях с другими ViPNet -сетями и др.);

– проведения централизованного обновления программного обеспечения (ПО) ViPNet на узлах защищенной сети;

– поддержания удаленного доступа к журналам событий на узлах защищенной сети.

УКЦ выполняет функции центра выработки ключей шифрования и персональных ключей пользователей, а также Удостоверяющего Центра для организации PKI.

– выработка и хранение первичной ключевой информации (мастер-ключи шифрования и межсетевые мастер-ключи);

– выработка ключей шифрования для узлов защищенной сети и ключей шифрования между пользователями защищенной сети (двухуровневая схема);

– выполнение процедур смены мастер-ключей и компрометации ключей шифрования;

– выработка персональных ключей защиты пользователей и надежных парольных фраз (паролей);

– запись персональных ключей пользователей на аппаратные носители ключей.

Основными функциями УКЦ являются:

Ключевой Центр выполняет ряд функций, среди которых основной является защита ресурсов и данных, передаваемых с различных устройств –рабочих станций, мобильных устройств, удаленных или локальных систем, а также серверов разнообразного назначения, включая веб-серверы, FTP, SMTP, SQL, файловые серверы. Кроме того, в его задачи входит генерация и сохранение исходной ключевой информации, такой как ключи шифрования и ключи обеспечения безопасности межсетевых соединений.

ViPNet Coordinator – это программно-аппаратное решение в области информационной безопасности, обеспечивающее защиту данных между территориально распределенными сетями. Эта технология разработана для предотвращения несанкционированного доступа, обеспечения шифрования и гарантирования целостности передаваемой информации[1].

Важной особенностью является поддержка мобильности. ViPNet Coordinator имеет возможность безопасно подключаться к ведомственным ресурсам удаленным пользователям, если это регламентировано. При этом пользователи получают такой же уровень защищенности, как если бы находились непосредственно в одной сети. Основную функциональность ViPNet Coordinator обеспечивают:

– криптошлюз для организации защищенных туннелей в рамках виртуальной частной сети ViPNet;

[1] ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. 2019. URL: https://docs.cntd.ru/ document/1200161708#7D20K3 (дата обращения: 14.03.2024); Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня. 2021. URL: https://docs.cntd.ru/ document/603366553 (дата обращения: 14.03.2024).

– межсетевой экран;

– сервер IP-адресов виртуальной частной сети ViPNet (поддержка работы удаленных мобильных пользователей и любых других узлов сети с динамическими IP- адресами);

– сервер-маршрутизатор почтовых конвертов;

– сервер для организации безопасного подключения к Интернету отдельных узлов сети ViPNet без их физического отключения от локальной сети.

Таким образом, ViPNet – инструмент, который превращает территориально распределенные локальные вычислительные сети в защищенные с помощью криптографических алгоритмов. Он сочетает актуальные технологии с ориентированной на пользователя функциональностью для обеспечения защиты данных. Его архитектурная гибкость в сочетании с перспективными технологиями обеспечивает защиту от сетевых угроз.

Однако высокий уровень безопасности, хотя и является ключевым преимуществом ViPNet, иногда может приводить к определенным сложностям при интеграции в многоуровневые сетевые структуры.

Поэтому поддержка системы включает в себя ряд важных аспектов.

Во-первых, успешная реализация технологии ViPNet неразрывно связана с обучением ее администраторов и пользователей. Очевидно, что создание и реализация образовательных программ требуют времени.

Во-вторых, регуляризация и интеграция обновлений системы безопасности имеют решающую роль для защиты информации. Эта область не ограничивается простым применением обновлений, а воплощает комплекс мероприятий с беспрерывным мониторингом и внедрением усовершенствований в области обеспечения информационной безопасности.

В-третьих, управление политикой безопасности в контексте ViPNet требуют особого внимания в связи с особо сложной в распределенной сетевой структуре в ОВД с множеством пользователей [3].

Список литературы:

1. *Акинина Л. Н., Попов В. Б., Перехрест Р. Д.* Программно-аппаратные комплексы ViPNet и их использование в корпоративных сетях // Научный вестник Крыма. 2016. № 3 (3).

2. *Гусев В. В., Чаплыгин В. Е.* Администрирование системы защиты информации ViPNet (Windows & Linux). Москва: Горячая линия – Телеком, 2018. 366 с.

3. *Минаев В. А., Поликарпов Е. С., Еременко В. Т., Рытов М. Ю.* Управление информационной безопасностью: учебное пособие. Москва: МосУ МВД России имени В. Я. Кикотя, 2022. 310 с.

4. *Прудников А. И., Шахов В. Г.* Особенности использования технологии ViPNet для защиты информации в корпоративных сетях. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniyatehnologii-ViPNet-dlya-zaschity-informatsii-v-korporativnyh-setyah (дата обращения: 14.03.2024).

Михаил Сергеевич Лащёнов,
кандидат социологических наук,
доцент кафедры теории и методологии
государственного управления
Академия управления МВД России
E-mail: Laschenov.m@yandex.ru

Павел Михайлович Лащёнов,
слушатель факультета подготовки специалистов
в области информационной безопасности
Московский университет МВД России
имени В. Я. Кикотя
E-mail: Laschenov.p@yandex.ru

Информационно-аналитическое обеспечение деятельности ОВД по противодействию цифровому мошенничеству в сфере частного инвестирования

Аннотация

Современные тренды в сфере частного инвестирования значительно скорректированы в направлении цифровых финансовых активов. Аналитики отмечают большое количество новых инвесторов и продолжающуюся эйфорию на криптовалютном рынке. Согласно ежегодному исследованию *Huobi* [6] Россия заняла третье место в мире (после США и Вьетнама) по степени зрелости криптовалютного рынка. Практически каждый десятый россиянин, а это 14,6 млн человек, владеет криптовалютой.

Современные тенденции в сфере частных инвестиций привносят свои коррективы в структуру преступности, порождая новые виды мошенничества, основу которых составляют новые преступные схемы и технологии (фишинг, скамминг, кардинг, технологии блокчейна и т. п.). Этому процессу невозможно противостоять коррекцией исключительно штатной либо организационной деятельности органов внутренних дел. Эффективное включение правоохранительного субъекта в решение обозначенных задач невозможно без отлаженных алгоритмов выявления финансовых рисков, блокирования финансовых крипто-пирамид, блокчейн-анализа транзакций, мониторинга блокчейн-сетей, адресов, пулов и скам-проектов, технологической возможности блокирования финансовых криптопирамид, организации должного взаимодействия с централизованными криптовалютными биржами, да и в целом без информацион-

но-аналитического обеспечения деятельности правоохранителей по противодействию подобной категории преступлений. Поиск мер и выработка алгоритмов информационного противодействия мошенничеству в сфере привлечения частных инвестиций, в том числе и цифровых финансовых активов, выступают актуальной проблемой в свете предупреждения, раскрытия и расследования указанной категории преступлений.

Ключевые слова и словосочетания: *цифровые финансовые активы; частное инвестирование; мошенничество; информационное противодействие; анализ финансовых рисков; алгоритмы выявления; методика расследования.*

На фоне нестабильной ситуации в мировой экономике и растущих процентных ставок инвесторы все чаще стали рассматривать криптовалюту в качестве альтернативного варианта финансовых вложений. При этом, помимо обычных инвесторов (физических лиц), потенциал криптовалют признают и институциональные инвесторы – юридические лица и организации, осуществляющие инвестирование на деньги вкладчиков. Среди таковых можно выделить *BlackRock, Goldman Sachs, Fidelity Investments, Grayscale и др. Например, BlackRock* (БлэкРок) – американская международная инвестиционная *компания, которая* сохраняет за собой лидирующее первое место с 2009 г. в рейтинге крупнейших компаний мира, управляющих активами ($1.158/507) [8]. Конечно, доля институциональных инвесторов еще мала, и согласно исследованию JPMorgan за 2023 г. число компаний, инвестирующих в криптовалюту, выросло всего на один процент «с 8 % до 9 %, еще 12 % планируют начать торговлю в течение ближайших пяти лет» [7], но сам факт их количественного роста привлекает внимание рядовых граждан и укрепляет их сознание в перспективности финансовых инвестиций в криптовалюту.

Более того, на заинтересованность инвесторов оказывает влияние инвестиционное поведение медийных личностей. В числе известных персон, инвестирующих в криптовалюты, можно назвать миллиардера Питера Тиля, инвестиционного гуру Роберта Кийосаки, предпринимателя Илона Маска, боксера Майкла Тайсона, актера Эштона Катчера и многих других [3].

Сильнейшее влияние на рост рынка и инвестиционную популярность криптовалюты оказывают иные экономические и политические факторы: продолжающиеся инфляционные процессы, риск рецессии, геополитические конфликты, свертывание традиционных

средств инвестирования (рынка недвижимости, драгоценных металлов, акций), ожидаемый халвинг биткоина и т. п. Все это в совокупности порождает рост рынка криптовалюты и как закономерный эффект привлекает огромное количество граждан, желающих вложиться в «волшебные бобы» и «закупиться монетами» в расчете на высокую доходность. При этом в подавляющем большинстве случаев криминологический портрет потенциального потерпевшего характеризуется отсутствием элементарных навыков финансовой грамотности (умение человека принимать взвешенные финансовые решения в повседневной жизни). Эксперты Аналитического центра НАФИ утверждают, что в 2024 г. индекс доли финансовой грамотности россиян составил 12,7 %, в то время как низкий уровень финансовой грамотности – 30 % [5]. Фактически это треть общества, которая является «лакомым кусочком» и привлекает своим «потенциалом» внимание мошенников. Статистика фиксирует закономерный рост преступлений, связанных с криптовалютой. Согласно исследованию, проведенному МГИМО МИД России, количество судебных приговоров, вынесенных по делам о преступлениях, связанных с криптовалютами, в период 2017–2021 гг. выросло почти на 5000 %. Если за пять лет – с августа 2012 г. по октябрь 2017 г. – судами было вынесено 72 приговора по делам, связанным с незаконным использованием криптовалюты, то за период 2017–2021 гг. их количество составило более 2 500 приговоров [4]. И это только видимая часть, учитывая, что большая часть аналогичных преступлений (около 60 %) остаются в числе латентных, скрытых пострадавшими по причине отсутствия в стране правового регулирования криптовалют, что зачастую рассматривается гражданами как незаконное предпринимательство.

Таким образом, состояние сферы частных инвестиций характеризуется ростом повышенного внимания к рынку криптовалюты при одновременно фиксируемом уровне низкой финансовой грамотности населения и отсутствии правового статуса виртуальных денег, что безусловно порождает новые способы противозаконного использования информационных технологий в различных областях бизнеса от телекоммуникаций до банковского сектора, увеличивая риски граждан в сфере частного инвестирования.

Целью настоящей статьи является поиск мер и выработка алгоритмов информационного противодействия мошенничеству в сфере привлечения частных инвестиций. Оптимальным методом исследования выступает качественный контент-анализ интернет-сай-

тов[1], создающих инструментальные платформы по идентификации и пресечению мошеннических практик в сфере оборота цифровых валют, а также отчетов компаний, применяющихся для отслеживания и возврата похищенных средств.

Методика исследования состоит в контент-анализе отчетов таких компаний, как *Angara Security, Chainalysis Reactor, Storyline* и др. [6]. Например, согласно отчету Angara Security аналитиками компании выявлено 22 000 постов (криптовалютных материалов) в *Telegram*, из которых 9 000 (40 %) были помечены как подозрительные и удалены. В то же время, несмотря на то что мошеннические сообщения удаляются технической поддержкой мессенджера или самими авторами, их посты остаются в архиве *Telegram* и доступны для анализа. В результате проведенный анализ сохранившейся в архиве информации позволил выявить типовые преступные схемы мошенничества в сфере частного инвестирования в цифровые финансовые активы (далее – ЦФА), описать основные цифровые блокчейн-технологии, используемые мошенниками в качестве инструментов совершения преступлений, предложить алгоритм действия правоохранительных структур в целях раскрытия и расследования указанной категории преступлений. Проведенный анализ является необходимым условием для проектирования информационного противодействия исследуемому виду мошенничества.

В начале определимся с основными категориями. Категория «инвестиции» вполне доступная для общего понимания – это вложение денежных средств с целью их преумножения (получения дохода) либо сохранения капитала. Инвестирование выступает необходимым условием развития цивилизованного и высокоэффективного финансового рынка, и поэтому вовлечение в инвестиционный процесс является принципиально важным даже с позиции размещения незначительных сбережений граждан. Под сферой частных инвестиций мы будем понимать набор инвестиционных направлений, доступных для использования физическими и юридическими лицами, не являющимися специализированными субъектами инвестиционного мира (трейдерами). Это обычные граждане: работники предприятий, офисные менеджеры, врачи, учителя, военнослужащие и т. д., а также заинтересованные юридические лица, рассматривающий уставной капитал организации с позиции капиталовложения. Их отличительной особенностью выступает

[1] Интернет-сайт – особым образом структурированная информация (совокупность связанных между собой веб-страниц и электронных файлов), объединенная одним доменным именем.

то, что инвестирование происходит путем вложения (размещения) исключительно частного капитала, что следует отличать от государственного, национального, корпоративного, муниципального и иного вида инвестирования.

Что касается возможных направлений инвестирования, то определить границы довольно сложно, так как это достаточно широкий спектр возможностей, начиная от приобретения ценных бумаг и недвижимости до вложений в крупные инвестиционные проекты, стартапы, венчурные фонды и франчайзинг. Однако, начиная с 2012 г., активным направлением инвестирования выступают цифровые валюты (криптовалюты), рост доходности которых значительно превосходит все традиционные объекты вложения. Например, рост доходности *CoinGecko* в 2023 г. вырос на 7,3 тыс. процентов [1]. Закономерным результатом такой доходности выступает повышенное внимание частных инвесторов к цифровой валюте. Многие российские граждане активно использую ЦФА в качестве средств хранения личных сбережений, размещая их на криптовалютных биржах либо «холодных[1]» или «горячих кошельках[2]». Ровно по той же причине возрастает и число лиц, вынашивающих преступные намерения в сфере частного инвестирования в цифровую волюту. Растет число форм и способов совершения мошеннических действий при инвестировании в криптовалюты.

Предлагаем уточнить предмет нашего исследования и более детально описать категорию интересующих нас преступлений. На сегодняшний день в российской судебной практике известно более тысячи приговоров, где употребляется слово «криптовалюта». При этом все преступления, которые совершены с использованием криптовалюты, условно можно разделить на четыре основные группы. К первой группе преступлений следует отнести те случаи, в которых криптовалюты используются для конспирации преступной деятельности и сокрытия незаконных операций. В первую очередь это легализация преступных доходов, незаконный оборот наркотиков, финансирование терроризма и другие преступления, в том числе коррупционные и экономические.

Ко второй группе относятся преступления, в которых криптовалюты используются в качестве предметов преступления: кражи, грабежи, разбои и т. д. Например, Петроградским районным судом

[1] Холодные кошельки – аппаратные кошельки с физическим доступом, приобретаемые только на официальных сайтах.

[2] Горячие кошельки – это браузерные кошельки и их мобильные приложения, которые можно скачать с официального сайта или в магазинах приложений.

осуждены лица, которые, узнав, что у потерпевшего имеется криптовалюта, под угрозой применения насилия, расправы, похитили у него криптовалюту стоимостью на момент совершения преступления свыше 55 млн руб. (95 биткоинов).

К третьей группе относятся те преступления, которые связаны со злоупотреблениями при совершении майнинга. Сюда можно отнести, например, факты хищения электроэнергии.

И наконец к четвертой группе – преступления, где криптовалюты выступают виртуальными активами (предметом инвестирования, предметом вовлечения в преступные мошеннические схемы и финансовые пирамиды). Это именно та категория преступлений, которая отвечает предмету настоящего исследования. Особенность этой категории состоит в том, что в числе пострадавших состоят лица, имеющие определенный опыт и специальные познаний в области цифрового инвестирования, однако в силу растущего числа технологий не всегда являются способными отличить стандартные криптовалюты от их скам-копий (от англ. *scam* – «мошенничество», «афера»)[1].

Нашу точку зрения разделяют многие эксперты в области крипторынка, все финансовые схемы, связанные с использованием криптовалют, в основном основываются на принципах создания финансовых пирамид. И здесь следует отметить, что число таких фактов только за 2023 г. возросло на 30 %. При том что указанная категория преступлений имеет очень высокую степень латентности, что обусловлено нерегулируемостью рынка криптовалюты, анонимностью сделок, их децентрализованностью и трансграничным характером. Потерпевшие не всегда обращаются в правоохранительные органы из-за того, что факт использования и/или владения цифровой валютой воспринимается ими как незаконный или по крайней мере сомнительный с точки зрения его законного использования.

При анализе судебных приговоров следует обратить внимание на то, что вне зависимости от отсутствия правового статуса криптовалюты (она не признана имуществом) российские суды склонны защищать позицию пострадавшей стороны и при вынесении обвинительных решений ссылаются на ст. 6 УПК РФ, чем обеспечивают государственную защиту и восстановление нарушенных прав потерпевшего. Кроме того, следует учитывать, что российское законодательство допускает возможность добровольного декларирования

[1] Скам-копии – это мошеннический инвестиционный проект, созданный для получения быстрой выгоды. Под скамом часто подразумевается намеренное нарушение условий сделок, банкротство компании и прекращение выплат ее участникам или клиентам.

криповалюты. Налоговую декларацию в этом случае сопровождают нотариально заверенные скриншоты с биржевых аккаунтов о совершенных операциях по покупке/продаже криптовалют и банковские выписки, по которым видны передвижения средств в рублях. В этом случае задача судопроизводства упрощается с точки зрения определения стоимостного эквивалента похищенной цифровой валюты. Таким образом, объективной стороной анализируемой нами категории преступлений является мошенничество, т. е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, в котором предметом преступного посягательства являются цифровые финансовые активы частных инвесторов.

Разберем практическую ситуацию, относительно стандартную для анализируемой группы преступлений. Итак, условный мошенник подбирает открытый телеграмм-канал, на котором часто предлагаются курсы по заработку на криптовалютах и инвестиции в цифровые активы, размещается реклама групп и каналов инвесторов, криптоинструментов, скрытая реклама различных платформ, скидки, бонусы и т. п. Мошенник создает в открытом телеграмм-канале пост (публикацию), где предлагает пользователям инвестировать в криптовалюты, обещая, например, приумножить вложенные финансовые средства в 70 раз и сделать из 1 руб. – 70 руб. Анализ таких публикаций показывает, что для привлечения внимания мошенники используют в названиях пабликов такие фразы, как «быстрый заработок», «путь к успеху», «финансовая независимость», «заработок сейчас», «криптоферма», «умные инвестиции» и т. д. Инициатор поста предлагает оказать очередному посетителю своего аккаунта консультативную помощь в части грамотного размещения цифровых валют посредством создания субаккаунта на *Binance*[1] под предлогом того, что он не будет иметь прямого доступа к средствам (имеется ввиду к снятию/выводу), а сможет только правильно их инвестировать. Юридическим лицам предлагают регистрировать офшорные компании и инвестировать в криптовалюты, чтобы избежать формальностей при легализации бизнеса в иностранных юрисдикциях. Мошенники убеждают своего нового клиента, что их цель исключительное, альтруистическое желание поделиться своими навыками инвестирования и увеличить средства

[1] *Binance* (Бинанс) – крупный онлайн-сервис обмена цифровых валют, блокчейн-система и поставщик инфраструктуры для криптовалютной отрасли с комплексом продуктов, среди которых – торговля цифровыми активами, инвестиции, децентрализация и инфраструктурные решения.

клиента. Иногда оговаривается некий процент от полученной прибыли либо предлагается самостоятельно оценить помощь и соответствующий размер ее вознаграждения, т. е. действовать на усмотрение клиента.

Получив одобрение своего нового клиента, злоумышленник предоставляет ему адрес для пополнения, который может выглядеть следующим образом: TFrT3EMHdroQ6YSwLZtSLuWxFEbMbLibnE, введя в заблуждение относительно того, что представляемый адрес и есть тот самый субаккаунт Binance. В действительности же представленный клиенту адрес – это адрес в блокчейне *TRON*[1] и принадлежит злоумышленнику. Предложенную платформу, как правило, используют для оплаты контента, к которому пользователи хотят получить доступ. Оплата идет непосредственному создателю адреса. Клиент пополняет этот адрес на некую сумму в токенах *USDT*[2], после чего мошенник пропадает и перестает отвечать на сообщения. Созданный субаккаунт оказывается недоступным клиенту, размещенные на нем финансовые средства исчезают. Обманутый инвестор обращается к правоохранителям с целью восстановления своих нарушенных прав и возмещения причиненного вреда.

Документально оформив обращение «горе-инвестора», сотрудник ОВД приступает к расследованию совершенного преступления по следующему алгоритму:

1. Проверяет адрес, указанный мошенником как субаккаунт *Binance*. Как правило, выясняется, что это обычный пользовательский адрес, не имеющий никакого отношения к бирже.

2. Проводит анализ транзакций (перевода финансовых средств через несколько адресов) на предмет выявления электронного кошелька, с которого преступник вывел финансовые активы. Вывод средств, как правило, происходит через некрупный обменник[3], кото-

---

[1] *TRON* – Блокчейн-платформа, ориентированная на масштабируемость и высокую пропускную способность, предназначенная для цифрового контента и развлечений. Низкие комиссии и высокая скорость транзакций.

[2] *USDT (Tether)* – токен (англ. – «привязь», «привязывать»), курс которого равен (привязан) одному доллару США в пропорции 1:1.

[3] Обменник – это сервис для покупки или продажи цифровых активов, в том числе за фиат. Подобные площадки отличаются от бирж или P2P-операций: разовым характером транзакций (в основном для «входа» на рынок и «выхода» в фиат); автоматизацией (может быть автоматизирован при помощи программного обеспечения, что повышает удобство как для владельца, так и для пользователя); подтвержденной репутацией (например, при помощи отзывов, оценок агрегаторов и пользователей, в то время как при использовании P2P-сервисов клиенту приходится «верить на слово» контрагенту); большим числом платежных инструментов (обменные сервисы поддерживают методы оплаты, недоступные на биржах или P2P-платформах).

рый фиксирует всю цепочку интересующих нас транзакций вплоть до вывода на *Qiwi*-кошелек, что позволяет установить номер телефона, используемого преступником в схеме. Если финансовые средства посредством серии транзакций были выведены на централизованную биржу (например, *OKEx*[1] или любую иную), то у правоохранителей появляется возможность получения персональных данных преступника (рис.1).

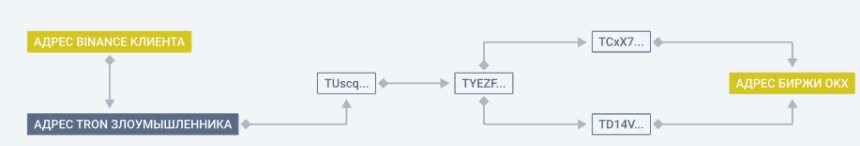

Рис. 1. Схема получения персональных данных преступника

Фиксация факта вывода размещенных пострадавшим финансовых активов на *Qiwi*-кошелек или через централизованную биржу является достаточным основанием для принятия решения о возбуждении уголовного дела по ст. 159 УК РФ (мошенничество).

3. Факт возбуждения уголовного дела выступает законным основанием для служебного обращения в сервисы *Qiwi* и *OKEx* в целях получения интересующих следствие сведений о схеме транзакций, используемом телефонном номере, персональных данных лица, осуществившего вывод финансовых активов, с последующей реализацией стандартной методики проведения следственных действий и оперативно-розыскных мероприятий.

Основной акцент рассмотренного алгоритма состоит в проведении блокчейн-анализа, целью которого является выявление аффилированных и/или принадлежащих преступнику адресов, ведущих на централизованную платформу для торговли крптовалютами либо на *Qiwi*-сервис.

Рассмотренная нами практическая ситуация может получить развитие в несколько ином контексте, например, когда по совету «преступника-консультанта» приобретенные потерпевшим токены отправляются с биржи не на свой адрес, а в пул ликвидности на *PanCake Swap*[2] в пару *Sweat Coin -BUSD*[3]. После ввода средств

[1] *OKEx* – инновационная криптовалютная биржа с расширенными финансовыми услугами.

[2] *PancakeSwap* – это децентрализованный сервис обмена, работающий в сети Binance Smart Chain, со множеством других функций, которые позволяют получить и выиграть токены.

[3] BUSD (Binance USD) – это стабильная монета, привязанная к доллару США в соотношении 1:1.

отмеченный пул показывает (демонстрирует) значительный рост в стоимости, а, значит, существенный заработок для участников, что порождает у него уверенность в действительности (легальности) транзакции. Иными словами, потерпевший действительно «наблюдает» в цифровом выражении возросшие активы – вознаграждение в токенах *BUSD*, однако на самом деле цифры, фиксирующие вознаграждение, фиктивны и не имеют ничего общего с действительной ситуацией. Это становится понятно жертве в тот момент, когда она попытается вывести токены снова на Binance. Биржа (*Binance*) отказывает в приеме токена, поскольку обнаруживается его неоригинальность, т. е. отсутствие схожести со смарт-контрактом. Предлагаемая для вывода Sweat Coin оказывается скам-монетой, созданной тем же самым мошенником.

Обман в рассматриваемой схеме заключается в подмене *USDC*-токена скам-токеном[1] *USDC*. Если правильный смарт-контракт токена *USDC* выглядит следующим образом: «0x8AC76a51cc950d 9822D68b83fE1Ad97B32Cd580d», то смарт-контракт скам-токена *USDC* выглядит как «0x926292794C0bc2FB9ab2238c59E1485d86645 EB7», что по факту слабо различимо. В результате оказывается, что пострадавший вложил настоящие ЦФА в поддельный пул ликвидности и получил прибыль в скам-монете. И монета и пул ликвидности были созданы преступником, презентовавшим себя коучем, ментором, экспертом, советником в области криптоинвестирования, консультантом академии и т. д. Как правило, блокчейн-анализ, проведенный по сайту академии мошенников (*fatherinvestments.com*), показывает, что данные не соответствуют стране нахождения потерпевшего. Данные для регистрации были новыми и не содержали сведений и информации о преступнике. Платной рекламой сайта не он пользовался, соответственно, платежные реквизиты не всегда удается установить, а Телеграм-аккаунт мошенника зачастую создается по фиктивным персональным данным, что значительно затрудняет поиск и получение информации о преступнике.

В этом случае алгоритм расследования следует дополнить следующими позициями:

1. Блокчейн-анализ должен проводиться в целях выявления адреса преступника, контактировавшего с кошельком жертвы. В результате может быть выявлена крупная сеть поддельных пулов ликвидности и/или копий популярных токенов, длительное время работающих по описанной схеме. Вот, как она может выглядеть (рис. 2):

[1] Скам-токены – это фальшивые криптовалюты , которые создаются мошенниками с целью обмана пользователей и завладения их цифровыми финансовыми активами (ЦФА).

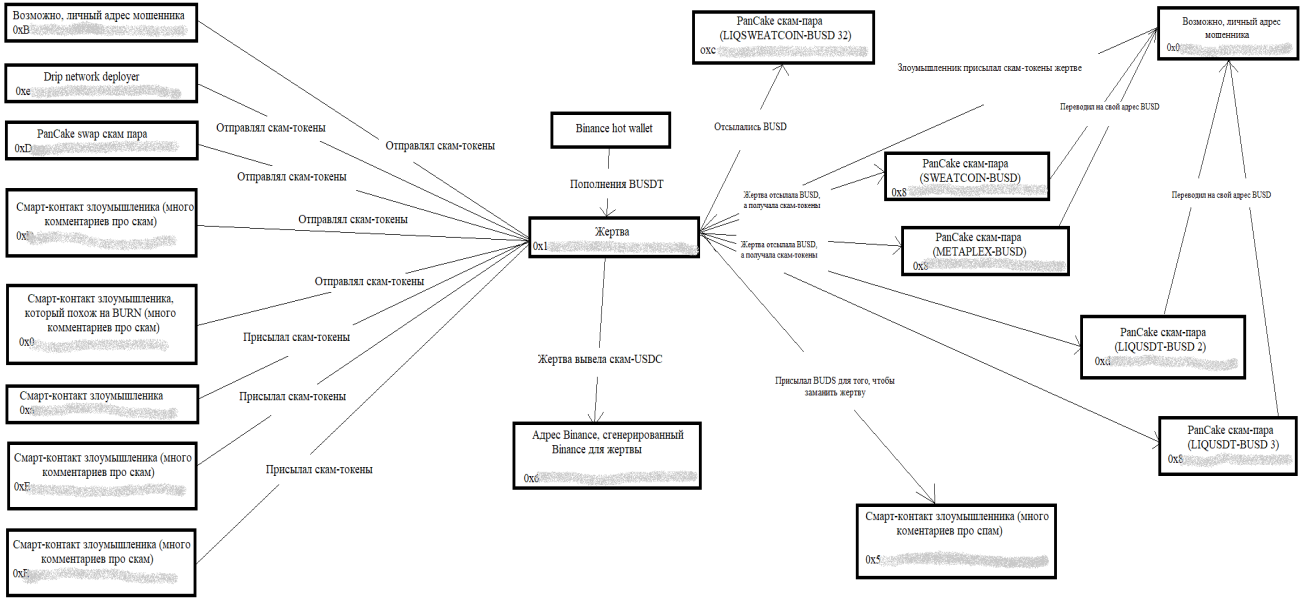

Рис. 2. Сеть поддельных пулов ликвидности и/или копий популярных токенов

Следует обратить внимание на темно-зеленый цвет (потерпевший) и розовые цвета (мошенник). Потерпевший отправляет в пул настоящие *BUSD* → пул получает в качестве обратной связи скам-вознаграждение. Настоящие же *BUSD* переводит на адрес мошенника. Обилие таких адресов говорит о том, что мошенники создали множество пар и пулов для хищения средств, что возможно отследить по содержанию комментариев к адресам, указывающим на скам. Фиксация подобной ситуации является достаточным основаниям для принятия решения о возбуждении уголовного дела по ст. 159 УК РФ (мошенничество).

2. Последующая задача правоохранителя состоит в том, чтобы обнаружить несколько выводов средств на биржу *Binance* с адреса преступника. Наличие возбужденного уголовного дела позволяет составить официальное обращение на биржу для блокировки средств и предоставления данных преступника.

3. Параллельно продолжается поиск других возможных жертв мошеннической сети для их оповещения в целях информационного противодействия мошенническим действиям и предупреждения новых преступных фактов. В блокчейн-эксплореры пишутся запросы для маркировок адресов, пулов и монет мошенника как скам-проекты. Это поможет другим пользователям блокчейн-сетей увидеть эту маркировку и не потерять свои финансовые средства.

4. Адрес преступника подвергается регулярному (постоянному) мониторингу для получения сведений о дальнейших движениях ЦФА. Следует заметить, что это огромный объем работы. Так, согласно отчету Angara Security только в 2023 г. в российском сегменте интернета было зарегистрировано около полторы тысячи доменов, связанных с инвестициями в ЦФА, из которых 697 (или 47 %) в настоящее время неактивны (заблокированы, выставлены на продажу, пустые и т. п.) [2].

В качестве итогов проведенного исследования, следует обратить внимание на необходимость законодательного регулирования, а существующие промедление и нерешительность в этой части лишь порождает рост организационных проблем. В то время как государственные законодательные органы вырабатывают общее мнение относительно развития крипторынка в России, определяются со статусом цифровой валюты, проектируют и предлагают механизмы регулирования крипторынка, рассматривают варианты лицензирования деятельности и регистрации всех провайдеров услуг виртуальных активов (криптобирж, обменников, майнинг пулов), определяют субъектов регулирования и их полномочия, для правоохранительных органов очень важно сохранять организаци-

онную активность в части мониторинга криптовалюты, выявления финансовых рисков, мошенничеств, преступных транзакций и скам-проектов, вырабатывать технологические решения информационного противодействия цифровому мошенничеству в сфере частного инвестирования, что заставляет действовать на опережение и инициативно (самостоятельно) выстраивать взаимоотношения с централизованными криптобиржами, финансовыми сервисами и приложениями в целях эффективного выполнения возложенных на органы внутренних дел функций по предотвращению преступлений, их выявлению и раскрытию.

Список литературы:

1. В CoinGecko назвали самые доходные в 2023 году криптовалюты из топ-100. URL: https://www.rbc.ru/crypto/news/658ebcff9a79472da89d1142?from=copy (дата обращения: 21.03.2024).

2. Годовой отчет «Глобальная криптовалюта. Обзор индустрии и трендов». URL: https://www.rbc.ru/crypto/news/639310fd9a79470919f50130?from=copy (дата обращения: 04.03.2024).

3. Новости криптовалют. URL: https://amp.rbc.ru/crypto/news/65aa54c69a79475266e880d7 (дата обращения: 25.03.2024).

4. Число связанных с криптовалютами приговоров в России выросло на 5000 %. URL: https://www.rbc.ru/crypto/news/65784c179a79478632728c92?from=copy (дата обращения: 14.03.2024).

5. Эксперты назвали долю россиян с низким уровнем финансовой грамотности. URL: https://amp.rbc.ru/rbcnews/finances/30/03/2024/66071ec39a79473fe8dac5f2?utm_source=amp_textincutes (дата обращения: 14.03.2024).

6. Chainalysis in Action: How Law Enforcement Tracked Millions' Worth of Illicit Bitcoin in the Harmon Brothers Cases. URL: https://www.chainalysis.com/blog/helix-mixer-harmon-brothers-investigation (дата обращения: 06.03.2024).

7. JP Morgan: 78 % институционалов не планируют вести криптоторговлю. URL: https://ru.investing.com/news/cryptocurrency-news/article-2366451 (дата обращения: 04.03.2024).

8. The world's largest 500 asset managers. Thinking Ahead Institute. URL: https://www.thinkingaheadinstitute.org/content/uploads/2022/10/PI-500-2022_final_1013.pdf (дата обращения: 04.03.2024).

Михаил Валерьевич Леминов,
преподаватель кафедры профессиональной подготовки
Восточно-Сибирский институт МВД России
E-mail: leminov.mv@mail.ru

УДК 004 05.25.05

Информационное общество

Аннотация

Актуальность темы определяется стремительным развитием цифровых технологий и их влиянием на все сферы жизни человека. В данной статье кратко рассматриваются различные определения и концепции информационного общества, обсуждаются его характеристики.

Ключевые слова и словосочетания: *информационная экономика; информационное общество; цифровая трансформация; искусственный интеллект; информационные технологии.*

Информационное общество с его стремительными изменениями и необычайной скоростью обмена информацией стало ареной глубоких преобразований. Информационное общество, которое в настоящее время основано на разработке и использовании высокотехнологичных средств коммуникации, влияет на все аспекты нашей жизни: от экономики и науки до культуры и образования.

Информационное общество – это общество, в котором электронные информационные технологии в основном облегчают производство, распределение и потребление товаров и услуг.

Она характеризуется широким доступом граждан к оцифрованной информации, интерактивностью в общении и изменениями в социальных организациях, обусловленными технологическими усовершенствованиями [2].

Примером информационного общества может служить широкое использование смартфонов и мобильных приложений. Благодаря смартфонам люди могут получать доступ к различным видам данных «на лету», доступ к которым ранее можно было получить только через просмотр определенных страниц в компьютере.

Теперь всего несколькими нажатиями на телефоны можно совершать транзакции с коммерческими организациями или удаленно общаться с коллегами, пользуясь разнообразными предло-

жениями. В целом информационное общество открывает множество возможностей, одновременно создавая новые вызовы, которые могут потребовать от общества решения для раскрытия потенциала таких технологий.

В современном мире информация становится одним из факторов развития общества. В условиях глобализации происходит ряд изменений в экономической, политической, военной, культурной, образовательной и многих других областях. Картина мира и взаимоотношения между отдельными государствами, народами, группами меняются. Причиной всему этому является появление новых информационно-коммуникационных технологий и развитие существующих.

Новые технологии, такие как интернет, ведут к глобализации всего мира. Информация распространяется с беспрецедентной скоростью и достигает самых отдаленных уголков мира, тем самым коренным образом изменяя картину мира и происходящих в нем событий.

Одно из научных определений понятия информационного общества, предложенное Мануэлем Кастельсом, гласит, что информационное общество – это социальная структура, характеризующаяся сетью цифровых технологий, которые генерируют, обрабатывают и распространяют информацию. Это предполагает экономику, основанную на знаниях, где рабочие процессы интегрированы с информационными технологиями и коммуникационными сетями [5, с. 55].

Информационное общество – это социально-экономическая система, в которой производство и обмен товарами и услугами в основном осуществляются с помощью цифровых средств массовой информации, таких как компьютеры или другие электронные устройства.

Эта интеграция информационных технологий (ИТ) в социальную и деловую практику общества создает новые возможности для потребления, распределения и совместного использования (например, рост электронной коммерции), одновременно ускоряя способы и каналы коммуникации между людьми, охватывающими географические регионы, тем самым ускоряя технологическую глобализацию.

По мнению Г. В. Жигуновой и В. В. Синицына, термин «информационное общество» в настоящее время является наиболее распространенным способом обозначения совокупности воздействий и социальных последствий новых информационно-коммуникационных технологий [3, с. 137].

Мы живем в постоянно развивающемся обществе, основанном на информации. Следствием этого является зависимость человека от информации. Люди принимают решения на основе информации, которую получают из различных источников.

Информация обозначается как фактор развития, то, что при правильном использовании принесет прогресс определенному обществу, определенному государству. Именно из-за этого все больше вкладывается в информационно-коммуникационные системы, в создание информационных служб документации, развитие и обучение специалистов по информационным коммуникациям, построение общества на основе знаний.

Информационная деятельность возникает и развивается в результате роста знаний и (научных) публикаций; между информацией и знанием есть различия. Знание – это структура понятий, связанных их отношениями, а информация –небольшая часть такой структуры [1, с. 193]. Вторая группа аргументов говорит о развитии информации как средства коммуникации. Информация и знания не являются одинаковыми категориями, те, кто владеет информацией, определяют, какие знания будут преобладать в обществе.

Не все общества одинаково подходят к информации. Западные общества чаще всего рассматривают развитие общества через техническую и технологическую часть, игнорируя другие важные детерминанты развития общества, такие как культурная, ценностная и т. д. В то время как другие страны (например, Япония) подходят к знаниям с точки зрения культурного измерения, а наука и техника следуют только этому культурному измерению. В Японии считается, что информационное общество является лишь одной из форм развития их общества, в то время как Запад начинает с совершенно иной точки зрения: культура стремится к технологии [6, с. 5].

Информационное общество – это не общество, которое дает неограниченную свободу для распространения и получения информации, оно просто позволяет находить большой объем информации, открывает различные способы получения информации, учит различным способам применения информации.

Информационное общество – это общество, основанное на информации, как основной источник энергии сегодняшнего дня. Точно так же, как на протяжении всей истории были различия, в которых преобладали отдельные источники энергии, такие как вода, газ, нефть и т. д. В современном мире источником энергии служит информация. Разница между «ценностями», которые имели большое значение в прошлом (некоторые до сих пор имеют), и информацией заключается в том, что информация не имеет срока

годности, она безгранична и может только увеличиваться без риска исчезновения.

Центральным элементом информационного общества, основанного на широком участии, является доступ к информации. Каждый человек становится активным участником обмена информацией в связи с широким распространением Интернета и мобильных технологий. Соответственно, объем информации, которую мы потребляем ежедневно, достигает рекордных уровней, а скорость ее распространения беспрецедентна в истории [4, с. 208].

Современные технологии облегчают взаимодействие и обмен мнениями на международном уровне. Сообщества формируются не только на основе географических или социокультурных особенностей, но и на основе общих интересов и идей. Виртуальные сообщества, социальные сети и другие онлайн-платформы позволяют людям из разных уголков мира объединяться и обмениваться идеями вне зависимости от пространственных ограничений [5, с. 55].

Информационное общество передает не только правдивую информацию, но и дезинформацию. С целью дальнейшего развития информационного общества, важно прилагать усилия для сокращения количества дезинформации. Если информационное общество будет способствовать распространению дезинформации, тогда это будет дезинформационное общество, а не информационное. Если мы хотим построить информационное общество, мы должны руководствоваться позитивными ценностями, которые будут способствовать человеческому прогрессу с точки зрения улучшения жизни и ее условий и содействовать новым открытиям, которые облегчат повседневную жизнь, обеспечат лучшие и более качественные условия.

Итак, информационное общество – это социально-экономическая структура, которая относится к переходу от индустриального образа жизни к такому, где преобладают данные, информация и услуги. Основные черты информационного общества вращаются вокруг использования и распространения информации с помощью цифровых технологий.

Список литературы:

1. *Гринева О. А.* Информационная перегрузка человека в информационном обществе // Миссия конфессий. 2022. № 65.

2. *Давудов Д. А., Спикина Т. В.* Человек в информационном обществе и информационном государстве // Цифровая наука. 2020. № 5.

3. *Жигунова Г. В., Синицын В. В.* Инновации в России: основные проблемы // Экономика и бизнес: теория и практика. 2024. № 1-1.

4. *Орлов С. В.* К вопросу об основных подходах к изучению формирования информационного общества в России // Клио. 2024. № 2 (206).

5. *Птицына С. С.* Теория сетевого общества М. Кастельса: теоретикосоциологический анализ // Всероссийский журнал научных публикаций. 2011. № 3 (4).

6. *Умарова Н. Р.* Стратегия развития информационного общества // Наука и образование сегодня. 2020. № 2 (49).

Владимир Александрович Минаев,
доктор технических наук, профессор,
профессор кафедры специальных
информационных технологий
Московский университет МВД России
имени В. Я. Кикотя
Email: m1va@yandex.ru

Александр Владимирович Мокшанцев,
кандидат технических наук, доцент,
заместитель начальника кафедры
информационных технологий
Академия государственной
противопожарной службы МЧС России
Email: mok-av@yandex.ru

УДК 004.94

Системное описание оперативной обстановки по линии служб чрезвычайного реагирования

Аннотация

Рассматривается оперативная обстановка как системный объект, в рамках которой происходит управление службами чрезвычайного реагирования (СЧР). Обсуждаются системные признаки оперативной обстановки. Показано, что имеется отставание аналитического инструментария, которым располагают СЧР, от уровня их информационно-методического обеспечения. Делается вывод, что математическое моделирование выступает ключевой методологией решения аналитических задач СЧР.

Ключевые слова и словосочетания: *служба чрезвычайного реагирования; оперативная обстановка; моделирование; аналитическая работа.*

Современное понимание оперативной обстановки является принципиально важным в сфере организации деятельности служб чрезвычайного реагирования (СЧР), к которым относятся ряд подразделений полиции, МЧС и других. Нужно отметить, что по линии МВД существует историческая преемственность и содержательная совместимость дефиниций «*оперативная* и *криминогенная* обста-

новка». В работах, где проведено сравнительное исследование указанных определений, показана эквивалентность их применения.

В последние годы в связи с возрастающей потребностью более эффективного управления подразделениями служб чрезвычайного реагирования существенно усилилась необходимость целенаправленного анализа, оценки и прогнозирования оперативной обстановки (ОО). Развитию современных моделей и методов управления значительно способствовали усилившиеся возможности информационно-коммуникационных технологий и математического аппарата количественной обработки данных о процессах, происходящих в современном обществе.

Но сегодня, с одной стороны, имеется значительное отставание аналитического инструментария, используемого в практической деятельности СЧР, от уровня информационно-методического обеспечения подобных структур ведущих зарубежных стран. А с другой – современные информационные системы СЧР располагают огромными, но не всегда в достаточной степени реализуемыми возможностями. Эти возможности позволяют обеспечить «добывание» более глубокой аналитической информации о постоянно эволюционирующей ОО, предупреждение новых опасных тенденций в ее развитии, а также опережающее противодействие таким современным явлениям по линиям СЧР – киберпреступности и деструктивной идеологии в социальных медиа.

Именно ОО как главный объект практического анализа фактически включает в себя все многообразие различных сторон объективной действительности, которые учитываются и оцениваются в процессе организации деятельности СЧР.

Поэтому совершенно естественно, что проблемы изучения и оценки оперативной обстановки нашли в научной литературе довольно широкое освещение [1–16]. Многие из имеющихся в этой сфере разработок на соответствующих этапах их создания, применения и оценивания оказали существенное влияние на практику управленческой деятельности СЧР, способствовали улучшению качества аналитической работы.

При разработке методологии математического моделирования ОО в указанных выше работах выделены следующие аспекты:

– особенности обслуживаемой СЧР территории (объекта) в зависимости от линии реагирования (состояние преступности, характеристики пожарной обстановки, наличие и состояние сил и средств чрезвычайного реагирования);

– условия, в которых происходит деятельность СЧР по реагированию на ситуацию;

– совокупность явлений, факторов, обусловливающих возможность возникновения чрезвычайных ситуаций;

– совокупность данных, характеризующих состояние и динамику чрезвычайной ситуации, эффективность использования сил и средств при ее ликвидации.

Системные признаки оперативной обстановки. Характерным признаком для процесса моделирования ОО является выраженный функциональный подход. При этом отмечается уход от простых подходов и методов, применявшихся в области теории и практики исследования ОО, к выработке качественно нового подхода, использованию более сложных и глубоких методов и средств.

Это тогда и в настоящее время обусловливалось объективными изменениями окружающей действительности, возрастанием уровня требований к деятельности СЧР и ее конечным результатам, развитием взаимодействия социальных и естественных наук, внедрением современных технологий обработки и анализа информации.

Результаты изучения ОО играют основную роль при обосновании и выработке управленческих решений в СЧР; они позволяют рационально использовать имеющиеся ресурсы, осуществлять конкретные мероприятия по оптимизации деятельности служб и повышению их влияния на ЧС. При этом создаются предпосылки для решения задач прогнозирования развития ЧС, происходит выбор основных направлений деятельности СЧР, оценивается эффективность функционирования их систем.

Сложность ОО и многогранность практических задач, связанных с ее изучением и оценкой, объективно предопределяют целесообразность разработки новых концепций избранного объекта исследования на основе системной методологии. Ценность системного подхода заключается в возможности, несмотря на огромное разнообразие различных явлений и процессов, применить к исследованию общие концептуальные схемы, использовать единый формально-логический аппарат и получить на этой основе новые результаты, относящиеся к объекту анализа – оперативной обстановке по линии деятельности различных СЧР.

Поэтому исследования в данной области на предметно-содержательном уровне должны быть ориентированы на разработку системы моделей ОО, позволяющих анализировать механизмы ее изменения, связи и зависимости между различными процессами, выявлять требуемые закономерности и обеспечивать возможности компьютерного «проигрывания» различных управленческих ситуаций.

С помощью рассматриваемой методологии описания между всеми сторонами реальной действительности могут быть прослежены и исследованы функционально ориентированные связи, которые влияют на деятельность СЧР. Следовательно, представляется возможность рассматривать ОО как систему и на основе системного подхода проводить разносторонний анализ этого объекта и его свойств.

Представим важные стороны теоретического осмысления свойств ОО: системную целостность; проявление сложности; динамичность и устойчивость; гомеостаз; структуру. Охарактеризуем их особенности.

Наиболее существенным проявлением отношений между элементами сложного образования часто считается его *целостность*, служащая одновременно и определяющим признаком системы. Нередко реальные объекты и процессы, принадлежащие к разным целостным образованиям, могут влиять на действия СЧР только в определенном сочетании и взаимодействии, в том числе и случайном (например, обстоятельства совершения отдельных преступлений либо условия возникновения конкретного крупного пожара).

Ключом к пониманию целостности ОО, определенным критерием выделения ее элементов служит признак их *относимости* к деятельности СЧР. Это значит, что ОО составляют только те объекты, явления, процессы или их отдельные стороны, которые в той или иной форме существенно влияют на эту деятельность. При этом они также вступают во взаимодействие (в самом широком смысле) с иными «участниками», определяя условия и параметры функционирования СЧР, т. е. имея значимое отношение к их деятельности.

Критерий относимости имеет выраженный функциональный характер. Именно через относимость проявляется диалектическая взаимосвязь деятельности СЧР, как части системы государственного управления, с другими сферами деятельности государства, которые в той или иной мере влияют на выполнение задач СЧР; с различными элементами среды их функционирования

В качестве системообразующего критерий относимости позволяет сохранять четкое представление целостности обстановки в ее функциональных вариантах: при различных направлениях или линиях деятельности; уровнях управления (от центрального органа до объекта оперативного обслуживания); в зависимости от стратегического, оперативного или тактического характера задач; а также с учетом полноты влияния конкретных объектов на выполнение функций СЧР.

Благодаря использованию критерия относимости появляется возможность целостного представления ОО в динамике. Это прежде всего категория настоящего (в значительной части охватывающая прошлое и уже сформировавшееся состояние элементов обстановки) и определенный «потенциал», который определяет условия и параметры последующего функционирования СЧР.

Определение нашего системного объекта предполагает выделение его из окружающей среды, что сопряжено с известными сложностями. Дело в том, что условия, определяемые по отношению к деятельности СЧР – это социально-экономическая среда, население, входящие в содержание самой оперативной обстановки и другие ее компоненты. При этом «границы» между оперативной обстановкой и средой имеют достаточно подвижный характер.

Проявление сложности. Одним из важных признаков, свойственных объектам системного исследования, является *сложность* ОО. Сложность характеризуется тем, что составляющие ОО реальные объекты и явления отличаются большим разнообразием по своей природе (население, экономика, природные и иные компоненты) и разной степенью внутренней упорядоченности. Сложное переплетение в одной системе объектов различной природы не позволяет отнести ее к какому-то одному классу систем (механическим, биологическим, социальным и т. д.), предопределяя тем самым необходимость исследования свойств разнообразных взаимодействующих компонентов.

Сложность обусловлена и характером отношений между элементами ОО: действием связей самой различной природы; наличием множества прямых и обратных связей; множеством вариантов их сочетаний; одновременными проявлением случайного и необходимого. Особенностью взаимодействий в системе, отражающей ОО, является и то, что некоторые объекты воздействия СЧР, например, лица, замышляющие и подготавливающие совершение преступлений, нередко предпринимают специальные меры к недопущению прохождения или искажению информации.

Любой человек и общество в целом одновременно находятся в сфере воздействия самых разнообразных систем и реализации различных процессов. В ОО также наблюдается огромное разнообразие контуров воздействия, а их характер и направленность могут варьироваться вплоть до противоположности (например, многоаспектность и противоречия борьбы с пьянством).

Известная относительность познания объективной действительности и неадекватность ее отражения в понятиях и представлениях составляют сущность *познавательного аспекта* сложности

ОО. Значима и степень неопределенности ОО, в частности, связанной с наличием латентной преступности, непознанных или малоизученных иных криминогенных явлений.

Сложность также связана с ситуативностью включения в обстановку многих компонентов, нередко даже случайных (например, неосторожных дорожно-транспортных происшествий), а порой обусловлена принятием нарушителями специальных мер маскировки, уничтожения следов, дезинформации. Отсюда очевидна необходимость у познающего субъекта специальных знаний и навыков распознавания относимых компонентов и их признаков, сущности их связей.

В результате из-за невозможности анализа всего целостного объекта осуществляется оперирование неполными сведениями о его элементах, компенсируя «белые пятна» общими и профессиональными знаниями, а в некоторых случаях – предположениями и косвенными оценками.

С учетом отмеченной сложности в результате системного описания и анализа ОО представляется возможным подойти к постановке и решению задач на основе многомерных моделей, способных учесть ее основные параметры, в том числе – скрытые связи и структуру.

Динамичность ОО интерпретируется как постоянно меняющееся реагирование СЧР на вновь возникающие сигналы – происшествия, чрезвычайные обстоятельства, антиобщественные отклонения в поведении, нарушении специальных норм и т. д. Но наряду с этим имеется существенное изменение некоторых компонентов оперативной обстановки в результате реагирования (и не только системы СЧР) на всевозможные ее изменения. В итоге совокупное проявление компонентов отражается в динамике процессов, которые наиболее существенно характеризуют саму ОО в целом.

При всем разнообразии темпа, характера и даже направленности изменений различных элементов ОО она в целом сохраняет основные соотношения, свою *качественную устойчивость*. Колебания более всего заметны на низовых уровнях управления, на коротких отрезках времени и, как правило, сглаживаются при увеличении количества наблюдений. В этом проявляется свойство *гомеостазиса*.

Структурные свойства. Любую систему можно охарактеризовать как некоторую структуру в движении (развитии). Именно структура или внутреннее строение системы создает общий качественно-определенный и относительно устойчивый порядок внутренних пространственно-временных связей и отношений между

подсистемами. Этот порядок определяет функциональное проявление данной системы и характер ее взаимодействия с другими системами и окружающей средой.

Понятие ОО определяется через деятельность СЧР и наоборот. Следовательно, в ее структуру всегда включаются субъекты деятельности – сами СЧР, реализующие определенный масштаб и уровень решаемых задач.

Любое проявление деятельности СЧР (от общего до частного, единичного) обусловливается частными или суммарными, обобщенными действиями других сил. Прежде всего, это – люди (нарушающие какие-либо нормы) или силы природы (создающие чрезвычайные, опасные обстоятельства для жизни и здоровья людей, сохранности материальных средств). Данная совокупность объектов составляет «противодействующую сторону» в ОО, и в известном смысле, и в определенных пределах, является объектом воздействия СЧР. Перечень ее конкретных проявлений (поведение, развитие) обладает широкими возможностями вариаций, но сама «противоборствующая сторона» с ее прошлым, настоящим и будущим состоянием и активностью обязательно присутствует в структуре ОО.

Наконец, всякая деятельность, как и развитие предметов и явлений неодушевленных, имеют пространственно-временные координаты, конкретную физическую и социальную среду и конкретные обстоятельства времени, проявляющиеся как социально-исторические условия с их собственной сложной структурой. Поэтому следует учитывать *иерархию* подсистем, которые, в свою очередь, составлены из блоков ОО одного порядка и имеют свойства внутренней структуры.

В результате изложенных положений ОО предстает как система взаимодействующих и взаимосвязанных элементов, существуя объективно. Ее содержание приобретает относительно субъективный характер в том смысле, что отбор элементов, образующих систему ОО, производится исследователем (ученым или практиком СЧР) в соответствии со стоящими перед ним задачами и его представлениями о значимых для их решения сторонах объективной действительности.

На формирование содержательного представления об основных элементах и связях оперативной обстановки может оказать влияние выбор методов ее изучения. Так, еще Р. Шеннон отмечал, что различные методы анализа одного и того же объективного процесса или явления могут привести к созданию весьма отличающихся концепций реальных систем. Поэтому системное исследование ОО

в зависимости от различных аспектов и методов ее анализа предполагает построение различных логических схем описания реального объекта.

Будучи основной методологической предпосылкой моделирования, системный подход служит своеобразным мостом между реальной ОО и моделями ее изучения. Если ОО как реальный объект изучения, представима различными системами, так и каждая из них может служить основанием для построения моделей, отличающихся как конкретными средствами, так и адекватностью. Исходя из сказанного, представление о возможности создания некой универсальной модели ОО лишено оснований. Речь может идти о разработке множества взаимодополняющих моделей и их применении для изучения ОО.

Ведущим фактором воздействия на функционирование СЧР является оперативная обстановка со всем сложным комплексом ее характеристик. Именно она выступает предметом тщательного изучения, анализа, оценки и прогнозирования, поскольку полученные при этом результаты создают базу формирования эффективных управленческих решений по надежному функционированию территориальных СЧР, определяют смысл, последовательность, качественные и количественные параметры использования сил и средств с реальными негативными изменениями оперативной обстановки.

Аналитическое исследование статистических и иных сведений, отражающих состояние оперативной обстановки, осуществляется органами СЧР с использованием различных методов и средств математического обеспечения. Среди математических возможностей все более значимое место для решения указанных задач занимает математическое моделирование, позволяющее глубоко и разносторонне обеспечивать современный анализ огромного массива сведений об оперативной обстановке, системно решая частные задачи управления, в том числе используя имитационное моделирование.

Математическое моделирование в настоящее время выступает как система разнообразных практических применений в аналитической деятельности структур СЧР [12; 13].

Список литературы:

1. *Брушлинский Н. Н.* Системный анализ деятельности государственной противопожарной службы: учебник. Москва: МИПБ МВД России, 1998. 255 с.

2. *Герасимов В. В.* Оценка оперативной обстановки: цели, задачи, пути совершенствования // Вестник МВД России. 2006. № 5.

3. *Гилинский Я. И.* О системном подходе к преступности // Правоведение. 1981. № 5.

4. *Гончарова М. В. [и др.].* Комплексный анализ состояния преступности в РФ по итогам 2020 г. ожидаемые тенденции ее развития: аналитический обзор. Москва: ФГКУ ВНИИ МВД России, 2021.

5. *Ипакян А. П.* Оперативная обстановка: методологические вопросы моделирования: учебное пособие. Москва: Академия МВД СССР, 1982. 87 с.

6. *Кларк Р.* Преступность в США. Москва: Прогресс, 1975. 422 с.

7. *Клушин О. З.* Оперативная обстановка: понятие, анализ, прогноз: учебное пособие. Москва: Академия управления МВД России, 2009.

8. *Кузнецова Л. В., Миронов Е. В., Бояркин А. Б.* Аналитическая работа в территориальных органах МВД России на районном уровне: учебно-методическое пособие. Барнаул: ФГКОУ ВО «Барнаульский юридический институт Министерства внутренних дел Российской Федерации», 2017. 51 с.

9. *Меньших В. В., Горлов В. В.* Оптимизация действий органов внутренних дел при чрезвычайных обстоятельствах криминального характера // Информационная безопасность регионов. 2014. № 3.

10. *Минаев В. А.* Кадровые ресурсы органов внутренних дел: современные подходы к управлению. Москва: Академия МВД СССР, 1991. 161 с.

11. *Минаев В. А., Бондарь К. М.* Опыт и перспективы математического моделирования криминогенной обстановки // Криминологический журнал. 2022 (1).

12. *Минаев В. А., Бондарь К. М., Дунин В. С., Скрипко П. Б.* Математические модели анализа, оценки, прогнозирования и управления в органах внутренних дел: монография. Хабаровск: ДВЮИ МВД России, 2022. 308 с.

13. *Минаев В. А., Бондарь К. М., Рабчевский А. Н., Федорович В. Ю.* Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: монография / под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: ДВЮИ МВД России, 2023. 232 с.

14. *Минаев В. А., Курушин В. Д., Захаров Д. В.* Математическое моделирование региональных криминологических процессов. Новосибирск, 1992. 159 с.

15. *Минаев В. А., Топольский Н. Г., Чу Куок Минь.* Управление пожарными рисками с использованием теории активных систем // Пожары и чрезвычайные ситуации: предотвращение, ликвидация. 2014. № 4.

16. *Goldammer J. A., Sukhinin A. I., Chiszar I. D.* The Present Wildfire Situ- ation in Russian Federation. Moscow: World Bank, 2004.

Владимир Александрович Минаев,
доктор технических наук, профессор,
профессор кафедры специальных
информационных технологий
Московский университет МВД России
имени В. Я. Кикотя
Email: m1va@yandex.ru

Евгений Андреевич Рабчевский,
директор по науке компании
СЕУСЛАБ
Email: e.rabchevskiy@seuslab.ru

УДК 004.94

Идентификация ролей пользователей в социальных медиа

Аннотация

Рассмотрена задача идентификации ролей пользователей в социальных медиа, включая их место в распространении сетевых протестных настроений. Обсуждаются основные подходы к решению указанной задачи – графовый, игровой, акциональный. Приводятся результаты распределения ролей пользователей, полученные при анализе эмпирических данных, отражающих распространение фейковой информации по темам «Жыве Беларусь» и «Дворец Путина».

Ключевые слова и словосочетания*: социальные медиа; роль пользователя; сетевое влияние; фейковая информация.*

Большинство негативных информационно-психологических воздействий сегодня наиболее эффективно достигает своей результативности (вовлечение в преступную среду, экстремистские движения, суицидальные сообщества и т. п.) посредством социальных медиа (СМ). Создаваемые при этом информационные волны, инициируемые конкретными социальными поводами, вбрасываются в сеть, усиливаются многочисленными обсуждениями, находя одобрение среди определенного контингента ее пользователей.

Организацию и поддержание требуемого вектора развития деструктивных воздействий осуществляют конкретные пользователи, играющие определенные роли в СМ. Очевидно, что наибольшее

негативное воздействие оказывают те из них, которые имеют максимальный уровень информационного влияния.

В то же время современные методики их идентификации в сетях не учитывают некоторые существенные характеристики, включая роли *ключевых пользователей* (*КП*). Идентификация ролей пользователей позволяет выявлять структуру воздействия на сеть. Анализ ролей обеспечивает выявление закономерностей информационных атак, а также признаков их целенаправленного воздействия; прогнозирование поведения сетевых структур, а на этой основе – блокирование их ключевых узлов для противодействия негативному влиянию.

Таким образом, очевидна актуальность разработки эффективных методов идентификации ролей пользователей и уровня их влияния в СМ. Это обеспечивает необходимый уровень поддержки решений при организации противодействия целенаправленным деструктивным влияниям, распространению деструктивной идеологии в пространстве СМ.

Формализация понятия ролей пользователей в социальных сообществах осуществлялась в работе [6].

Для решения задачи идентификации ролей пользователей в работах [3; 4] применялись различные методы кластеризации; в работе [8] осуществлялась нейросетевая классификация.

Важным аспектом рассматриваемой предметной области является изучение вопросов идентификации мостов в кластерных сетях [7].

Изучению проблемы идентификации КП СМ посвящены многие исследования [1].

Наиболее опасными являются такие виды влияния, какие активно провоцируют пользователей СМ на совершение противоправных действий.

В работе [5] анализируются протестные тенденции в России и делается вывод о повышении эффективности протестов при построении их по сетевому принципу, когда существенно увеличивается скорость распространения призывов к ним.

Выделяются следующие подходы в задачах выявления ролей пользователей: графовый, игровой, акциональный.

Графовый базируется на представлении сети в виде графа (вершин и ребер), реализующего модель передачи информации. Классический графовый метод направлен на прогнозирование распространения контента в сети без учета характеристик пользователей и параметров передаваемого контента.

Игровой представляет вершины графа в виде агентов, наделенных определенным набором свойств, и рассматривает возможность

объединения вершин графа в коалиции, реализуя варианты их конкурентного поведения. Игровая модель решает задачу прогнозирования распространения контента с учетом конкурентного влияния и учитывает возможность вступлений пользователей в коалицию.

Акциональный подход основан на активности пользователей в сети. Акциональная модель пытается выявить КП на основе параметров сетевой активности, т. е. по количеству опубликованных пользователями материалов.

Авторами статьи использован комплексный учет структурных характеристик и параметров активности пользователей. Для этого проведен контент-анализ СМ за выбранный период времени на определенной территории. Признаком вовлеченности является публикация пользователями в СМ материалов (постов, репостов, комментариев) целевой тематики.

В качестве примера на рис. 1 приведены распределения по шкале времени количества пользователей, создавших публикации по протестной тематике в Московском регионе в течение 2019 года.

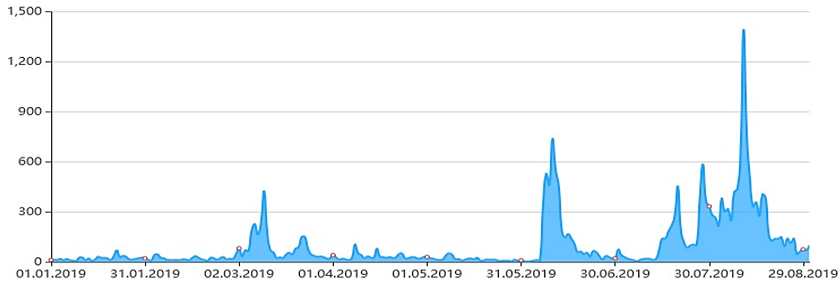

Рис. 1. Распределение количества пользователей, вовлеченных в протестное движение

Пикам распределения соответствуют наиболее крупные протестные акции, которые проходили в тот период времени. По результатам расчета формируется таблица рейтинга активности для каждого пользователя. По этим данным можно определять пользователей, играющих наиболее значимую роль применительно к исследуемому явлению.

Далее в исследовании с помощью технологии СЕУС собраны данные о пользователях, опубликовавших материалы в СС ВКонтакте по информационным поводам *«Жыве Беларусь»* (выборы президента Республики Беларусь в 2020 г.) и *«Дворец Путина»* (в начале 2021 г.), а также данные о количестве их постов, репостов

и комментариев по исследуемой тематике. В результате выявлены пользователи, которые вовлечены в целевую тематику, составив протестную сеть.

Для определения связей выявленных пользователей собраны данные об их друзьях и друзьях их друзей в сети. Такой подход объясняется тем, что количество связей очень сильно зависит от того, с кем именно связан пользователь. При одинаковом количестве друзей на первом уровне их количество на втором может различаться на порядки.

Практический опыт показал, что дальнейшее увеличение уровней в графе нецелесообразно. К тому же резко возрастает объем вычислительных ресурсов, требуемых для сбора графовой информации, построения графов.

Статистические данные по обоим информационным поводам представлены в табл. 1.

Таблица 1

Статистические данные выборки по пользователям, вовлеченным в тематику «Жыве Беларусь» и «Дворец Путина»

№	Показатель выборки	Информационный повод	
		«Жыве Беларусь»	**«Дворец Путина»**
1	Количество вовлеченных пользователей	28 447	35 502
2	Количество опубликованных материалов	42 148	61 967
3	Количество друзей и друзей их друзей	18 508 073 467	4 161 468 616

По каждой выборке сформирован рейтинг публикационной активности путем сортировки пользователей по количеству опубликованных ими материалов. Рейтинг публикационной активности по информационному поводу «Дворец Путина» представлен на рис. 2.

Как видно из рис. 2, из 35 тыс. пользователей только около 500 имеют значимое количество публикаций, что составляет 1,4 % от их общего количества в рейтинге. В том числе только первые 100 пользователей имеют уровень активности выше 20 публикаций. Остальные имеют крайне низкую активность.

Рис. 2. Рейтинг публикационной активности по теме «Дворец Путина»

Схожая зависимость рейтинга публикационной активности наблюдалась и по теме «Жыве Беларусь».

Сопоставление данных об уровне публикационной активности и количестве связей в сети показало, что наиболее активные пользователи не всегда имеют большое количество связей. В то же время пользователи с большим количеством связей, как правило, имеют невысокий уровень активности.

В каждой информационной волне, связанной с каким-либо инфоповодом, конкретные пользователи выполняют определенные роли. Одни пользователи в СС генерируют идеи, другие их распространяют, третьи комментируют, а четвертые «накручивают лайки», чтобы поднять популярность распространяемой идеи. Набор и определение социальных ролей пользователей зависят от типа сообщества и от контекста, в котором рассматриваются роли.

Для разделения пользователей на классы используются различные методы графового анализа, кластеризации или классификации. В то же время исследование различных аспектов моделей поведения пользователей не позволяет создать единый набор их ролей.

Эта же проблема проявляется и в контексте противодействия деструктивным влияниям в СС в виде организации протестного движения и мобилизации пользователей на участие в протестных акциях. В контексте противодействия в СС протестной активности граждан выделяются следующие типы ролей.

1. *Постер* – генератор идей, создатель контента. Он часто является лидером общественного мнения и при наличии большого коли-

чества связей может объединять вокруг себя большое количество пользователей.

2. *Репостер* – распространитель идей. Этот пользователь редко создает контент, а в основном репостит уже готовые публикации, нацелен на максимальное распространение чужого контента.

3. *Комментатор* – не создает контент и не репостит его, но оставляя множество своих комментариев, участвует в осуждениях и спорах. Часто создает комментарии для увеличения популярности темы обсуждения.

4. *Пассивный участник* – пользователь, который не очень активен в сети в части создания контента, репостов или комментариев. Но такой пользователь регулярно посещает различные страницы в СС, является реципиентом информации, созданной постерами, репостерами и комментаторами.

По результатам исследований авторов, параметрами, которые существенно влияют на различие пользователей по ролям и на основании которых выполнялась их классификация, выступают: возраст аккаунта, количество друзей, количество опубликованных постов, количество опубликованных репостов, количество опубликованных комментариев.

Для определения ролей пользователей решалось две основных задачи.

Первая задача состояла в том, чтобы выделить в массиве пользователей активных и пассивных. Принято, что соотношение материалов, опубликованных активными и пассивными пользователями, составляет пропорцию 7/3.

Для выявления первых рассчитан рейтинг активности путем ранжирования по убыванию суммы количества публикаций (постов, репостов и комментариев) для каждого пользователя.

Последовательно двигаясь по рейтингу вниз, подсчитывалась общая сумма материалов, опубликованных пользователями, начиная с лидера рейтинга, и сравнивалась с общей суммой материалов.

Когда сумма материалов достигла значения 70 % от общей суммы публикаций, подсчет останавливался. Затем определялся список пользователей, сумма публикаций которых составляет 70 % от общей суммы опубликованных материалов.

Результаты деления на активных и пассивных пользователей представлены в табл. 2.

Таблица 2

Активные и пассивные пользователи, вовлеченные в тематику «Жыве Беларусь» и «Дворец Путина»

№ п/п	Параметр	«Жыве Беларусь»	«Дворец Путина»
1	Всего пользователей, в том числе:	28 447	35 502
2	активных	1 257	4 847
3	пассивных	27 190	30 655

Вторая задача состояла в том, чтобы классифицировать активных пользователей по ролям постеров, репостеров и комментаторов. Принято, что пользователь играет конкретную выраженную роль, если активность в ней составляет не менее 60 % от всех видов.

В то же время среди активных пользователей выявились и те, кто не удовлетворяет правилу отсечки 60 % ни по одному из видов активности. Такие пользователи отнесены к универсалам. Данные о ролях пользователей представлены в табл. 3.

Таблица 3

Выявленные роли пользователей, вовлеченные в тематику «Жыве Беларусь» и «Дворец Путина»

№ п/п	Параметр	«Жыве Беларусь»	«Дворец Путина»
1	Всего пользователей, в том числе:	28 447	35 502
2	пассивные пользователи	27 190	30 655
3	постеры	81	531
4	репостеры	74	1 050
5	комментаторы	521	132
6	универсалы	581	3 134

Идентификация ролей пользователей позволяет выявлять характер распространения деструктивных информационных волн и последующих протестных настроений, которые провоцируют пользователей социальных медиа на совершение противоправных действий. Анализ сетевых структур обеспечивает выявление закономерностей информационных атак, а также признаков их целенаправленного воздействия на население; прогнозирование поведения таких структур, и на этой основе – блокирование ключевых узлов для противодействия их влиянию [2].

В каждой информационной волне необходимо выявлять социальные роли пользователей, среди которых выделяются постеры, репостеры, комментаторы, пассивные участники. Основными характеристиками при их классификации выступают возраст, количество сетевых «друзей», количество опубликованных постов, репостов, комментариев. В качестве моделей по выявлению социальных ролей целесообразно применять модели нейросетевой классификации и кластеризации.

Список литературы:

1. *Губанов Д. А., Чхартишвили А. Г.* Влиятельность пользователей и мета-пользователей социальной сети // Проблемы управления. 2016.
2. *Минаев В. А., Бондарь К. М., Рабчевский А. Н., Федорович В. Ю.* Противодействие экстремистской идеологии в социальных медиа: монография / под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: РИО ДВЮИ МВД России, 2023. 232 с.
3. *Arularasan A. N.* Identification and classification of best spreader in the domain of interest over the social networks / A. N. Arularasan, A. Suresh, K. Seerangan // Cluster Computing. 2019. V. 22.
4. *Brandtzaeg P. B., Heim J.* A typology of social networking sites users // International Journal of Web Based Communities. 2011. V. 7
5. *Chen D.* Identifying influential nodes in complex networks // Physica A: Statistical Mechanics and its Applications. 2012. V. 391.
6. *Füller J.* User Roles and Contributions in Innovation-Contest Communities // Journal of Management Information Systems. 2014. V. 31.
7. *Jensen P.* Detecting global bridges in networks // IMA Journal of Complex Networks. 2015.
8. *Wijenayake P.* Automated Detection of Social Roles in Online Communities using Deep Learning // Proceedings of the 3rd International Conference on Software Engineering and Information Management. ACM, New York, 2020.

Владимир Александрович Минаев,
доктор технических наук, профессор,
профессор кафедры специальных
информационных технологий
Московский университет МВД России
имени В. Я. Кикотя
Email: m1va@yandex.ru

Алексей Сергеевич Толпыгин,
кандидат технических наук,
доцент кафедры защиты информации
Московский государственный технический
университет им. Н. Э. Баумана
E-mail: tas59417@yandex.ru

УДК 528.71:004.512.4

Кибербезопасность беспилотного транспорта

Аннотация

Рассматриваются вопросы обеспечения кибербезопасности беспилотного транспорта. Проводится анализ угроз безопасности его системам управления. Обсуждается подход к формированию актуальных угроз на этапах жизненного цикла – от формирования требований к ним до вывода из эксплуатации. Предлагается иерархическая структура системы контроля и управления беспилотным транспортом и подход к разработке системы моделей угроз кибербезопасности для беспилотного транспорта.

Ключевые слова и словосочетания: *кибербезопасность; беспилотный транспорт; искусственный интеллект; модель угроз; жизненный цикл.*

Беспилотный транспорт проникает во все сферы жизни общества и отрасли хозяйственного механизма страны. Активно развиваются автомобильный, авиационный, железнодорожный, морской виды беспилотников.

Беспилотные автомобили становятся неотъемлемой частью умных городов, строятся специализированные федеральные трассы с необходимой инфраструктурой для их движения. Разработкой беспилотных автомобилей занимаются не только крупнейшие авто-

концерны – Tesla, Ford, General Motors, BMW, Audi, Mercedes-Benz, Toyota, Nissan, Honda, Группа ГАЗ, Камаз, НАМИ, Меркатор Холдинг, но и многие технологические компании – Google (Waymo), Apple, Uber, Lyft, Baidu, Nvidia, Яндекс, Сберавтотех.

На территориях Москвы и Республики Татарстан с 2018 г. проводится эксперимент по опытной эксплуатации высокоавтоматизированных транспортных средств на автомобильных дорогах общего пользования[1]. С июня 2023 г. движение беспилотных автомобилей открыто по трассе М-11.

Беспилотные летательные аппараты (БПЛА) активно применяются для решения таких задач, как мониторинг объектов критически важной инфраструктуры городов (трубопроводы, линии электропередач (ЛЭП), дорожная инфраструктура, инфраструктура связи, вокзалы, аэропорты и пр.); грузоперевозки в труднодоступные регионы и отдаленные территории; разведка в труднодоступных местах (геологоразведки).

Ряд стран, в числе которых Германия, Россия, Япония, проводит испытания беспилотных поездов. Норвегия, Россия, США, Турция применяют беспилотные морские суда гражданского и специального назначения.

В России принимаются меры государственной поддержки, которые направлены на стимулирование развития беспилотного автомобильного транспорта[2] и беспилотных авиационных систем (БАС)[3].

---

[1] Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств [Электронный ресурс]: Постановление Правительства Рос. Федерации от 9 марта 2022 г. № 309. Доступ из справ.-правовой системы «КонсультантПлюс»; О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств [Электронный ресурс]: Постановление Правительства Рос. Федерации от 26 ноября 2018 г. № 1415. Доступ из справ.-правовой системы «КонсультантПлюс»

[2] Об утверждении плана мероприятий («дорожной карты») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Автонет» [Электронный ресурс]: Распоряжение Правительства Рос. Федерации от 29 марта 2018 г. № 535-р. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Об утверждении Стратегии развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года и плана мероприятий по ее реализации [Электронный ресурс]: Распоряжение Правительства Рос. Федерации от 21 июня 2023 г. № 1630-р. Доступ из справ.-правовой системы «КонсультантПлюс»

По имеющимся оценкам [5–6], к 2027 г. производство БПЛА в России достигнет 2 млн шт. в год, на дорогах будет функционировать не менее 100 тыс. беспилотных автомобилей.

В то же время существуют и негативные последствия активизации применения беспилотных транспортных средств (БТС) [1; 3–4]. Так, из-за слабого контроля БТС увеличивается вероятность террористических актов, шпионажа и другие противоправных действий. Этому способствуют: складывающаяся геополитическая обстановка, быстрое развитие перспективных технологий, цифровизация общества, недостаточность государственного регулирования.

Для предотвращения подобных инцидентов необходима система, которая обеспечит:

– полный контроль трафика в границах зон защищаемых объектов критической инфраструктуры;

– киберустойчивость БТС и защиту их от неправомерного применения;

– контроль выполнения маршрутных (полетных) заданий;

– выявление и предотвращение аномалий в поведении БТС;

– соответствие БТС законодательству РФ и требованиям регуляторов по безопасности их применения.

Угрозы кибербезопасности системе управления беспилотником

Под угрозами кибербезопасности беспилотного транспорта понимается совокупность условий и факторов, создающих потенциальную опасность в связи с нарушением конфиденциальности, доступности и (или) целостности информации, циркулирующей в системе управления БТС.

Реализация угроз кибербезопасности БТС в первую очередь связана с уязвимостями в системе управления БТС, которая представляет собой комплекс программно-аппаратных средств и каналов связи, обеспечивающих автономное управление БТС без участия человека. Анализ реализации киберугроз, связанных с интеллектуальными транспортными системами, приводится в [1; 3–4].

Существующие системы управления беспилотным транспортом используют различные технологии, включая системы глобального позиционирования (ГЛОНАСС, GPS), радары, лидары, камеры, датчики и сенсоры, которые собирают информацию об окружающей среде. Программное обеспечение систем управления БТС реализует алгоритмы и модели, которые обрабатывают эту информацию и принимают решения о движении БТС.

Важную роль в системах управления беспилотным транспортом играет искусственный интеллект (ИИ). ИИ может использоваться для обучения моделей и алгоритмов, которые помогают

БТС принимать решения о движении и обеспечивать безопасность. Он используется для анализа данных и прогнозирования поведения участников дорожного движения.

Вместе с тем необходимо учитывать киберугрозы инфраструктуре, необходимой для систем управления беспилотным транспортом. Она включает такие элементы, как система связи, системы хранения и обработки данных, системы организации и управления движением, которые помогают БТС ориентироваться в пространстве и двигаться по безопасному маршруту.

В качестве алгоритма формирования актуальных угроз безопасности информации в системе управления (СУ) БТС предлагается использовать классический подход (рис.1).

Для оптимизации усилий на начальном этапе эвристического формирования системы факторов (угроз), воздействующих на безопасность защищаемой информации, предлагается формировать первичный перечень угроз на основе просеивания (исключения) угроз из полного перечня банка данных угроз ФСТЭК России (ubi.fstec.ru).

Для базовой модели угроз основу перечня должны составить типовые угрозы, характерные для любого этапа жизненного цикла СУ БТС.

По методике просеивания угроз из Банка данных угроз (БдУ) безопасности информации ФСТЭК авторами выявлены более 30 угроз, которые могут быть осуществлены с высокой вероятностью и иметь высокий уровень влияния.

Выделены следующие группы угроз кибербезопасности беспилотного транспорта:

1. Угрозы безопасности данных:

– несанкционированный доступ к данным, хранящимся в системах управления беспилотным транспортом;

– кража или изменение конфиденциальной информации (например, личные данные пассажиров или информация о маршруте);

– внедрение вредоносных программ, которые могут влиять на системы управления и привести к сбоям или утечке данных;

– подмена данных, на основе которых принимаются решения по управлению движением БТС, например, маршрутное задание, данные об окружающей среде.

Рис.1. Алгоритм формирования множества угроз кибербезопасности системам управления беспилотного транспорта

2. Угрозы безопасности связи:

– фальсификация сигналов связи между БТС и системой управления;

– внедрение вредоносных программ, нарушающих работу систем связи с целью перехвата управления БТС.

3. Угрозы безопасности системе управления:

– ошибки в программном обеспечении, которые могут привести к сбоям или уязвимостям в системе;

– ошибки идентификации БТС и взаимодействующих элементов инфраструктуры;

– уязвимости в аппаратном обеспечении, которые могут быть использованы для несанкционированного доступа к системе.

4. Угрозы безопасности инфраструктуре связаны с недостатками в системах:

– организация движения, которые могут привести к сбоям или уязвимостям в системах управления флотом БТС;

– которые могут привести к потере связи между БТС и внешней системой управления.

5. Угрозы безопасности системам искусственного интеллекта, приводящие к:

– ошибкам в моделях обработки данных;

– извлечению данных, получению конфиденциальной информации путем обмана системы ИИ;

– преднамеренному внесению некорректных данных с целью манипуляции системой ИИ, искажения результата работы системы;

– переусложнению системы искусственного интеллекта.

Следует отметить, что в условиях, когда продолжает использоваться существенная доля зарубежного программного обеспечения (ПО) и ресурсов глобальной сети Интернет, а организации сталкиваются с отказами в технической поддержке ИТ-оборудования и обновления ПО, снижение доступа к источникам пополнения знаний о новых киберугрозах и уязвимостях приводит к существенному возрастанию вероятности реализации кибератак на системы управления транспортом, включая его беспилотные виды.

Необходимо также учитывать, что уязвимости в систему управления БТС могут быть внесены на всех этапах ее жизненного цикла: формирование требований; проектирование (реконструкция, модернизация); разработка; ввод в действие; эксплуатация; вывод из эксплуатации.

Система моделей угроз кибербезопасности

С целью учета всех возможных факторов и сфер проявления угроз безопасности системам управления необходимо разработать модель угроз безопасности (МУБ) для каждого конкретного вида и класса БТС.

Предлагается в систему МУБ включить:

– базовую модель угроз (БМУ) безопасности беспилотного транспорта, основанную на иерархии уровней автономности БТС;

– частные (по видам БТС) модели угроз (ЧМУ);

– типовые МУ безопасности составных частей системы управления БТС.

БМУ является разделом методического документа, описывающего модель угроз и нарушителей, и предназначена для выполняющих проектирование инфраструктуры системы управления беспилотным транспортом и осуществляющих работы по аттестации (оценке соответствия) информационных систем требованиям о защите информации.

Базовая модель уточняется при периодической переоценке и выявлении новых угроз безопасности информации, способов и средств их реализации; совершенствовании (модернизации) сети

центров контроля и управления беспилотным транспортом, изменении конфигурации ее инфокоммуникационной структуры.

Принимая во внимание, что развитие беспилотного транспорта включено в приоритетные направления проектов технологического суверенитета Российской Федерации[1] и формирование отрасли носит стремительный характер, подчеркнем необходимость обеспечения полного контроля трафика БТС в границах зон защищаемых объектов критической инфраструктуры, киберустойчивости БТС и защиты от их неправомерного применения, контроля выполнения маршрутных (полетных) заданий, выявления и предотвращения аномалий в поведении БТС, соответствия БТС законодательству РФ и требованиям регуляторов по безопасности их применения. Для всего вышесказанного целесообразно создать сеть центров контроля и управления движением БТС, обеспечивающих ситуационную осведомленность и поддержку управленческих решений, используя для этого, в том числе систему цифровых двойников [2].

Список литературы:

1. Киберугрозы в транспортной отрасли. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/ (дата обращения: 14.03.2024).

2. *Минаев В. А. [и др.].* Цифровые двойники объектов в решении задач управления // Радиопромышленность. 2019. № 3.

3. Развитие киберугроз в автоиндустрии. URL: https://habr.com/ru/articles/794344/ (дата обращения: 14.03.2024)

4. *Соколов И. А. [и др.].* Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности // International Journal of Open Information Technologies. 2017. Т. 5. № 7.

[1] «Об утверждении приоритетных направлений проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации и Положения об условиях отнесения проектов к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации, о представлении сведений о проектах технологического суверенитета и проектах структурной адаптации экономики Российской Федерации и ведении реестра указанных проектов, а также о требованиях к организациям, уполномоченным представлять заключения о соответствии проектов требованиям к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации» [Электронный ресурс]: Постановление Правительства Рос. Федерации от 15 апреля 2023 г. № 603. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Future Readiness Indicator. URL: https://www.imd.org/future-readiness-indicator/home/automotive-2023/ (дата обращения: 14.03.2024).

6. KPMG's Autonomous Vehicles Readiness Index (AVRI) for 2020. URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehicles-readiness-index.pdf (дата обращения: 14.03.2024).

Владимир Александрович Минаев,
доктор технических наук, профессор,
профессор кафедры специальных
информационных технологий
Московский университет МВД России
имени В. Я. Кикотя
Email: m1va@yandex.ru

Александр Олегович Фаддеев,
доктор технических наук, доцент,
профессор кафедры экономической безопасности
Рязанского филиала
Московский университет МВД России
имени В. Я. Кикотя
E-mail: fao1@mail.ru

УДК 004.056

Геофизические факторы как угрозы кибербезопасности

Аннотация

С целью совершенствования системы противодействия угрозам кибербезопасности рассмотрены первичные и вторичные факторы негативного влияния геофизических процессов на информационные компьютерные системы. Среди таких процессов обсуждаются геодинамические, ионосферные, антропологические. Представлены их системные взаимосвязи, показывающие направления воздействия на состояние и динамику кибербезопасности. Определены приоритетные задачи обеспечения геофизической кибербезопасности, а именно исследование воздействия: звуковых волн инфразвукового диапазона и электромагнитных волн, распространяющихся по волноводам земной коры; криповых подвижек на формирование и развитие в земной коре дилатансных структур, а также накопление сдвиговых деформаций, определяющих изменения напряженности атмосферного электрического поля; генерации механических волн естественного и искусственного происхождения, способствующих развитию дилатансных структур в земной коре.

Ключевые слова и словосочетания: *кибербезопасность; геофизические угрозы; информационные системы.*

Наряду с основными опасными факторами, напрямую связанными с сейсмической активностью и формирующими угрозы устойчивому функционированию информационных компьютерных систем (ИКС), существуют сопутствующие ей и генетически с ней связанные. Они носят название «вторичных» [9], влияя на здоровье населения, качество природной среды не столь масштабно и реализуясь не так ярко. Тем не менее они весьма важны для обеспечения безопасности человека, а также кибербезопасности его информационно-коммуникационного пространства. В статье последний аспект исследуется комплексно. Во внимание принимаются как первичные факторы, так и вторичные факторы геофизических угроз кибербезопасности.

Важнейшим вторичным геодинамическим фактором выступает электрическое поле, возникающее непосредственно перед сейсмическим событием. Напряженность указанного поля настолько велика, что как в его эпицентральной зоне, так и в достаточно большой его окрестности наблюдаются свечение атмосферы, ореолы по контурам людей, животных и различных природных и техногенных объектов [1]. Например, за сутки до мощного, с магнитудой 7,0, Балканского землетрясения в 1986 г. в аэропорту Бухареста отказали все компьютеры, работа аэропорта была парализована на несколько часов. Было заметно свечение атмосферы на расстоянии более двух сотен километров от эпицентра!

В феврале прошедшего года при реализации катастрофического сейсмического события в Турции наблюдались подобные световые явления, а возникшее перед землетрясением мощное электрическое поле оказало фатальное влияние на электронную технику в зоне своего воздействия.

Говоря о вторичных факторах, необходимо вспомнить о криповых подвижках [9]. По другому они называются «ползучими землетрясениями». Они опасны не только формированием опасных деформаций в геологической среде, но и своей главенствующей ролью в образовании исключительно вредных для человека и электронной техники, телекоммуникационных и информационных систем, акустических полей инфразвукового диапазона [10].

Указанные биоактивные поля «работают» постоянно, наращивая свою пагубную для человека аномальность и приводя к «неожиданным» повреждениям зданий и сетей различных коммуникаций.

Одно из самых опасных аномальных медико-биологических явлений в этой связи – это изменение психического состояния человека при воздействии на него спектра колебаний от сильного землетрясения [9]. Подобные явления распространяются на огромные территории, на которых проживает большое количество людей.

Среди них могут оказаться операторы сложных компьютеризованных систем, включая АЭС, объекты военной и ракетно-космической техники, оборонного комплекса, других критических производств. Когда случилось Ташкентское землетрясение 1966 года интенсивностью 8 баллов, из 1 623 случаев гибели и тяжелых травм около 55 % было связано с психическим состоянием пострадавших – паникой, страхом, спутанностью сознания, неосознанными опасными действиями.

Все вышесказанное достаточно убедительно показывает, насколько велика роль геофизических процессов в жизнедеятельности современного сообщества, в генерировании угроз и реализации рисков кибербезопасности.

Система геофизических опасностей

Специалисты в области кибербезопасности достаточно солидарны во мнении, что обеспечение кибербезопасности представляет целенаправленную деятельность, позволяющую защитить компьютерные устройства, информационные системы и сети от цифровых атак[1] [2; 8; 12].

Чтобы сохранить информацию, находящуюся в компьютерных системах различного масштабного и иерархического уровня, необходимо обеспечить ее защиту от компьютерных угроз в их традиционной совокупности, а также неизменность таких свойств информации как конфиденциальность, целостность и доступность [5].

При обеспечении кибербезопасности современного российского общества, его государственных, экономических, силовых структур необходимо учитывать целый комплекс внешних факторов. Важными выступают факторы, формируемые природной средой и целенаправленной антропогенной деятельностью, приводящие к дестабилизации, повреждению, а порой – и к уничтожению информационных компьютерных систем (ИКС) различного целевого назначения [3–7; 10].

Осознавая многогранность данной проблемы, ограничимся только таким их множеством, как геофизические киберопасности (рис.1).

При этом источниками формирования угроз выступают такие геодинамические процессы, как землетрясения, криповые подвижки, движения земной коры, ионосферные процессы, проявляющиеся в виде ионосферных возмущений и искусственных воздействий на геологическую среду, обусловленных целенаправленной враждебной техногенной деятельностью человека.

[1] ГОСТ ISO/IEC 27100:2020. Информационная технология. Кибербезопасность. Обзор и концепции. 2020. 24 с.

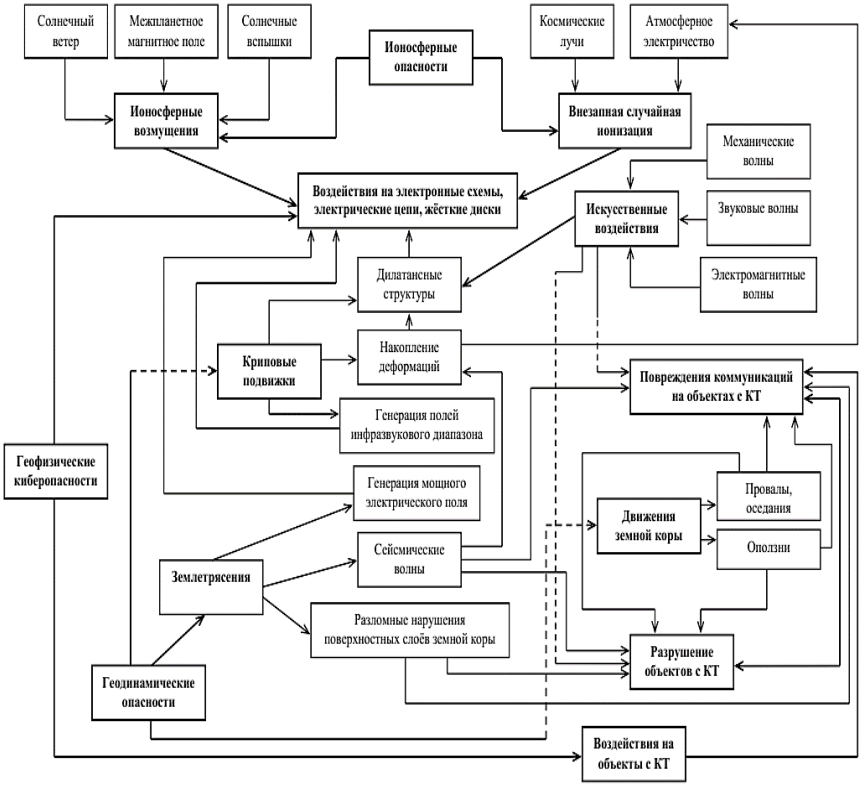

Рис. 1. Система воздействий геофизических факторов на компьютерные системы

Анализ изложенного приводит к выводам, что приоритетными направлениями исследований по проблеме геофизических угроз кибербезопасности выступают:

1. Воздействия звуковых волн инфразвукового диапазона и электромагнитных волн искусственного и естественного происхождения через волноводы земной коры, генетически связанные с дилатансными структурами, на электронные схемы, устройства компьютерной техники, в том числе – носители информации. Под дилатансией понимается эффект нелинейного разуплотнения упругой геологической среды вследствие лавинообразного формирования трещин сдвига [11].

2. Влияние криповых подвижек на формирование и развитие в верхних слоях земной коры дилатансных структур, способству-

ющих распространению электромагнитных волн, а также звуковых волн инфразвукового диапазона по связанным с ними волноводам.

3. Изучение влияния криповых подвижек посредством накопления сдвиговых деформаций на изменения напряженности атмосферного электрического поля.

4. Исследование влияния генерации в земной коре механических волн естественного и искусственного происхождения на накопление сдвиговых деформаций, способствующих формированию и развитию дилатансных структур в верхних слоях земной коры.

Решение задач в указанных направлениях позволит повысить уровень обеспечения кибербезопасности как современного российского сообщества в целом, так и его государственных, экономических, силовых структур, в частности учреждений и подразделений МВД России, а также отдельных граждан.

Современный этап развития системы кибербезопасности характеризуется все большим погружением науки и практики в исследования, связанные с отраслями знаний, не имеющими, на первый взгляд, отношения к формированию и развитию новых направлений в рассматриваемой области.

Появление и распространение терминологии, относящейся к «кибербезопасности», относится к тем событиям научной жизни, когда на устоявшемся фундаменте информационной безопасности возникло перспективное научное течение, вобравшее традиционные концепции и идеи, расширившее поле изучаемых факторов, и одновременно более четко определившие свои границы [8].

В статье сделана попытка очертить круг научно-практических задач, связанных с изучением важного, но пока недостаточно исследованного направления анализа, оценки и прогнозирования воздействия геофизических угроз на кибербезопасность.

Список литературы:

1. *Адушкин В. В., Соловьев С. П., Спивак А. А.* Электрические поля техногенных и природных процессов. Москва: ГЕОС, 2018. 464 с.

2. *Алпеев А. С.* Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 4 (38).

3. *Арутюнян Р. В. [и др.].* Системный анализ причин и последствий аварии на АЭС «Фукусима-1». Москва: ИБРАЭ РАН, 2018. 408 с.

4. *Ахметшин Т. Р. [и др.].* Геодинамические риски: моделирование, оценки, управление: монография / под ред. В. А. Минаева. Уфа: УГНТУ, 2023. 338 с.

5. *Винокуров С. А. [и др.].* Основы кибербезопасности: учебник. Воронеж, Москва: Воронежский институт МВД России, Московский университет МВД России имени В. Я. Кикотя, 2022. 392 с.

6. *Корячко В. П. [и др.].* Моделирование сейсмических рисков на территориях расположения объектов критической инфраструктуры // Вестник Рязанского государственного радиотехнического университета. 2023. № 84.

7. *Кочарян Г. Г., Спивак А. А.* Динамика деформирования блочных массивов горных пород / под ред. В. В. Адушкин. Москва: Академическая книга, 2003. 422 с.

8. *Марков А. С.* Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1 (47).

9. *Минаев В. А. [и др.].* Вторичные геодинамические факторы и экологическая безопасность территорий // Вестник Воронежского государственного университета. 2016. № 4.

10. *Николаевский В. Н.* Геомеханика. Том 2. Земная кора. Нелинейная сейсмика. Вихри и ураганы. Москва, Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2010. 560 с.

11. *Собисевич Л. Е., Собисевич А. Л.* Дилатансные структуры и электромагнитные возмущения УНЧ диапазона на этапах подготовки и развития крупного сейсмического события // Вестник ОНЗ РАН. 2010. № 2.

12. *Харрис Ш.* Кибервойн@: Пятый театр военных действий. Москва: Альпина нон-фикшн, 2016. 390 с.

Андрей Анатольевич Майдыков,
кандидат юридических наук,
доцент кафедры
организации оперативно-разыскной деятельности
Академия управления МВД России
E-mail: maydikov@mail.ru

Магомед Микаилович Мусаев,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: musmag123@mail.ru

УДК 343.01

Аспекты оперативно-розыскной деятельности в организации контроля оборота беспилотных летательных аппаратов в Российской Федерации как нового элемента рынка оружия

Аннотация

Беспилотные летательные аппараты становятся все более доступными и распространенными. Это приводит к росту их использования в различных сферах, включая гражданскую, научную и правоохранительную.

В военной области беспилотные летательные аппараты используются для разведки, наблюдения, обнаружения целей и выполнения боевых задач без участия пилота.

Кроме того, граждане законно могут вносить изменения сами в беспилотные летательные аппараты, например, увеличивать мощность мотора.

В гражданской сфере беспилотные летательные аппараты используются для различных задач, таких как контроль над границами, поиск пропавших людей, аэрофотосъемка и даже доставка товаров.

В научной сфере беспилотные летательные аппараты используются для сбора данных и исследований в области геологии, экологии, метеорологии и многих других областях. Особенно важно, что некоторые беспилотные летательные аппараты, использующиеся в быту простыми гражданами, разрешены в свободной продаже.

В правоохранительной сфере беспилотные летательные аппараты используются для обеспечения безопасности и выявления

правонарушений, пресечения нарушений правил дорожного движения (например, превышение скорости или езда по встречной полосе) и пресечения экологических нарушений (например, незаконная рубка леса или загрязнение водоемов). Беспилотные летательные аппараты могут использоваться для сбора доказательств коррупционных действий, таких как взяточничество или хищение государственных средств. Сфера применения беспилотных летательных аппаратов в правоохранительной деятельности постоянно расширяется, и по мере развития технологий можно ожидать появления новых способов их использования.

Обращение к вопросу использования беспилотных систем в оперативно-розыскной деятельности обусловлено рядом обстоятельств.

В современных условиях эффективное обеспечение безопасности личности, общества и государства от противоправных посягательств без использования новых технологий цифровой трансформации весьма затруднительно. Именно их использование в сфере оперативно-розыскной деятельности обеспечит эффективное решение задач по раскрытию и расследованию уголовных дел, предупреждению преступлений.

Несмотря на появление совершенно новых вызовов существенно изменивших геополитическую конъюнктуру в мире, вопросы борьбы преступлений используемых беспилотных летательных аппаратов выходят на первый план. Президент Российской Федерации специально отметил, что производство и использование беспилотных летательных аппаратов в России становится государственной задачей, и для ее решения выделяют значительные бюджетные средства. Введение беспилотных аппаратов в качестве нового элемента рынка оружия требует особых мер по контролю и мониторингу, включая не только правоохранительные, но и юридические, технологические, и рыночные аспекты.

Ключевые слова и словосочетания: *беспилотные летательные аппараты; оперативно-розыскная деятельность; контроль над оборотом оружия; противоправные цели; рынок оружия.*

В современных условиях эффективное обеспечение безопасности личности, общества и государства от противоправных посягательств без использования новых подходов оборота оружия невозможно. Технологии цифровой трансформации весьма активно используются преступными элементами. Это, в свою очередь, требует от оперативных сотрудников применения более совершенных информационных

технологий. Повышается компетенция граждан по управлению беспилотными летательными аппаратами (далее – БПЛА).

Исходя из выше сказанного, неконтролируемое использование БПЛА возможно в виде оружия для совершения противоправных действий. БПЛА оснащается огнестрельным оружием, однако в настоящее время законодатель БПЛА не относит ни к одному из видов оружия. Сложность выявления противоправной составляющей в использовании БПЛА по всем выше обозначенным направлениям требует применения специальных методов правоохранительной деятельности. К ключевому методу относится оперативно-розыскная деятельность (далее – ОРД). Следует также учитывать, что путем ОРД должно не только контролироваться использование БПЛА, но и в самой ОРД должны использовать БПЛА при проведении гласных и негласных ОРМ. Именно их использование в сфере ОРД обеспечит эффективное решение задач по раскрытию и расследованию уголовных дел, предупреждению преступлений [4, с. 36–41].

Эффективное внедрение и использование беспилотных аппаратов как элемента рынка оружия требует комплексного подхода со стороны правоохранительных органов и государственных органов, чтобы обеспечить безопасное и законное использование данной техники и предотвратить ее злоупотребление в противоправных целях. Контроль оборота БПЛА становится все более актуальной задачей в связи с их распространением и широким спектром применения. Рассмотрим некоторые аспекты, которые следует учитывать при организации контроля оборота БПЛА:

– усиление и разработка законодательства, регулирующего оборот и применение БПЛА, включая лицензирование, регистрацию и ограничения их использования;

– мониторинг сети Интернет, рынка БПЛА для выявления подозрительных объявлений и сообщений о продаже или использовании БПЛА в недопустимых целях, а также производителей и дистрибьюторов. Это могло бы помочь в регулировании и контроле цепочки поставок, обеспечивая соблюдение правил;

– обязательная регистрация всех БПЛА и их владельцев, чтобы иметь возможность отследить их использование в случае возникновения проблем;

– сотрудничество с производителями БПЛА для внедрения средств защиты и мониторинга в аппараты на уровне производства;

– обучение сотрудников правоохранительных органов и общественности о правилах использования и контроля БПЛА;

– обеспечение кибербезопасности при использовании БПЛА для предотвращения и предупреждения кибератак или хакерских атак через БПЛА;

– внедрение систем аналитики и мониторинга для выявления аномального поведения БПЛА и их использования в недопустимых целях.

ОРД в организациях, контролирующих оборот БПЛА, должна быть направлена на предотвращение угроз безопасности, обеспечение эффективного мониторинга и контроля над использованием беспилотных аппаратов, а также на пресечение их незаконного использования в качестве оружия или для других незаконных целей [3, с. 103–107].

Непосредственно ОРД при планировании ОРМ следует выделять мероприятия, направленные на использование БПЛА и иных противоправных задач:

– для доставки взрывчатых веществ или оружия;

– перевозки наркотиков, оружия или других запрещенных предметов;

– сбора разведывательной информации;

– совершения хулиганских действий или для нарушения работы критически важной инфраструктуры;

– анализа информации из различных источников;

– сбора и фиксация доказательной базы для применения административных мер, таких как штрафы;

– возбуждения уголовных дел;

– сбора доказательств, таких как видеозаписи, фотографии и записи телефонных разговоров, чтобы доказать вину лиц;

– анализа данных, полученных с БПЛА, чтобы установить их маршруты, места взлета и посадки и другую информацию, которая может быть полезна для расследования.

Следует также не игнорировать сегмент экономической безопасности использования БПЛА. Это, в свою очередь, ведет к возможности совершения коррупционных и экономических преступлений. БПЛА становятся все более важным элементом рынка вооружений. Военные и правоохранительные органы многих стран мира используют БПЛА для разведки, наблюдения и целеуказания. Технологии производства БПЛА становятся все более доступными, что облегчает их производство и использование в противоправных целях. Обладая трансграничным характером, БПЛА может легко пересекать границы, что затрудняет контроль над их оборотом [1, с. 231–242].

В связи с новыми вызовами необходимо совершенствовать ОРД в области контроля над оборотом БПЛА. Это требует разра-

ботки новых методов и средств ОРД для документирования противоправного использования БПЛА. Необходимо следующим образом сформировать доказательную базу: законодательство в области ОРД должно быть адаптировано к новым условиям и учитывать особенности использования БПЛА. Сотрудники ОРД должны пройти специальную подготовку, чтобы эффективно работать с БПЛА [2, с. 18–23].

Можно сделать вывод, что контроль над оборотом БПЛА является важной задачей, которая требует комплексного подхода. ОРД играет важную роль в обеспечении контроля над оборотом БПЛА и предотвращении их использования в противоправных целей.

Список литературы:

1. *Аверченко С. В., Белоусов В. В.* Беспилотные летательные аппараты в военных конфликтах второй половины XX – начала XXI веков: основные вехи истории // Современная научная мысль. 2023. № 1.

2. *Косовский В. Б., Мартынюк С. Н.* Актуальные вопросы практического применения беспилотной техники в органах внутренних дел Российской Федерации // Общество: политика, экономика, право. 2020. № 3.

3. *Попов В. А.* Использование оперативно-розыскной информации в обеспечении экологической безопасности // Вестник МГУЛ – Лесной вестник. 2003. № 4.

4. *Шишкин Р. В.* Преступления, совершаемые с использованием цифровых технологий: проблемы противодействия // Вестник Уральского юридического института МВД России. 2022. № 4.

Владимир Анатольевич Николаев,
начальник отдела
ФКУ «НИЦ «Охрана» Росгвардии
E-mail: nicohrana@rosgvard.ru

Дмитрий Андреевич Прошутинский,
старший научный сотрудник
ФКУ «НИЦ «Охрана» Росгвардии
E-mail: nicohrana@rosgvard.ru

Николай Васильевич Талышев,
кандидат технических наук, доцент,
главный научный сотрудник
ФКУ «НИЦ «Охрана» Росгвардии
E-mail: nicohrana@rosgvard.ru

УДК 519.876.5

Перспективы создания программно-аппаратного комплекса средств цифрового моделирования для повышения эффективности служебной деятельности правоохранительных органов

Аннотация

В работе обозначена актуальность проведения исследований в направлении создания программно-аппаратных комплексов ситуационного моделирования на основе цифровых двойников и их применимость в служебной деятельности правоохранительных органов, а также освещены особенности, которые необходимо учитывать при создании и использовании имитационных моделей.

Ключевые слова и словосочетания: *цифровой двойник; 3D-визуализация; ситуационное моделирование.*

Правоохранительным органам в процессе повседневной деятельности приходится постоянно сталкиваться с необходимостью решения ряда оперативных и служебных задач, которые в большинстве случае многовариантны и относятся к классу открытых задач. Сотрудникам приходится на основе своего накопленного опыта и приобретенных компетенций в ограниченное время осуществлять выбор одного из вариантов, не имея при этом четких представлений

о вероятности достижения необходимого результата и последствиях принятого решения. Практическим работникам в подразделениях в настоящее время не предоставлено каких-либо математических инструментов, позволяющих на основе сравнительного анализа оценить эффективность предлагаемых вариантов решений и выбрать наиболее оптимальный из них.

Одним из таких надежных инструментов может стать предлагаемый к разработке программно-аппаратный комплекс средств цифрового моделирования с применением технологий искусственного интеллекта, который позволит осуществлять многовариантное ситуационное моделирование на основе цифровых двойников окружающей обстановки, сооружений, граждан, сил и средств обеспечения безопасности и преступной деятельности, их вариантов действий и реакций на воздействия.

Цифровые двойники окружающей обстановки и сооружений дают общую детализированную картину места, территории, объекта, конструкции, имеющихся связей и реакций элементов системы. Технология «Цифровые двойники» предусматривает создание виртуальных моделей физических объектов.

Применение 3D-моделирования позволяет визуализировать топологию объекта путем создания пространственной модели местности – наглядного и измеримого трехмерного изображения земной поверхности на электронных средствах отображения информации, воспроизведенного в соответствии с заданными условиями наблюдения (обзора) на основе цифровой информации о местности (электронных карт, цифровых моделей местности), полученной с географических карт, кадастровых планов и фотоматериалов, рельефных карт и видеоизображений [4, с. 17].

Программное обеспечение 3D-визуализации представляет собой приложение трехмерной графики. 3D-моделирование решает задачи информативности и наглядности представления об объекте. 3D-модель – это совокупность элементов модели, организованных в иерархическую структуру, которая позволяет получить подробную картину объекта:

– 360 градусная съемка фиксирует все детали без мертвых зон, даже не попавшие в объектив традиционные средства фото- и видеофиксации;

– пространство (близлежащие объекты, окна и двери, элементы конструкций) фиксируется целиком.

Для съемки пространств с целью создания высокоточных трехмерных моделей объектов («Цифровых двойников») применяются

активные оптические системы – лидары и видеокамеры, в том числе размещаемые на беспилотных авиационных системах (далее – БАС).

Лидар дает гораздо более детализированную и более оттеночную картинку и позволяет точно узнать физические размеры объектов, что повышает уровень качества 3D-моделирования [2, с. 175].

Данные лидарной съемки представляют собой наборов данных, содержащих облака точек, которые могут управляться, отображаться, анализироваться и совместно использоваться при помощи специального программного обеспечения [1, с. 56].

Плотность генерируемых точек такова, что лидар строит полноценную картину местности, в которой видны строения, заграждения, пешеходы, столбы и деревья и т. д. Также на 3D-модели объекта можно отображать дополнительные устройства, такие как элементы систем охранно-пожарной сигнализации, освещения, электропитания и др.

Помимо позиционных значений X, Y и Z, системой также сохраняется дополнительная информация. Для каждого лазерного импульса записываются и сохраняются следующие атрибуты: интенсивность, номер отражения, количество отраженных сигналов, значения классификации точки, крайние точки линии движения, время GPS, угол и направление сканирования.

Обработанные в дальнейшем пространственно-организованные данные лазерной и видеосъемки (облако точек) посредством 3D-моделирования преобразуются в цифровой двойник объекта.

Для автоматизации этого процесса необходимо проводить интегрирование в программно-аппаратный комплекс средства распознавания и интерпретации схематических изображений (плана объекта, его инфраструктур и систем), совмещение лидарных изображений с фотографическим панорамным изображением помещений (территорий).

Для съемки протяженного объекта дополнительно возможно применение БАС с размещенными на них лидаром [5, с. 54–57].

Лидар воздушного базирования позволяет ускорять создание цифровых моделей территорий, которые лягут в основу цифровых копий ландшафта и позволят получить высококачественные цифровые модели зданий, территорий и всего объекта в целом с минимизацией искажений, вызываемых близким расположением лидара к анализируемой поверхности.

3D-моделирование решает задачи информативности и наглядности представления об объекте. Вместе с тем для моделирования действий нарушителя и сил правопорядка необходимо проведение моделирования системы отношений между элементами системы безопасности, гражданами, сотрудниками и правонарушителями.

С этой целью строится модель нарушителя, которая представляет собой совокупность данных логически объединенных в группы в соответствии с тактическим предназначением.

Структура модели нарушителя обладает следующими параметрами:

– уровень осведомленности, который определяется наличием у нарушителя информации об элементах системы обеспечения общественной безопасности или охраны объекта;

– уровень мотивации – это степень риска, на который нарушитель готов пойти для достижения цели противоправного действия;

– уровень полномочий (доступа) ограничивается перечнем зон, в которые нарушитель имеет санкционированный доступ;

– уровень технической подготовленности к совершению незаконного действия, который определяется возможностью или невозможностью его совершения.

Возможному деструктивному воздействию нарушителей необходимо противопоставить спектр мер анализа и моделирования противодействия.

Для этого применяется ситуационное моделирование, т. е. моделирование комплекса связей между элементами объектами системы и их значениями. При этом для анализа возможных решений поставленных оперативных задач целесообразно применять динамическое ситуационное моделирование, описывающее изменение состояний всех элементов моделирования во времени и пространстве.

К методам ситуационного моделирования относятся:

– дискретные ситуационные сети;

– RX-KOjxbi, язык бинарных отношений;

– логика предикатов;

– универсальный семантический подход.

Наибольшее распространение для решения задач динамического моделирования получили в настоящее время дискретные ситуационные сети.

Для построения ситуационной модели необходимо определить состояния, в которых может находиться элемент системы моделирования, и рассчитать вероятности перехода между состояниями.

Необходимым компонентом для ситуационного моделирования ситуации боевого взаимодействия с преступником является программное обеспечение для оценки результатов боестолкновения и вероятности успешной нейтрализации нарушителя.

Анализ технологии создания и использования цифровых двойников показывает, что основой для их существования является имитационное моделирование [3, с. 65–66].

Имитационная модель позволяет произвести предварительный расчет возможных начальных условий боестолкновения, информированности сотрудников правоохранительных органов и нарушителей, позволяет повысить адекватность оценки принимаемых решений в каждой конкретной ситуации воздействия с учетом сложившихся условий.

Для ситуационного моделирования результатов боевого столкновения сил правопорядка и преступников необходимо учитывать комплекс факторов, влияющих на конечный результат:

– видимость и очередность обнаружения противника;
– имеющееся вооружение;
– имеющиеся индивидуальные средства защиты, укрытия, снижающие вероятность поражения;
– условия освещения;
– степень владения оружием;
– боевая скорострельность и скорость прибытие подкреплений;
– средства связи;
– тактические приемы сил охраны и нарушителей.

Вышеуказанные элементы позволяют с большей вероятностью оценить предполагаемые тактические действия правонарушителей и сотрудников, влияние на них внешних стационарных и динамических факторов и спрогнозировать необходимые условия для поражения противника.

При этом большинство известных методик математической оценки боестолкновений, например, «table top», проводят имитационное моделирование в пошаговом режиме, который является достаточно точным для достижения адекватного результата.

Ситуационное моделирование с помощью программно-аппаратного комплекса средств на основе приведенных выше цифровых моделей, а также баз данных, описывающих действия и реакции каждого из элементов имитационной модели в пространственно-временных координатах, позволяет производить анализ существующих вариантов угроз, возможных способов противоправных действий. Результаты этого анализа можно применять в служебной деятельности правоохранительных органов с целью выработки алгоритмов своевременного реагирования и противодействия, вариантов действия правонарушителей.

Создание цифровых двойников объектов может найти эффективное применение при создании базы объектов, охраняемых правоохранительными органами Российской Федерации, а также при составлении паспортов антитеррористической защищенности. Кроме того, при помощи цифровых двойников можно создать 3D-модели мест преступлений и осуществлять моделирование различных вариантов действий

правонарушителей, выделяя те, которые с наибольшей вероятностью соответствуют картине совершенного преступления.

Цифровые двойники собственных объектов правоохранительных органов позволяют также определить их уязвимость к сторонним воздействиям. При помощи моделирования и анализа цифрового двойника таких объектов можно определить наиболее вероятные пути проникновения нарушителей. При этом стоит учитывать, что разработка и поддержание цифрового двойника потребует дополнительных требований к соблюдению условий по защите информации.

Применение цифровых двойников и имитационного моделирования наиболее эффективно в составе единого программно-аппаратного комплекса, состоящего из средств сбора информации (лидар, средство фотофиксации, БАС), обработки и преобразования информации в унифицированный формат данных (цифровых моделей и имитационного моделирования), программных средств ситуационного моделирования, мощных вычислительных средств. При этом комплекс должен максимально обеспечивать автоматизацию каждого из этапов занесения, интерпретации и обработки информации, иметь подробную базу данных типовых элементарных объектов (их свойств и реакций на воздействие) и средства ее редактирования.

Таким образом, создание программно-аппаратного комплекса средств цифрового моделирования в современных условиях несомненно является одним из перспективных направлений информационно-технического развития правоохранительных органов, который в перспективе позволит значительно повысить эффективность оперативно-служебной деятельности подразделений.

Список литературы:

1. *Лыгин А. Н.* Методические указания по оцифровке растра в ArcGIS 9.3. Москва: МИИГАиК, 2015.

2. *Новаковский Б. А., Пермяков Р. В.* Комплексное геоинформационно-фотограмметрическое моделирование рельефа: учебное пособие. Москва: МИИГАиК, 2019.

3. *Петров А. В.* Имитация как основа технологии цифровых двойников // Вестник ИрГТУ. 2018. № 10.

4. Проект архитектуры программного обеспечения. Инфологическая модель базы данных. Москва, 2021.

5. *Самбаеф Б. Ш.* Построение 3D-строений по данным с БПЛА // Молодой ученый. 2019. № 14 (252).

Сергей Сергеевич Ошкуков,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: oshkuk@yandex.ru

УДК 004.934.2

Выявление признаков применения технических средств для модификации речи на фонограммах

Аннотация

Актуальность данной статьи обусловлена интенсивным развитием технических средств для модификации голоса, позволяющих изменять естественный голос человека. Данные технические средства являются общедоступными, не требуют специальной подготовки для их применения и могут быть использованы в целях маскировки голоса при совершении преступлений против личности, общественной безопасности и государственной власти. Поиск криминалистических методов, направленных на выявление признаков использования таких программ для изменения речи, является новой задачей, которая ранее не решалась. В статье приводится обзор основных алгоритмов модификации фонограмм с целью изменения тембрально-темпоральных характеристик голоса, а также предлагаются инструментальные методы для выявления признаков применения данных средств.

Ключевые слова и словосочетания: *алгоритмы модификации речи; инструментальный анализ фонограмм; исследование речи; криминалистическое исследование фонограмм; модификация голоса; тембрально-темпоральные характеристики речи; программы для модификации голоса; фоноскопическая экспертиза.*

В настоящее время существует значительное количество технических средств, позволяющих изменять голос. Под изменением голоса в данной статье понимается изменение как темпоральных, так и тембральных характеристик естественной речи. Данные средства являются общедоступными и не требуют специальной подготовки для их применения. Возможности этих программ могут быть использованы в том числе и при совершении преступлений в целях маскировки голоса, например, при заведомо ложных сообщениях об актах терроризма.

При поступлении на исследование фонограмм, содержащих измененный голос, у экспертов возникают трудности в выявлении признаков применения специальных программных средств для изменения голоса.

Современные технологии по обработке речи нацелены на максимальное сближение измененной и естественной речи. Достижения в данной области таковы, что отличить измененную речь от естественной все сложнее. С учетом темпов развития технологий по обработке речи и их доступности пользователям прогнозируется рост потребности в исследовании таких объектов.

Анализ источников показал, что научные исследования, посвященные выявлению признаков применения таких программ в криминалистическом аспекте, практически отсутствуют.

Для криминалистического исследования речи поиск признаков применения специальных программных средств для изменения голоса является новой задачей. В этой связи актуальным становится выявление и систематизация признаков изменений голоса с использованием технических средств, а также выработка подходов к выявлению таких изменений при проведении фоноскопических экспертиз.

Алгоритмы модификации речи

В целях решения обозначенной проблемы были изучены следующие алгоритмы изменения темпа речи:

– *Time-Domain Harmonic Scaling (TDHS);*
– *Synchronized Overlap-Add (SOLA);*
– *Synchronized Overlap-Add, Fixed Synthesis (SOLAFS).*

Time-Domain Harmonic Scaling (TDHS) [5]. Речевой сигнал масштабируется (сегментируется) во временной области на основе информации об извлеченной высоте основного тона (длительность сегментов речевого сигнала зависит от высоты основного тона). Частотное масштабирование речевых сигналов производится методами, основанными на кратковременном Фурье-анализе. Алгоритм производит взвешивание нескольких смежных сегментов речевого сигнала с помощью вычисленной оконной функции для получения выходного сегмента. На основе полученных данных производится сокращение смежных сегментов речевого сигнала или их удвоение.

На рис. 1, 2 и 3 приведены осциллограммы и спектрограммы речевого сигнала (на примере фразы «В мае на рыбалку на реку Волга»). На рис. 1 представлен оригинальный речевой сигнал, обозначенный вертикальными маркерами, на рис. 2 и 3 – результат работы алгоритма *TDHS* со сжатием и растяжением во временной области речевого сигнала соответственно.

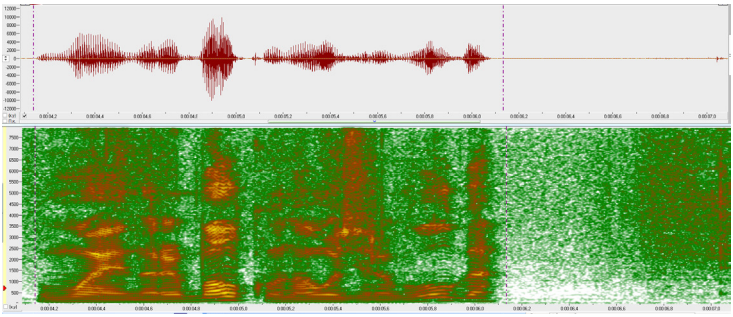

Рис. 1. Осциллограмма и спектрограмма оригинального речевого сигнала

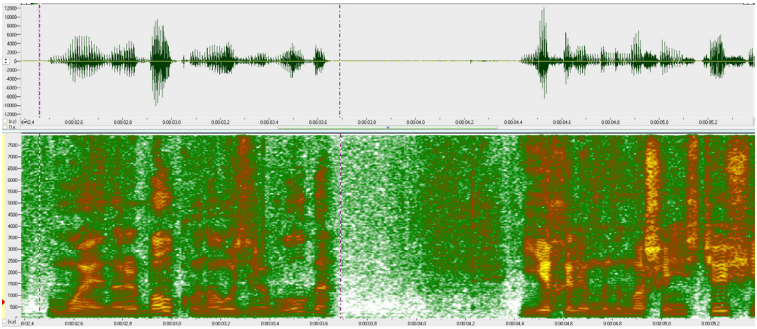

Рис. 2. Осциллограмма и спектрограмма речевого сигнала со сжатием во временной области

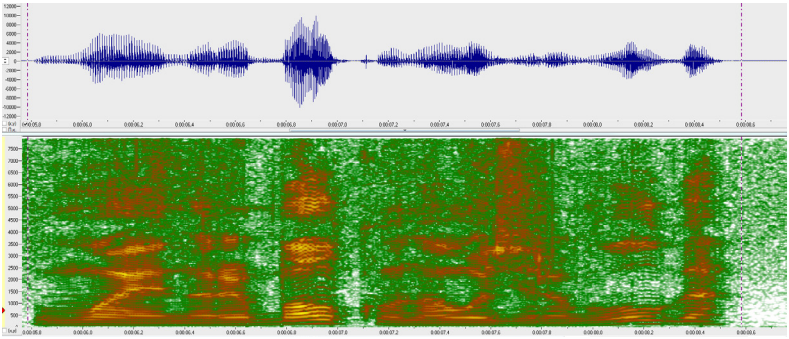

Рис. 3. Осциллограмма и спектрограмма речевого сигнала с растяжением во временной области

Анализ работы алгоритма показал, что изменение во временной области должно быть незначительным для сохранения адекватных тембральных характеристик речевого сигнала.

На рис. 4 представлены осциллограммы и кепстрограммы оригинального и растянутого во временной области речевых сигналов. При растяжении оригинального речевого сигнала во временной области (замедление темпа) наблюдается выравнивание (резкое уменьшение ширины диапазона частот) основного тона, появляются амплитудные и частотные искажения (импульсы), вызванные некорректным соединением сегментов удвоения. На осциллограмме измененного речевого сигнала амплитудные искажения показаны стрелками.

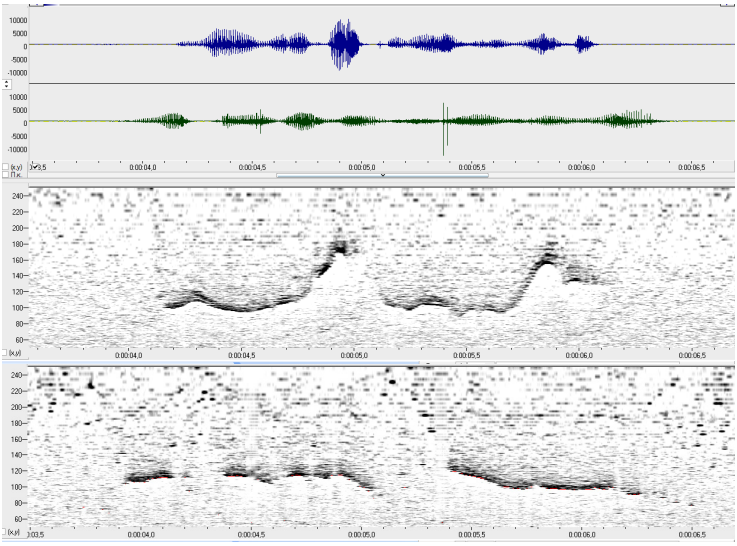

Рис. 4. Осциллограммы и кепстрограммы оригинального речевого сигнала и с растяжением во временной области

Synchronized Overlap-Add (SOLA) [3]. Суть работы данного алгоритма сводится к разбиению входного акустического сигнала на перекрывающиеся окна фиксированной длины, разделенные фиксированным расстоянием анализа. Затем с использованием быстрого Фурье-преобразования окна накладываются друг на друга и восстанавливаются, при этом расстояние между окнами уменьшается или увеличивается. Полученный выходной акустический сигнал будет сжат по времени, если новое расстояние анализа будет меньше исходного, и, наоборот, увеличен по времени, если новое расстояние анализа будет больше исходного.

Сложность алгоритма *SOLA* заключается в том, что величина перекрытий окон может меняться. Это усложняет вычисления усреднения, сходства окон и затухания в области перекрытия. Как след-

ствие, возникают артефакты[1] как в области перекрытий, так и во временной характеристике сжатия или растяжения.

В качестве примера возникновения артефактов на рис. 5 представлены две пары осциллограмм и спектрограмм оригинального речевого сигнала (слово «там», выделенное вертикальными маркерами) и аналогичного речевого сигнала, растянутого во временной области алгоритмом *SOLA*. При растяжении речевого сигнала на спектрограмме наблюдается многократное дублирование импульса согласного звука «т», что не соответствует визуальному представлению оригинального речевого сигнала. Кроме того, на осциллограмме растянутого речевого сигнала амплитудная характеристика ударного гласного звука «а» также не соответствует амплитудной характеристике оригинального речевого сигнала.

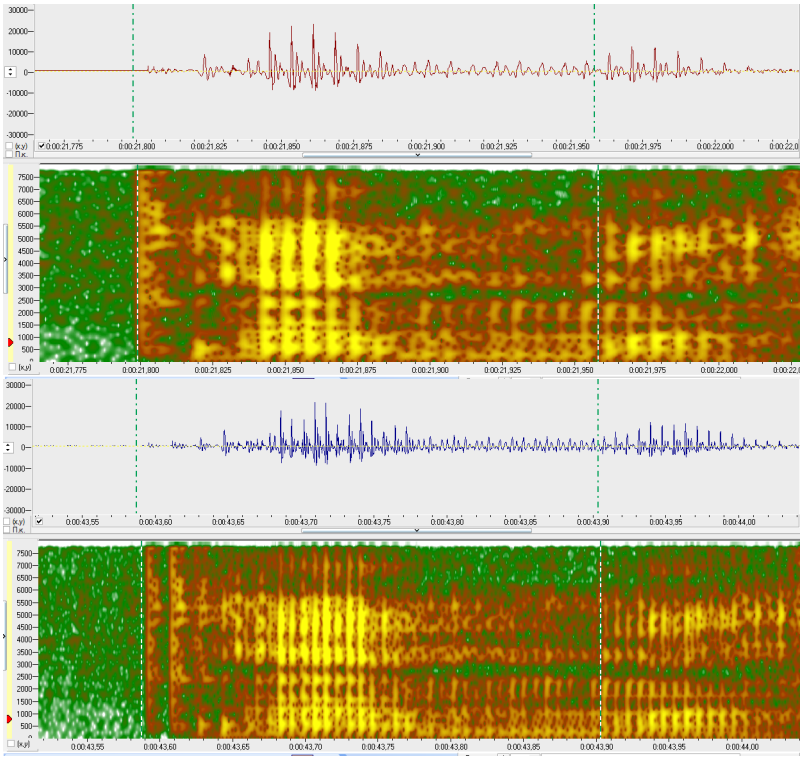

Рис. 5. Осциллограммы и спектрограммы оригинального речевого сигнала (вверху) и с растяжением во временной области (внизу)

[1] Под артефактом понимается искажение естественного речевого сигнала, возникновение которого по естественным причинам невозможно или маловероятно.

Synchronized Overlap-Add, Fixed Synthesis (SOLAFS) [4]. Данный метод является модификацией алгоритма *SOLA*. Окна, на которые разбит входной сигнал, добавляются в выходные данные с перекрытием с фиксированным расстоянием, в то время как начальные положения окон корректируются во время анализа, чтобы максимизировать сходство между выходными данными и новым окном в области перекрытия. За счет этого при умеренном сжатии или расширении обеспечивается плавность перехода между сегментами.

На рис. 6 приведена схема работы алгоритма *SOLAFS* со сжатием по времени, где *SA* и *SS* – окно анализа входных и выходных данных, *Kmax* – максимально допустимый сдвиг от исходного положения окна.

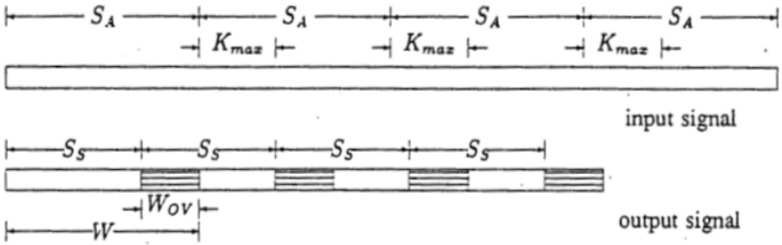

Рис. 6. Пример модификации сигнала алгоритмом SOLAFS

На рис. 7 представлены две спектрограммы оригинального речевого сигнала (фраза «сразу же на месте») и сжатого во временной области алгоритмом SOLAFS.

При сжатии речевого сигнала во временной области наблюдается удаление согласных звуков «р» и «т,» (показаны стрелками) и сокращение длительности согласных звуков «н» и «м,» (обозначены прямоугольниками).

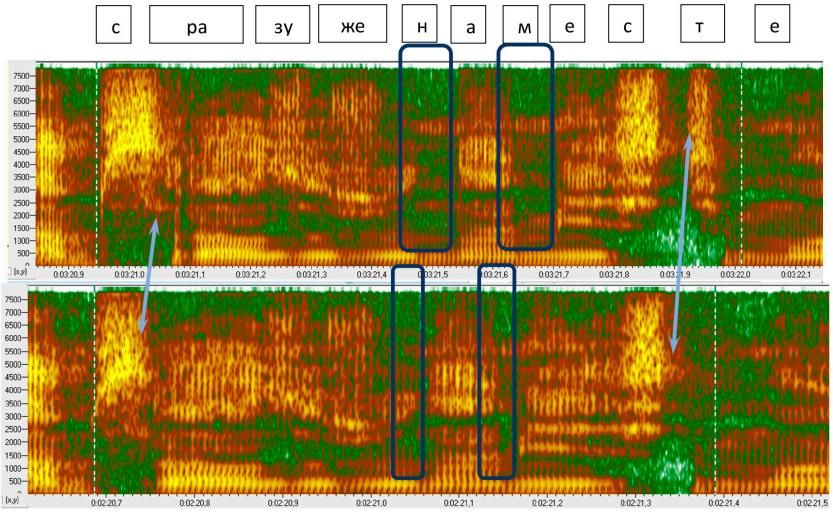

Рис. 7. Спектрограммы фрагмента высказывания «сразу же на месте», оригинальный речевой сигнал (вверху) и сжатый во временной области алгоритмом SOLAFS (внизу)

Данный алгоритм показывает наибольшее изменение невокализованных сегментов речевых сигналов. При этом отмечается плавное соединение сегментов речевого сигнала.

Данные алгоритмы хоть и были разработаны более 30 лет назад, до сих пор используются в качестве основы для создания новых модифицированных различным образом алгоритмов.

Для корректной модификации голосовых характеристик изменение только темпа речевого сигнала недостаточно. Необходимо также адекватно модифицировать основной тон речевого сигнала.

Алгоритмы изменения частоты основного тона:

– *Time-Domain Pitch Synchronized Overlap-Add (TD-PSOLA);*
– *Spectrum Interpolation (SPECINT);*
– *Linear-Predictive Pitch Synchronized Overlap-Add (LP-PSOLA);*
– *Frequency-domain Pitch Synchronized Overlap-Add (FD-PSOLA).*

Рассмотрим один из самых основных *Time-Domain Pitch Synchronized Overlap-Add (TD-PSOLA)* [1; 2].

Алгоритм *TD-PSOLA* (рис. 8) работает во временной области периодосинхронно, т. е. каждый обрабатываемый фрагмент представляет собой один период. Предварительно производится вычисление частоты основного тона речевого сигнала. Весь сигнал разбивается на фрагменты, содержащие два периода основного тона, взвешенных окном Хеннинга с определением его центра. Взвешенные

фрагменты смешиваются путем перемещения их центров и накладываются друг на друга. В итоге в зависимости от направления перемещения центра взвешенного фрагмента, происходит уменьшение или увеличение частоты основного тона речевого сигнала.

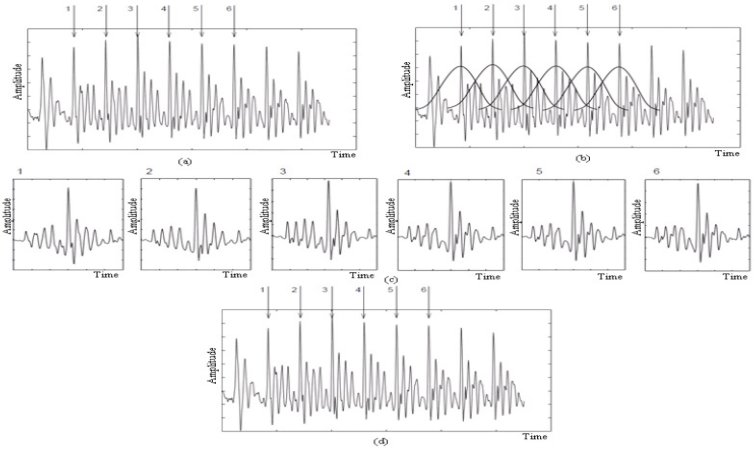

Рис. 8. Основные операции алгоритма *TD-PSOLA*: (a) участок вокализованного сигнала, размеченный на периоды основного тона, (b) взвешивающие окна Хеннинга, центрированные на каждом периоде, (c) полученная последовательность пар периодов после процедуры взвешивания окном, (d) измененный путем перекрытия с добавлением речевой сигнал

В связи с тем что данный алгоритм не производит добавление сигнала или его удаление, то при незначительных изменениях частоты основного тона (+/-10 %) выходной сигнал будет иметь хороший результат, а при больших изменениях частоты – будет звучать неестественно. Также могут появляться артефакты, связанные комбинированием фрагментов взвешенным окном Хеннинга.

На рис. 9 показаны осциллограммы оригинального речевого сигнала и растянутого во временной области алгоритмом *TD-PSOLA* (между окнами двукратная разница). На осциллограмме растянутого речевого сигнала наблюдаются искажения амплитудной характеристики (отсутствие однородности амплитуды на вокализованных участках), а также следы применения оконной функции и некорректное соединение фрагментов. На кепстрограмме растянутого речевого сигнала, представленного на рис. 10, наблюдаются искажения основного тона речи, не свойственные естественным речевым сигналам, появление основного тона на невокализованных сегментах речевых сигналов.

На спектрограммах оригинального речевого сигнала (слово «давали») и растянутого во временной области (рис. 11) наблюдаются искажения частотных характеристик речевого сигнала в низкочастотной области спектра:

– появление биения гармоник (две стрелки слева);

– некорректное соединение модифицированных сегментов речевых сигналов (вертикальная стрелка);

– появление дополнительных гармонических составляющих (обозначены сдвоенной стрелкой);

– появление раздвоенных гармоник (стрелка справа).

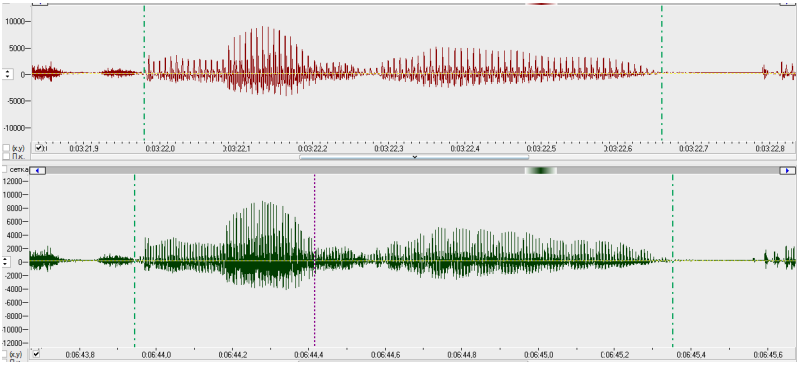

Рис. 9. Осциллограммы слова «можно», оригинальный речевой сигнал (вверху) и растянутый во временной области алгоритмом TD-PSOLA (внизу)

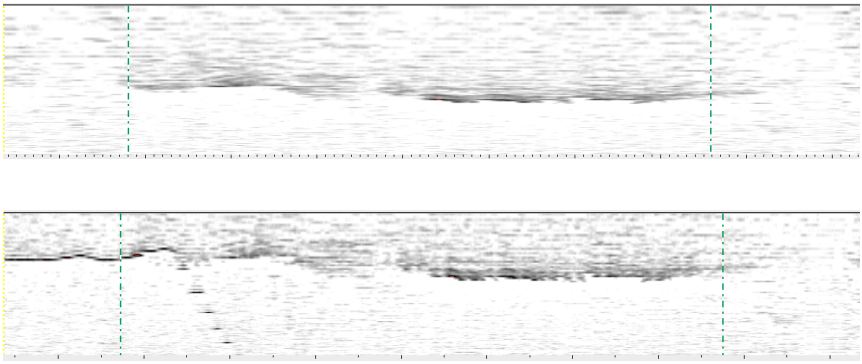

Рис. 10. Кепстрограммы слова «можно», оригинальный речевой сигнал (вверху) и растянутый во временной области алгоритмом TD-PSOLA (внизу)

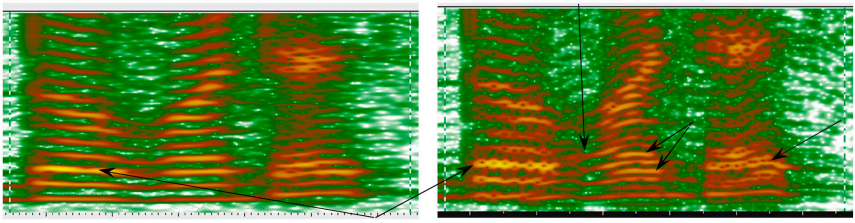

Рис. 11. Спектрограммы слова «давали», оригинальный речевой сигнал (слева) и растянутый во временной области алгоритмом *TD-PSOLA* (справа)

Анализ представленных методов (алгоритмов, подходов) к модификации естественных речевых сигналов показал, что в модифицированных речевых сигналах необходимо подвергнуть оценке их амплитудные, частотные и фазовые характеристики. В основном необходимо выявлять искажения речевых сигналов или появление в речевых сигналах артефактов, связанных с применением того или иного алгоритма. Также при анализе модифицированных речевых сигналов необходимо определять совокупность выявленных артефактов, а также их взаимозависимость с учетом канала звукозаписи и уровня шумов в сигнале.

Таким образом, обзор литературных источников по данной тематике, а также непосредственный анализ методов, алгоритмов и подходов к модификации речевых сигналов показал, что они имеют искажения, которые находят свое отражение в амплитудных, частотных и фазовых изменениях речевого сигнала. С развитием технологий, и в частности систем синтеза речи, возможности модификаций возрастают. Появляются различные подходы, состоящие из комбинации двух и более методов, а также новые методы, которые с каждым разом становятся более совершенными и менее детектированными.

Список литературы:

1. *Олейник А. Л.* Модификация временных и частотных характеристик речевого сигнала // Компьютерные инструменты в образовании. 2012. № 3.

2. *Рыбин С. В.* Синтез речи // Санкт-Петербург: университет ИТМО, 2014. 92 с.

3. *Hejna D., Musicus B. R.* The SOLAFS time-scale modification algorithm // BBN Technical Reports. 1991.

4. *Malah D.* Time-domain algorithms for harmonic bandwidth reduction and time scaling of speech signals // IEEE Transactions on Acoustics, Speech and Signal Processing. 1979.

5. *Rama-krishnan S.* Speech Enhancement, Modeling and Recognition-Algorithms and Applications // InTech. 2012.

Павел Алексеевич Панилов,
доцент кафедры систем автоматического управления
Московский государственный технический
университет имени Н. Э. Баумана
Email: panilovp.a@bmstu.ru

Андрей Викторович Кокорев,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
Email: majjor77@rambler.ru

УДК 004.81

Эволюционные алгоритмы оптимизации управления безопасностью критической инфраструктуры на основе когнитивных карт

Аннотация

Представленное исследование предлагает новый подход к обеспечению безопасности критической инфраструктуры, который основывается на интеграции эволюционных алгоритмов оптимизации и когнитивных карт. В основе этого подхода лежит разработанная модель безопасности, анализирующая ключевые компоненты уязвимости и потенциальные сценарии атак. Для оптимизации стратегий безопасности предлагается эволюционный алгоритм, который учитывает динамику и комплексность современных информационных угроз. Использование когнитивных карт дополняет предложенный подход, с помощью которого возможна визуализация взаимосвязей компонентов критической инфраструктуры.

Ключевые слова и словосочетания: *критическая инфраструктура; управление безопасностью; эволюционные алгоритмы оптимизации; когнитивные карты; модель безопасности; визуализация структуры.*

В современном информационном обществе критическая инфраструктура играет ключевую роль в обеспечении стабильности и безопасности жизнедеятельности государства и его граждан. Критическая инфраструктура включает в себя широ-

кий спектр объектов и систем, таких как энергетические сети, транспортные системы, телекоммуникационные сети, финансовые институты и другие, которые являются необходимыми для функционирования экономики и общества. Однако с развитием информационных технологий и интернета критическая инфраструктура стала все более уязвимой к кибератакам, что создает серьезные угрозы для национальной безопасности и стабильности [3; 6].

Управление безопасностью критической инфраструктуры представляет собой сложную задачу, требующую постоянного мониторинга, анализа и принятия решений в реальном времени. Сложность этой задачи обусловлена как большим разнообразием потенциальных угроз, так и динамической природой современной цифровой среды [7]. Кибератаки могут происходить внезапно и иметь различные формы: от распространения вредоносного программного обеспечения до атак на сетевую инфраструктуру.

Эволюционные алгоритмы широко применяются в различных областях, включая оптимизацию, обучение и управление [5]. Эти методы предлагают гибкий и адаптивный подход к решению сложных задач оптимизации, позволяя находить эффективные решения в условиях неопределенности и изменчивости.

Однако для эффективного управления безопасностью критической инфраструктуры требуется не только оптимизация, но анализ и принятие решений на основе знаний о среде и угрозах. В этом контексте когнитивные карты представляют собой мощный инструмент для моделирования когнитивных структур и анализа ситуаций в условиях неопределенности [4].

Модель безопасности критической инфраструктуры

Представим модель безопасности критической инфраструктуры, направленную на эффективное управление уровнями безопасности и оптимизацию работы ключевых компонентов (рис. 1).

Основные компоненты модели:

1. Энергетическая система. В данной модели энергетическая система играет решающую роль в обеспечении устойчивого энергоснабжения. Ее уровень безопасности (0,8) представляет собой баланс между эффективностью и надежностью в процессе генерации и распределения электроэнергии.

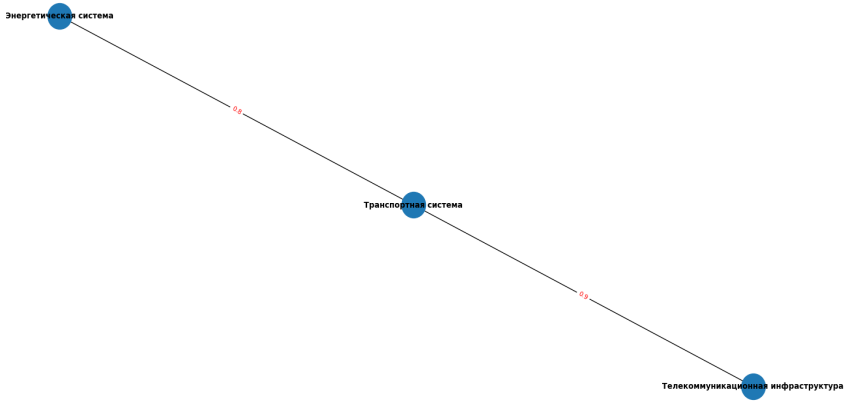

Рис. 1 Модель безопасности критической инфраструктуры

2. Транспортная система. Уровень безопасности транспортной системы (0,7) выражает важность эффективного движения людей и грузов в контексте критической инфраструктуры.

3. Телекоммуникационная инфраструктура. Система связи и передачи данных имеет высокий уровень безопасности (0,9), так как она служит основой для обмена информацией, координации и обеспечения связности внутри инфраструктуры.

Эта модель разработана с учетом современных вызовов и требований критической инфраструктуры. Уровни безопасности были выбраны на основе анализа важности каждого компонента для обеспечения устойчивой и безопасной работы системы [7]. Связи между компонентами отражают взаимозависимость и влияние каждого на общую безопасность.

Эволюционный алгоритм оптимизации

Эволюционные алгоритмы представляют собой класс метаэвристических алгоритмов оптимизации, которые моделируют процессы биологической эволюции для решения задач оптимизации. Они были разработаны на основе идеи о том, что механизмы естественного отбора и генетической мутации, присущие биологическим системам, могут быть применены для поиска оптимальных решений в задачах оптимизации [1; 2].

Алгоритм начинается с формирования популяции, где каждая особь представляет уровни безопасности ключевых компонентов, таких как энергетическая система, транспортная система и телекоммуникационная инфраструктура.

Далее для каждой особи вычисляется приспособленность, оцениваемая суммой уровней безопасности ее компонентов. Пусть P – текущая популяция, представленная матрицей размера $M \times N$, где N – размер популяции, M – количество компонентов инфраструктуры, $F(P)$ – функция приспособленности. Тогда приспособленность F_j особи j будет:

$$F_j = \sum_{i=1}^{M} S_{i,j},$$

где $S_{i,j}$ – уровень безопасности -го компонента в j-ой особи.

Мутация происходит с учетом мутационного коэффициента, который определяет вероятность мутации каждого компонента. Пусть p_m – вероятность мутации компонента. Тогда мутация каждого компонента особи j:

$$S_{i,j} = \begin{cases} S_{i,j} + \Delta \text{ с вероятностью } p_m \\ S_{i,j} \text{ с вероятностью } p_m - 1 \end{cases},$$

где Δ – случайное изменение уровня безопасности.

Родители для размножения выбираются через турнирный отбор, а кроссовер смешивает генетический материал для создания потомства.

Новая популяция формируется путем объединения лучших особей с мутировавшими потомками. Процесс повторяется в течение нескольких поколений, и результаты визуализируются через графики изменения уровней безопасности.

Наконец, выводятся параметры лучшей особи, представляющей оптимальный уровень безопасности для критической инфраструктуры. Этот алгоритм обеспечивает эффективный и адаптивный подход к управлению безопасностью, обеспечивая непрерывное совершенствование стратегий в реальном времени.

Связывание когнитивных карт с особями

Связывание когнитивных карт с особями в контексте эволюционных алгоритмов оптимизации управления безопасностью критической инфраструктуры представляет собой важный методологический подход. Каждая особь в популяции ассоциирована с индивидуальной когнитивной картой, которая отображает структуру взаимосвязей компонентов инфраструктуры. На графе когнитивной карты каждой особи представлены различные компоненты инфраструктуры (энергетическая система, транспортная система, телекоммуникационная инфраструктура), а ребра между ними отражают взаимосвязи и зависимости между компонентами.

Функция приспособленности особи j теперь учитывает информацию из ее когнитивной карты. Пусть ω_{ij} – вес ребра между ком-

понентами i и k в когнитивной карте C_j. Тогда приспособленность F_j вычисляется как сумма произведений уровней безопасности компонентов на веса ребер между ними:

$$F_j = \sum_{i=1}^{M} S_{i,j} \times \sum_{(i,k)\in E_j} \omega_{ij},$$

где E – представляет собой множество ребер в когнитивной карте j-й особи.

Когнитивные карты подвергаются мутациям, включающим изменения в структуре взаимосвязей между компонентами. Мутации могут включать в себя добавление, удаление или изменение весов связей. Динамическая адаптация когнитивных карт обеспечивает устойчивость и эффективность в новых условиях, позволяя системе быстро реагировать на изменяющиеся угрозы и условия.

После каждого поколения строятся графики изменения лучших и средних уровней безопасности (рис. 2), дополненные визуализацией когнитивных карт в виде графов для наилучших особей. Это помогает исследователям и практикам лучше понять принятые стратегии и выявить потенциальные улучшения.

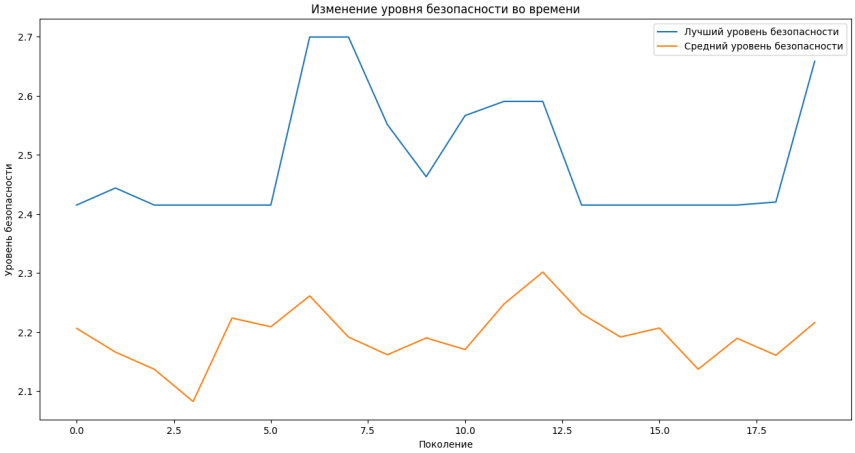

Рис. 2. Изменение уровня безопасности во времени

В представленных графах (рис. 3) каждая особь (обозначена как «Особь i») представляет собой отдельную конфигурацию уровней безопасности для компонентов критической инфраструктуры. Для каждой особи создан свой граф, где узлы представляют компо-

ненты (например, «Энергетическая система i»), а ребра представляют связи между компонентами.

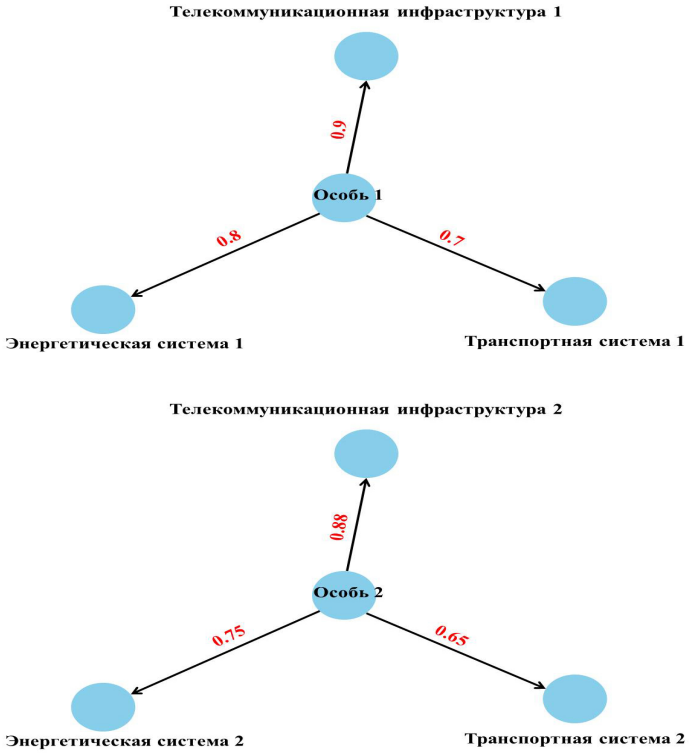

Рис. 3. Связь между когнитивной картой и уровнями безопасности (Особь {1, 2})

Особенность этого графа заключается в том, что, помимо уровней безопасности компонентов, включены веса связей между ними из соответствующей когнитивной карты. Эти веса отражают степень влияния одного компонента на другой с точки зрения безопасности.

Процесс интеграции когнитивных карт в эволюционный алгоритм выражается через связь между уровнями безопасности и весами связей в каждой особи.

В данной работе был представлен подход к оптимизации управления безопасностью критической инфраструктуры на основе эволюционных алгоритмов и когнитивных карт. Связывание когнитивных карт с особями позволяет эффективно учитывать сложные взаимосвязи между компонентами инфраструктуры, что способствует более точному и адаптивному управлению безопасностью.

Использование эволюционных алгоритмов для оптимизации параметров управления безопасностью позволяет достигать оптимальных решений в условиях сложной и динамически изменяющейся цифровой среды. Мы продемонстрировали применение этих методов на примере сети критической инфраструктуры, показав их эффективность и устойчивость в различных сценариях.

В статье также выдвигается ряд направлений для будущих исследований. В частности, можно дальше развивать методы адаптации когнитивных карт к изменяющимся условиям и угрозам, а также исследовать возможности применения более сложных моделей когнитивных карт для более точного моделирования системы.

Список литературы:

1. *Абузяров А. А., Макаров А. А.* Применение и сравнение эволюционных алгоритмов в рамках задачи обучения с подкреплением для неустойчивых систем // Инженерный вестник Дона. 2023. № 6 (102).

2. Методики и алгоритмы эволюционной процедуры обоснования требований к безопасности информации автоматизированных систем // Методы и средства эволюционного и структурного моделирования при обосновании требований к программным системам защиты информации. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2015.

3. *Северцев Н. А., Бецков А. В.* Введение в безопасность. ТЭИС. МГУ имени М. В. Ломоносова. 2009.

4. *Степанова Е. С., Машкина И. В., Васильев В. И.* Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности // Известия ЮФУ. Технические науки. 2010. № 11 (112).

5. *Тань Л., Новикова С. В.* Применение пошагового метода обучения для эволюционного алгоритма в задачах многокритериальной оптимизации // Вестник Казанского государственного энергетического университета. 2022. Т. 14. № 3 (55).

6. *Цибизова Т. Ю., Панилов П. А., Кочешков М. А.* Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования// Известия Тульского государственного университета. Технические науки. 2023. № 6.

7. *Шабуров А. С.* О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2018. № 26.

Евгений Сергеевич Поликарпов,
кандидат технических наук, доцент,
начальник кафедры специальных
информационных технологий УНК ИТ
Московский университет МВД России
имени В. Я. Кикотя
E-mail: binox@mail.ru

Денис Сергеевич Хорзов
курсант факультета подготовки специалистов
в области информационной безопасности
Московский университет МВД России
имени В. Я. Кикотя
E-mail: denis.khor03@gmail.com

УДК 004.056
УДК 004.032.26

WEB3 – технологии развития безопасного интернета будущего

Аннотация

Цель исследования состоит в сравнительном анализе развития технологий всемирной компьютерной сети (web). Рассматриваются этапы развития web-технологий с учетом применения современных механизмов безопасности информации. Выделяется главная особенность web3, заключающаяся в децентрализации, основанной на распределенном блокчейне. Исследуется степень интеграции интернет-технологий и цифровой криптографии. Выделяются основные принципы и тенденции развития открытого и безопасного интернета.

Ключевые слова и словосочетания: *web3; блокчейн; нейронная сеть; смарт-контракты; кибербезопасность; децентрализованные финансы (DeFi); криптовалюта; метавселенные.*

Современное состояние интернета характеризуется массовым использованием социальных сетей, онлайн-сервисов, электронной коммерции и различных приложений. Так называемый Web3 представляет собой новую фазу интернета, которая стремится к созданию децентрализованных, управляемых пользователями платформ, использующих в своей работе блокчейн-технологии. Основные

принципы Web3 включают в себя защиту личных данных, повышение безопасности и приватности, а также уменьшение зависимости от крупных корпораций. Необходимость перехода к Web3 обусловлена рядом проблем, таких как недостаточная защита данных, централизация информации в руках крупных компаний (на серверах), а также угрозы кибербезопасности. Переход к Web3 представляет собой шаг к созданию более безопасной, прозрачной и демократической среды в интернете, где пользователи имеют большой контроль над своими данными.

В условиях растущей цифровизации общества переход к более защищенной и децентрализованной модели интернета становится все более необходимым для обеспечения безопасности и конфиденциальности пользователей.

Следует различать понятия интернет и Web. Простыми словами, интернет – это так называемая глобальная сеть сетей, в то время как Web – одна из таких сетей. Также в сети можно найти частое сравнение этих двух понятий: если интернет был бы библиотекой, то Web в нем – коллекция книг.

Наконец, рассмотрение технологий и основных принципов построения Web3 невозможно без краткого погружения в историю развития данной интернет-технологии.

Началом появления Web, иначе именуемой некоторыми людьми как WWW (World Wide Web – Всемирная Компьютерная Сеть), считается 1989 год. Именно тогда Тим Бернерс-Ли, действующий глава W3C (World Wide Web Consortium – Консорциум Всемирной паутины), работая над внутренней сетью организации, предложил глобальный гипертекстовый проект (т. е. такой способ организации информации, при котором один источник информации будет связан с другим посредством связи – ссылок). Несколько позже Тим с его помощниками разработали протокол передачи данных HTTP и язык гипертекстовой разметки (HTML), а в 1991 г. – первый веб-сервер [1].

В целом можно сказать, что на первых порах Web позволял пользователям лишь просматривать информацию в сети. Буквально это была книга, которую можно было читать, никакого ныне привычного интерактивного взаимодействия (например, процесс регистрации на сайте), за исключением ссылок, между браузером и пользователем на тот момент не существовало.

Все названное выше описывает так называемый Web первой версии. Не существует четкой границы между первой и второй версиями технологии, однако с появлением таких инструментов и методов взаимодействия человека и устройства, как CSS, JavaScript,

интеграции с большими объемами данных и многие другие, связывают начало следующей версии Web – Web2. На данном этапе развития сети пользователям предоставляется право воздействовать на существующие ресурсы, например, появляются социальные сети, таргетированная реклама и др. Теперь сайты представляют собой не просто статичные страницы, а красивые, динамичные и, главное, многофункциональные сервисы. Пользователи могут общаться друг с другом, оплачивать покупки, смотреть фильмы посредством технологии Web.

Также стоит упомянуть, что на первоначальном этапе развития сети она в основном разрабатывалась компаниями для пользователей; в обновленной же ее версии уже пользователи стали играть большую роль в создании и совершенствовании как контента, так и самой технологии.

Переходя к описанию новой, третьей, версии Web, следует отметить, что на данный момент в широкое применение она пока не вошла: технологии работы Web2 больше изучены и привычны обычному пользователю. Однако, как и любая другая новая разработка, Web3 сперва должна доказать свое преимущество перед предшественниками, прежде чем будет принята сообществом.

Технологии работы Web3 значительно отличаются от ее старших версий. Здесь получили широкое распространение такие понятия как блокчейн, децентрализация, семантический анализ, искусственный интеллект и др. Если Web второй версии многими воспринимается как логичное продолжение, дополнение первой, то третья версия в корне меняет все ранее существовавшее представление о сети. Теперь это должен быть прозрачный, безопасный, универсальный и конфиденциальный инструмент взаимодействия пользователей [4].

Главная особенность Web3 – децентрализация. Она предполагает хранение информации не в одном конкретном месте, а в разных – у каждого пользователя, который имеет доступ к блокчейну, отдельно. Аналогом принципа децентрализации служит протокол BitTorrent – каждый торрент-клиент в сети одновременно хранит и получает данные с других устройств сети, а не с конкретного сервера.

Блокчейн (англ. «*block*» – блок, и «*chain*» – цепь) – технология распределения информации так, чтобы изменение или манипулирование данными было невозможно или затруднено. Если максимально упростить, то операция занесения данных в блокчейн выглядит следующим образом: пользователь производит какое-либо действие на платформе блокчейна, информация об этом подписывается циф-

ровой подписью владельца, после чего указанные данные заносятся в цифровой реестр, и вычисляется новая контрольная сумма блокчейна, далее описанный механизм повторяется для всех последующих операций. Данный механизм обеспечивает прозрачность и безопасность всех действий в среде. Здесь аналогом также выступает протокол BitTorrent: пользователи могут просматривать и добавлять данные, но не могут изменять уже существующие.

С появлением технологии блокчейн неразрывно связан термин смарт-контракта – технологии подтверждения достоверности проведенной транзакции. Аналогом смарт-контракту выступает обычный договор о покупке какой-либо вещи в реальной жизни. Отличие состоит лишь в том, что при несоблюдении условий договора потерпевшая сторона имеет право взыскать определенную неустойку за нарушение правил, в случае же со смарт-контрактом всевозможные нарушения пресекаются еще на этапе начала операции, что избавляет стороны от возможной рутины при различных конфликтах, автоматизируя тем самым процесс проведения транзакций в блокчейне.

В процессе поиска информации технология Web3 предполагает обработку не просто конкретных слов или фраз, а целого текста, составленного из множества слов. Яркий пример: ранее, при поиске необходимой информации в сети люди вводили запрос и получали на него ответ, исходя лишь из содержания ресурса, в котором расположена эта информация. Более продвинутые пользователи со временем научились искать необходимую информацию посредством ключевых слов. В Web3 полученный запрос прежде всего анализируется исходя из принципов семантического анализа, т. е. выделяется его смысл, полнота, структура, а уже после – выдается ответ пользователю на основе проведенного анализа запроса.

Указанный выше подход к обработке данных невозможен без машинного обучения – метода программирования устройства, основанного, в отличие от традиционного программирования, на получении решения задачи без явного указания инструкций. Иными словами, если в обычном программировании человек пишет код, который при любых обстоятельствах должен давать четкий определенный ответ, то в случае с машинным обучением программа при получении одних и тех же данных может выдать разный ответ. Машинное обучение уже сейчас используется практически во всех областях деятельности человека – это и составление текста, и создание изображений, видео, выявление заболеваний, анализ различных ситуаций и принятие на их основе решений и многое другое. Бесспорное преимущество машинного обучения перед его предше-

ственником – безграничные возможности применения и возможность решать различные задачи понятным человеку способом.

Изучив основные принципы технологии Web3, можно переходить к описанию реальных примеров ее применения – Dapps – децентрализованных приложений, таких как метавселенные, игры, биржи и др. [2]. Обычно DApps работает на технологии блокчейн, а для их использования обычно нужен криптовалютный кошелек и конкретная криптовалюта, которая поддерживает сеть, где работает приложение [3].

Метавселенные очень похожи на уже давно существующие технологии дополненной реальности, однако, в отличие от последних, они предоставляют пользователю не просто погрузиться в виртуальный мир, а стать его неотъемлемой частью, как в реальном мире. В метавселенных пользователи взаимодействуют друг с другом, в то время как дополненная реальность добавляет виртуальные элементы к реальному миру через специальные устройства. Один из наиболее известных и популярных примеров метавселенной – виртуальный мир «Second Life», где пользователи могут создавать своих уникальных персонажей, взаимодействовать с другими участниками, строить виртуальные объекты и среды, посещать мероприятия, торговать и даже заниматься бизнесом.

Главный продукт технологии Web3 – децентрализованные финансы (DeFi) – представляет собой различные биржи, например, «Binance», позволяющие пользователям безопасно и просто обращаться со своими сбережениями. Важным преимуществом здесь является отсутствие третьей стороны при проведении операций, что, в свою очередь, предполагает отсутствие дополнительной платы за обслуживание сервиса.

Web3 игры, такие как «Splinterlands» и «Sorare», используют технологию блокчейн в процессе работы. Web3 игроки имеют полный контроль над своими игровыми активами, которые могут быть проданы, обменены или использованы в других играх с помощью криптовалюты, что отличает их от обычных игр, где активы часто привязаны к конкретной платформе. Эти игры обеспечивают игрокам большую автономию, экономическую выгоду и интересные игровые механики, которые отличают их от традиционных игр.

Web3 платформы для обмена музыкой используют алгоритмы машинного обучения для анализа контента и выдачи пользователю определенных рекомендаций на основе его предпочтений. Также неоспоримым преимуществом здесь, как и в случае с DeFi, является отсутствие посредников при продаже контента, таким образом, его

правообладатель получает максимальную прибыль с продажи своего труда.

Как видно из описанного выше, технологии Web3 уже сейчас нашли для себя широкое применение. Такие ключевые понятия, как блокчейн и смарт-контракт, обеспечивающие безопасность, прозрачность и универсальность при проведении операций, семантический анализ и машинное обучение, позволяют программам понимать человеческий язык и выдавать на его основе более релевантные результаты, а также предоставляют практически безграничные возможности применения Web3 в повседневной жизни. Подводя промежуточный итог, Web3 технологии предоставляют ряд значительных преимуществ в сравнении с традиционными централизованными системами, способствуя развитию инноваций, увеличению безопасности и контроля пользователей над своими данными и активами.

Однако, несмотря на неоспоримые преимущества новой технологии, она имеет и ряд серьезных недостатков, которые могут свести к нулю все ее преимущества.

Первое, что стоит сказать, Web3 на начальных стадиях использования обычному пользователю может быть трудно освоить. Его могут отпугнуть принципы децентрализации или блокчейна, оплаты различных услуг с помощью криптовалюты и т. д., не существующие в Web2. Второе – большая экологическая нагрузка и зависимость от внешних источников, так как Web3 неразрывно связан с криптовалютами, которые, в свою очередь, являются основным источником проведения транзакций в блокчейне, и Web3 никак не может существовать без нее, а их получение сопровождается большими энергетическими затратами. Наконец, на данный момент не существует четкого регулирования данной области Web3, поэтому разрешение возникающих конфликтов может оказаться невозможной задачей.

Таким образом, технология Web3 является закономерным этапом в развитии сети, устраняя недостатки предшественников и повышая уровень сервиса для пользователей. Те принципы, что лежат в основе Web3, закрывают практически все ныне существующие потребности пользователей в конфиденциальности данных, прозрачности при проведении финансовых операций и простоте использования. Хотя технология еще находится на начальных этапах своего становления, перспективы ее применения практически безграничны – от развлекательного контента до финансовой деятельности, и, скорее всего, по мере развития этот список будет только расти вместе с потребностями пользователей.

Список литературы:

1. Всемирная паутина — Википедия. URL: https://ru.wikipedia.org/wiki/Всемирная_паутина (дата обращения: 17.04.24).

2. Что такое децентрализованные приложения (dApps)? URL: https://traderblog.net/dapps/ (дата обращения: 17.04.24).

3. Что такое децентрализованные приложения (DApp) | Binance Academy. URL: https://academy.binance.com/ru/articles/what-are-decentralized-applications-dapps (дата обращения: 17.04.24).

4. Что такое Web 3.0, и почему он всем стал нужен. URL: https://habr.com/ru/articles/653533/ (дата обращения: 17.04.24).

Геннадий Юрьевич Пучков
кандидат технических наук,
ведущий научный сотрудник
ЦСИТ НИИСТ
ФКУ НПО «СТиС» МВД России
E-mail: pgu7@ya.ru

УДК 001.89:343

К вопросу об использовании информационных технологий в сфере борьбы с незаконным оборотом наркотиков

Аннотация

Настоящая статья посвящена вопросам автоматизации деятельности подразделений по борьбе с незаконным оборотом наркотических средств и их прекурсоров (далее – подразделения НОН). В статье описываются основные результаты ОКР «Сервис НОН», внедрение которых позволило существенно повысить уровень автоматизации деятельности подразделений НОН, создать базис для дальнейшего развития информационных технологий в сфере борьбы с преступностью в данной области. В статье формулируются предложения по дальнейшему совершенствованию специального программного обеспечения, разработанного в рамках ОКР «Сервис НОН», в том числе в части, касающейся контроля за транспортными средствами, представляющими оперативный интерес для подразделений НОН.

Ключевые слова и словосочетания: *Сервис НОН; наркотические средства; незаконный оборот наркотиков; ИСОД МВД России; информационные технологии; транспортные средства.*

В 2021 г. в рамках ОКР ««Разработка информационно-поисковой системы Сервис ИСОД МВД России «Незаконный оборот наркотиков», шифр «Сервис «НОН», было разработано и с 1 декабря 2022 г. введено в эксплуатацию изделие «Сервис ИСОД МВД России «Незаконный оборот наркотиков» (далее – Сервис «НОН»), которое позволило существенно повысить уровень автоматизации оперативной деятельности подразделений центрального аппарата ГУНК МВД России и территориальных подразделений НОН.

Сервис «НОН» представляет собой специальное программное обеспечение, разработанное в соответствии с базовыми требовани-

ями, предъявляемыми к технологическим решениям, применяемым при создании, эксплуатации и развитии ИСОД МВД России и ее компонентов [2].

Создание Сервиса «НОН» явилось существенным событием в сфере автоматизации деятельности подразделений НОН. До его разработки в подразделениях центрального аппарата ФСКН России, а потом и в ГУНК МВД России, применялись отдельные компьютерные программы, предназначенные в основном для сбора и обработки статистической информации и решения отдельных поисковых задач. В территориальных подразделениях НОН применялись либо компьютерные программы, разработанные сотрудниками местного информационного центра в интересах данного подразделения (далее – СПО[1] регионов), либо стандартные инструменты, входящие в состав Microsoft Office.

В СПО регионов учет преступлений, лиц, их совершивших, и другой информации, представляющей оперативный интерес, осуществлялся на уровне обслуживаемого региона. Для этого, как правило, создавалась региональная база данных, в связи с чем возможность использования в оперативной деятельности информации, накопленной в такой базе, для сотрудников подразделений НОН другого региона не обеспечивалась. С введением в эксплуатацию Сервиса «НОН» ситуация кардинально изменилась.

Сервис «НОН» позволяет обеспечить работу абонентов в крупномасштабной компьютерной (вычислительной) сети, охватывающей подразделения центрального аппарата ГУНК МВД России и все подразделения территориальных подразделений НОН (при необходимости может охватывать и всех сотрудников подразделений НОН и ГУНК МВД России).

Для создания такой сети использовалась технология «тонкий клиент», принятая в качестве базовой для создания ИСОД МВД России. Она заключается в том, чтобы использовать общие для всех абонентов сети (сервиса) вычислительные ресурсы, выделяемые в центре обработки данных ИСОД МВД России. При помощи данных ресурсов создается централизованная база данных с возможностью использования общих для всех клиентов инструментов поиска и обработки хранящейся в ней информации. В данном случае компьютер сотрудника НОН применяется как средство ввода запросов в централизованный банк данных, получения и представления в требуемом виде ответов на сделанные запросы.

[1] СПО – специальное программное обеспечение.

Основная идея создания централизованного банка данных Сервиса «НОН» состояла в том, чтобы его формирование на первом этапе осуществлялось путем миграции данных из локальных баз территориальных подразделений НОН, а дальнейшее его развитие (наполнение) осуществлялось бы силами сотрудников подразделений НОН, получающих новые оперативные данные в процессе ОРД.

Таким образом, для любого сотрудника подразделений НОН появилась возможность доступа в онлайн-режиме к оперативно-значимой информации, накопленной подразделениями ГУНК МВД России и территориальными подразделениями НОН других регионов страны, а также к информации, хранящейся в базах данных сервисов, входящих в состав ИСОД МВД России, таких как СООП, СОДЧ, ИБД-Ф, ПТК «Розыск-Магистраль. Кроме того, в процессе разработки Сервиса «НОН» с учетом специфики деятельности подразделений НОН были созданы инструменты поиска и обработки информации, хранящейся в централизованном банке данных, в том числе и при помощи современных методов интеллектуального анализа, которыми теперь может пользоваться любой абонент (клиент) сервиса.

Все это позволило существенно повысить уровень автоматизации ОРД в сфере НОН особенно в отношении лиц, занимающихся преступной деятельностью, в процессе перемещения по различным регионам России.

Необходимость и полезность Сервиса «НОН» для использования в оперативной работе подтверждается заинтересованностью оперативных сотрудников в совершенствовании разработанного программного обеспечения: по результатам эксплуатации разработанного СПО в течение полугода с мест поступило несколько десятков предложений по его совершенствованию.

В связи с изложенным в настоящее время ведется подготовка для проведения комплекса мероприятий по модернизации Сервиса «НОН» в соответствии с данными предложениями.

Вместе с тем следует отметить, что современные технологии в области идентификации транспортных средств позволяют реализовать новые возможности по раскрытию преступлений в сфере НОН, в связи с чем при модернизации Сервиса «НОН» не стоит ограничиваться только поступившими с мест предложениям.

В рамках государственной программы города Москвы «Информационный город», утвержденной постановлением Правительства Москвы от 9 августа 2011 г. № 349-ПП [1], создана государственная информационная система «Единый центр хранения и обработки данных» (далее – ГИС «ЕЦХД»). Данная система предназначена

для сбора и обработки видеоинформации, поступающей от камер видеонаблюдения, установленных на территории г. Москвы. Для решения задач подразделений НОН интерес представляет сегмент системы, предназначенный для идентификации транспортных средств (далее – сегмент ИТС). Он разработан на базе специального программного обеспечения, позволяющего определять тип, марку и цвет автомобилей, их принадлежность, восстанавливать маршруты их движения в заданном отрезке времени, осуществлять прогнозирование маршрутов и определять текущее местонахождение мобильных объектов. Использование сегмента ИТС позволит существенно повысить эффективность ОРД в сфере контроля перевозок наркотических веществ и их прекурсоров.

Однако существенным недостатком ГИС «ЕЦХД» является ограниченность территории ее применения границами московского региона.

Для решения задач идентификации транспортных средств в других регионах страны представляется целесообразным использовать результаты исследований ФКУ НПО «СТиС» МВД России, полученные в 2023 г. в ходе тестирования и приемочных испытаний программного обеспечения «ЦАФАП-Москва» и программного обеспечения модуля центра хранения материалов единой сквозной системы перехвата и розыска транспортных средств на территории ЦФО.

Идея, предложенная разработчиками «ЦАФАП-Москва», как и в случае с ГИС «ЕЦХД», состоит в том, чтобы для сбора информации о транспортных средствах, представляющих оперативный интерес, использовать видеокамеры, устанавливаемые в регионах для контроля соблюдений правил дорожного движения, а информацию аккумулировать в центральном банке данных, доступ к которому осуществляется с использованием технологии «тонкий клиент».

По результатам испытаний приказом Министерства внутренних дел Российской Федерации от 29 марта 2021 г. № 169 данное программное обеспечение было поставлено на снабжение органов внутренних дел Российской Федерации (сервис ИСОД МВД России «Паутина») с целью дальнейшего его внедрения в деятельность территориальных органов МВД России как единого сервиса ИСОД МВД России федерального уровня.

Таким образом, представляется целесообразным при разработке технического задания на ОКР по модернизации Сервиса «НОН» предусмотреть работы по его сопряжению с сегментом ИТС ГИС «ЕЦХД» (для решения оперативных задач на территории

московского региона) и сервисом ИСОД МВД России «Паутина» (для решения данных задач на территории других регионов).

В заключение необходимо отметить, что комплексный подход к проведению мероприятий по совершенствованию Сервиса «НОН», включающий в себя реализацию предложений территориальных подразделений НОН и осуществление его сопряжения с сегментом ИТС ГИС «ЕЦХД» и сервисом ИСОД МВД России «Паутина», позволит существенно повысить эффективность деятельности подразделений НОН.

Список литературы:

1. *Ливанский А. Г., Пучков Г. Ю.* Опыт использования систем интеллектуального видеонаблюдения территориальными органами МВД России (на примере Московского региона) // Журнал «Научно-технический портал МВД России». 2021. № 4 (40).

2. *Пучков Г. Ю., Сергеева С. В., Дудникова Е. В.* Специальное программное обеспечение для автоматизации деятельности подразделений МВД России по борьбе с незаконным оборотом наркотических средств // Полицейский вестник Всероссийского института повышения квалификации сотрудников МВД России. 2022. № 1 (6).

Виктор Андреевич Рогожкин,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: vrogozhkin@internet.ru

УДК 004.94

Современные тенденции индивидуальной профилактической работы участковых уполномоченных полиции с применением информационных технологий

Аннотация

В статье идет речь о возможностях и перспективах использования модели социального рейтинга в вопросах проведения индивидуальной профилактической работы участковыми уполномоченными полиции.

Ключевые слова и словосочетания*: участковый уполномоченный полиции; индивидуальная профилактическая работа; девиантное поведение.*

Профилактическая деятельность органов внутренних дел является важным направлением по поддержанию правопорядка в Российской Федерации. В своем выступлении Министр внутренних дел Российской Федерации В. А. Колокольцев на расширенном заседании коллегии указал, что одной из наиболее продуктивных форм превентивного воздействия является индивидуальная профилактическая работа [5].

В системе МВД России индивидуальная профилактическая работа регламентируется Федеральными законами и ведомственными правовыми актами МВД России. Основная роль в данном направлении деятельности уделена службе участковых уполномоченных полиции по делам несовершеннолетних.

Одной из основных форм несения службы участковым уполномоченным полиции (далее – УУП) является индивидуальная профилактическая работа. В настоящий момент УУП проводит индивидуальную профилактическую работу с семью категориями лиц, состоящих на профилактическом учете в органах внутренних дел[1].

[1] О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности (вместе с «Инструкци-

Индивидуальная профилактическая работа включает в себя такую форму воздействия, как посещение по месту жительства лица, состоящего на профилактическом учете. Данная работа позволяет провести беседы с членами его семьи, соседями, установить круг общения, а также осознать подучетным элементом, что органами внутренних дел им уделяется особое внимание. Такая мера определенно имеет положительное воздействие, однако есть и обратная сторона.

Согласно требованиям приказа МВД России от 29 марта 2019 г. № 205 УУП обязан посещать по месту жительства (пребывания):

– лиц, указанных в подп. 33.1 Инструкции, не реже одного раза в месяц;

– лиц, указанных в подп. 33.2 Инструкции, не реже одного раза в месяц;

– лиц, указанных в подп. 33.3, 33.6 Инструкции УУП, не реже одного раза в квартал.

Допускается посещение по месту жительства (пребывания) лиц, состоящих на профилактическом учете чаще, но это может вызвать негативную реакцию у членов семьи и соседей, особенно если для первой категории судом вынесено постановление о запрете пребывания вне указанных помещений в определенное время суток.

Внедрение в деятельность органов внутренних дел Единой системы информационно-аналитического обеспечения деятельности органов внутренних дел позволило УУП вести электронный учет лиц, состоящих на индивидуальном профилактическом учете. Сервис позволяет накапливать такую информацию, как персональные данные родственников, круга общения, условия проживания, занятость, транспорт, охотничье и оружие ограниченного поражение, результаты посещения по месту жительства и проведения профилактической беседы, а также получать сведения о правонарушениях напрямую из Сервиса обеспечения деятельности дежурной части. В настоящее время идет модернизация СООП ИСОД МВД России[1], и его возможности будет только расширяться.

Авторы данной статьи предлагают в своей работе внедрить систему социального рейтинга в отношении лиц, состоящих на профилактическом учете. Система социального рейтинга необходима

ей по исполнению участковым уполномоченным полиции служебных обязанностей на обслуживаемом административном участке», «Наставлением по организации службы участковых уполномоченных полиции»): приказ МВД России от 29 марта 2019 г. № 205.

[1] СООП ИСОД МВД России – Сервис охраны общественного порядка Единой системы информационно-аналитического обеспечения деятельности МВД России.

для оценки определенных лиц или организаций на основании положительных или негативных весовых коэффициентов поведения при помощи сбора, обработки и предоставлении информации из цифровых сервисов и использования технологии больших данных [1].

Таким образом, УУП, используя сведения, внесенные в СООП ИСОД МВД России и сведения из внешних источников, сможет получить социальный рейтинг или так называемый коэффициент девиантного поведения. На основании рейтинга профилактируемых лиц УУП будет выстроена целевая профилактическая работа. Помимо выполнения минимума, регламентируемого ведомственными правовыми актами, УУП на основе коэффициента девиантного поведения сможет выявлять подучетный элемент, представляющий наибольшую социальную опасность, а также склонность к совершению повторных правонарушений [2–4].

Подводя итоги, можно сделать вывод:

Во-первых, внедрение в повседневную деятельность УУП учет рейтинга девиантного поведения подучетного элемента позволит проводить целенаправленную индивидуальную профилактическую работу и оптимизировать индивидуальную нагрузку на каждого УУП.

Во-вторых, минимизирует негативное отношение к правоохранительным органам родственников и соседей профилактируемого лица, не требующего излишнего внимания. Рейтинг девиантного поведения окажет положительное влияние на профилактируемое лицо не только из-за страха привлечения к ответственности за совершение правонарушения, но и стремления к социально-приемлемому поведению.

Список литературы:

1. *Комарова О. М.* Экономическое обоснование эффективности использования системы социального рейтинга как формы государственного контроля над обществом // Управленческий учет. 2022. № 4-1.

2. *Кубасов И. А.* Инновационные технологии в противодействии экстремизму и терроризму: сборник статей по материалам Всероссийской научно-практической конференции. Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2021.

3. *Кубасов И. А., Минаев А. В.* Аспекты применения технологий искусственного интеллекта для профилактики радикализма в молодежной среде: сборник статей по материалам Всероссийской

научно-практической конференции. Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации».

4. *Шапкин А. В., Кубасов И. А.* Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 годы: сборник статей по материалам Международной научно-практической конференции / отв. за вып. В. О. Лапин. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2019.

5. URL: https://xn--b1aew.xn--p1ai/document/10091957 (дата обращения: 29.01.2024).

Виктор Андреевич Рогожкин,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: vrogozhkin@internet.ru

Артем Викторович Кирюхин,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: nokia26340@mail.ru

УДК 343.4

Основные тенденции развития законодательства в области цифровой трансформации органов внутренних дел Российской Федерации

Аннотация

В статье рассмотрены аспекты современной цифровой трансформации органов внутренних дел Российской Федерации, обусловливающие эволюцию права. Выявлены основные тенденции развития законодательства в области цифровой трансформации органов внутренних дел. Обоснован вывод о необходимости постоянного совершенствования законодательства в области цифровой трансформации органов внутренних дел с учетом развития цифровых технологий, появления новых угроз и изменения потребностей общества.

Ключевые слова и словосочетания*: цифровая трансформация; органы внутренних дел; цифровые технологии; законодательство.*

Современная цифровая трансформация органов внутренних дел Российской Федерации предполагает развитие и внедрение цифровых технологий с целью повышения оперативно-служебной деятельности и оптимизации распределения ресурсов (в том числе людских). Эта трансформация охватывает различные аспекты, включая технологические, правовые и этические [2].

Одним из ключевых компонентов цифровой трансформации является внедрение передовых систем управления данными. Органы внутренних дел могут использовать цифровые платформы для эффективного хранения, обработки и анализа огромных объемов

данных. Это позволяет им получать ценную информацию и принимать решения на основе данных в режиме реального времени. Кроме того, цифровые инструменты (например, прогнозная аналитика) могут помочь в выявлении закономерностей и тенденций, способствуя разработке профилактических мер [4]. Внедрение современных информационно-коммуникационных технологий позволяет сотрудникам полиции в режиме реального времени обеспечить обмен информацией с населением и другими подразделениями органов внутренних дел. Используя цифровые платформы, сотрудники полиции могут установить прямые каналы связи с гражданами. Более того, платформы социальных сетей могут служить для общественности средством сообщения о преступлениях, обеспечивая более быстрое реагирование и более активное участие граждан в поддержании общественной безопасности.

В целом цифровая трансформация органов внутренних дел кардинально изменяет методы выявления, раскрытия и расследования преступлений. Передовые технологии, такие как искусственный интеллект и большие данные, позволяют оперативно осуществлять анализ больших объемов данных, выявлять закономерности. Так, инструменты цифровой криминалистики позволяют сотрудникам полиции собирать и анализировать цифровые доказательства, обеспечивая тщательное расследование [3]. Например, использование камер наблюдения, датчиков и устройств интернета вещей, устройств дополненной реальности может повысить ситуационную осведомленность и обеспечить существенное повышение эффективности оперативно-служебной деятельности органов внутренних дел. Осуществляемый мониторинг «критических» мест в режиме реального времени может обеспечить выявление и возможно предотвращение преступлений до их совершения, а интеллектуальные устройства могут предоставлять оперативные данные, помогая в принятии управленческих решений и обеспечении безопасность сотрудников полиции [1].

Рассмотренные аспекты современной цифровой трансформации органов внутренних дел обусловливают эволюцию права. Поэтому следует отметить основные тенденции развития законодательства в области цифровой трансформации органов внутренних дел.

1. Развитие законодательства в части цифровизации оперативно-служебной деятельности органов внутренних дел, основанной на сборе и анализе больших данных. Так, например, для уполномоченных участковых полиции имеется возможность накапливать информацию из физических носителей (бумажных журналов) в Электронный паспорт административного участка при рабо-

те с сервисом СООП ИСОД МВД России. Переход от бумажных носителей результатов профилактической работы к электронным не только автоматизирует оперативно-служебную деятельность сотрудников полиции, но и переводит в цифровое поле деятельность руководителя подразделения для контроля.

2. Развитие законодательства в части формирования и хранения цифровых доказательств о неправомерном доступе к компьютерной информации, краже данных с использованием вредоносных программ, онлайн-мошенничества и негативном воздействии на критическую информационную инфраструктуру.

3. Развитие законодательства в части достижения баланса между соблюдением прав и свобод граждан на неприкосновенность частной жизни и обеспечением безопасности информации.

4. Развитие законодательства в части расширения сотрудничества органов внутренних дел с компаниями, предоставляющими услуги в сфере информационных технологий, научными организациями и другими заинтересованными сторонами для широкого внедрения инновационных цифровых технологий в целях повышения эффективности оперативно-служебной деятельности на основе современных достижений научно-технического прогресса.

5. Развитие законодательства в части реформирования системы профессионального обучения и повышения квалификации сотрудников органов внутренних дел по эффективному противодействию правонарушениям с использованием информационно-телекоммуникационных технологий.

В заключение следует заметить, что развитие законодательства в области цифровой трансформации органов внутренних дел должно быть постоянным с учетом развития цифровых технологий, появления новых угроз информационной безопасности и изменения потребностей информационного общества.

Список литературы:

1. *Кубасов И. А.* Инновационные технологии в противодействии экстремизму и терроризму: сборник статей по материалам Всероссийской научно-практической конференции. Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2021.

2. *Кубасов И. А.* Искусственный интеллект как драйвер цифровой трансформации МВД России // Криминологический журнал. 2023. № 2.

3. *Кубасов И. А., Минаев А. В.* Аспекты применения технологий искусственного интеллекта для профилактики радикализма в молодежной среде: сборник статей по материалам Всероссийской научно-практической конференции. Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2021.

4. *Кубасов И. А., Минаев А. В.* Внедрение технологии искусственного интеллекта для выявления девиантного поведения в молодежной среде // Охрана, безопасность, связь. 2022. № 7-1.

Ольга Николаевна Рудакова,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: olg.rudackova8@mail.ru

УДК 342

Информационная безопасность как гарант защиты естественных прав человека

Аннотация

В данной статье рассмотрен вопрос обеспечения информационной безопасности, который подразумевает совместное взаимодействие человека, общества и государства. Автором обращено внимание на важность соблюдения личностью профилактических мер, направленных на обеспечение личной информационной безопасности.

Ключевые слова и словосочетания: *информационная безопасность; естественные права; человек; личность; интернет; цифровизация; статистика; утечка информации; личная информационная безопасность.*

Эпоха технологической революции стала новым этапом существования человечества, где в основу легло развитие информатизации и цифровизации. По этим причинам как никогда актуален вопрос об обеспечении информационной безопасности как гаранта естественных прав человека.

По мнению В. В. Баранова, под информационной безопасностью следует понимать «такое состояние защищенности национальных интересов Российской Федерации как совокупности сбалансированных интересов личности, общества и государства, при котором достигнут необходимый уровень готовности и способности противостоять деструктивным воздействиям, реальным и потенциальным опасностям и угрозам, возникающим в информационной среде». Иными словами, человек, общество и государство должны в равной степени вносить свой вклад в обеспечение информационной безопасности.

Безусловно, обеспечение информационной безопасности нормативно урегулировано как на международном, так и на национальном уровне, однако необходимо признать, что в настоящее время

действующее законодательство не способно в полной мере обеспечить максимальную безопасность в сети Интернет. Связано это с тем, что глобальная Всемирная паутина является другой реальностью и иным стремительно развивающимся миром [5], за которым реальная (оффлайн) жизнь не успевает.

Действительно, за короткий промежуток времени нтернет-технологии проникли во все сферы жизнедеятельности человека: в образование – все образовательные организации имеют платформы, позволяющие получать непрерывно основное и дополнительное онлайн образование; в здравоохранение – благодаря медицинской платформе возможно оперативно получить медицинскую помощь, а в недалеком будущем появится возможность самостоятельно поддерживать и сохранять свое здоровье; в экономику – большая часть населения страны управляет финансами с помощью чат-ботов; роботы дают консультации человеку по инвестициям; приложения банков и цифровые кошельки позволяют в считанные секунды осуществлять денежные операции и т. д.; в повседневность – помимо коммуникации и мгновенного поиска информации, всемирная сеть облегчает быт с помощью смарт-техники, позволяет на единой платформе купить билеты на любой транспорт, а также заказать такси и доставку еды; и др. Тем самым интернет стал для человека повседневным атрибутом жизнедеятельности.

В этой связи, данная проблематика вызвала интерес у ученых, которые сформулировали определенные мнения и позиции. М. Ю. Середой обращено внимание на возможности человечества реализовать любое конституционное право человека [8, с. 45]. По мнению Н. В. Виноградовой, в информационной среде возрастает роль всех прав человека, существование которых происходит в информационной среде, иными словами, они трансформируются в информационные права [3, с. 7]. А. В. Туликов отмечает, что в условиях развития сети Интернет и цифровой-среды формируется новая группа прав человека – это цифровые права, ценность которых выражена как свободой, так и информационной безопасностью [10, с. 9].

Следует согласиться с мнение последнего ученого, поскольку соотношение ценностей информационной свободы и безопасности в современном обществе не соответствуют балансу их правовой охраны, о чем свидетельствует опрос, проведенный «ВЦИОМ-Спутник», согласно которому в 2023 г. по сравнению с 2008 г. ценность информационной безопасности повысилась по отношению к ценности информационной свободы. Это выразилось в том, что в 2023 г. более 63 % опрошенных выступали за ограничение свободы выражения мнения в сети Интернет, тогда как в 2008 г. их было 58%

[1], и это при учете того, что государственная цензура прямо запрещена Конституцией Российской Федерации. Позиция граждан не представляется удивительной, поскольку современное общество всерьез обеспокоено защитой своих естественных прав.

Подтверждением угрозы информационной безопасности являются статистические данные, представленные на официальном сайте Генеральной Прокуратуры РФ, утверждающие, что за 2023 г. выросло на 39,3 % число преступлений, совершенных с использованием сети Интернет и интернет-технологий [7]. Также «Лаборатория Касперского» опубликовала на своем сайте неутешительные статистические данные: в 2023 г. зафиксировано увеличение объема «слитых» персональных данных сети Интернет более чем на 72 %, что составило 705 млн записей [9].

Представленные статистические данные демонстрируют высокий уровень опасности преступлений в сфере компьютерной информации для всех прав пользователей компьютерных технологий, в частности естественных прав человека.

Вместе с тем большинство граждан не осознают в полной мере своей значимости в обеспечении информационной безопасности своих естественных прав. Причиной тому являются: потеря бдительности, информационный патернализм, правовой нигилизм, низкая правовая, компьютерная грамотность и аномия. Так, по данным МВД Росии за 2023 г. на втором месте идут преступления, совершенные с использованием средств, принадлежащие жертве преступления (мобильные телефоны, пластиковые карты и др.). При этом важно отметить, что 81,2 % опрошенных пользователей сети Интернет уверены в ненадобности изучения новой информации о безопасном поведении в сети Интернет, а также способах защиты [4] своих естественных прав.

Предполагается, что такая уверенность у граждан сформировалась в связи с тем, что на международном и национальном уровне, как ранее было указано, гарантируется информационная защита, которая обеспечивает их осуществление и защиту. Тем самым человек самоустранился, возложив ответственность за свою информационную безопасность на государство. Представляется, что отрицание возможности человеком самостоятельно обеспечивать защиту ценностей информационной свободы и безопасности, выступает противоречием с автономией личностью. Одной из составляющей автономности личности является его самозащита, для реализации которой имеются правила, различные программы и технические средства, позволяющие человеку самостоятельно обеспечить личную информационную безопасность своих естественных прав.

В этой связи следует согласиться с мнением Мухаметзянова И. Ш., что на сегодняшний день самым эффективным способом обеспечения информационной безопасности является самосовершенствование уровня знаний и умений в области обеспечения собственной безопасности [6]. Действительно, проводя анализ преступлений в сфере IT-технологий с использованием интернета и IT-связи выявлено, что жертвы этих преступлений не в полной мере обезопасили себя от опасности. Например, сообщили третьим лицам код подтверждения учетной записи от банка или Госуслуг; не уведомили банк о неактуальности абонентского номера в их базах данных; перевели средства по просьбам незнакомых или знакомых лиц, не убедившись в достоверности информации, которая чаще всего поступает через сообщения в мессенджеры (Ватсап, Вайбер, Телеграмм и др.) и т. д. Тем самым личности, теряя бдительность и совершая необдуманные действия, компрометируют себя и подвергают опасности все свои права [2].

Именно поэтому для защиты своих естественных прав и обеспечения личной информационной безопасности личности необходимо:

– использовать надежные пароли и регулярно менять на новые, ранее не использованные;

– регулярно обновлять программное обеспечение на устройствах;

– с особой осторожность открывать электронные письма от неизвестных адресатов или с подозрительными вложениями;

– изучать основы информационной безопасности;

– знать законодательство в области информационной безопасности личности и т. д.

Данные меры позволят защитить права личности в сфере обработки и хранения персональных данных и тем самым обеспечить собственную информационную безопасность.

Таким образом, интернет оказывает значительное влияние на всю систему прав человека, в частности на естественные права. Основной задачей современного периода является понимание этого влияние с учетом всех факторов, способных привести к нарушению естественных прав человека. Конечно, решение данной задачи невозможно без государства, однако первостепенная роль отводится непосредственно самому пользователю сети Интернет в обеспечении личной информационной безопасности. Поскольку без соблюдения человеком элементарных мер по обеспечению информационной безопасности своих прав, в том числе естественных, принимаемые меры государства против информационных угроз окажутся бессильны.

Список литературы:

1. Аналитический отчет по результатам социологического исследования «Уровень социально-психологической напряженности в сети интернет и способы (приемы) защиты, выбираемые подростками». URL: https://docs.yandex.ru/ (дата обращения: 01.03.2024).

2. *Баранов В. В.* Информационная безопасность: сущностные характеристики Законы России: опыт, анализ, практика. 2007. № 8.

3. *Виноградова Н. В.* Правовой механизм защиты информационных прав и свобод человека и гражданина в Российской Федерации: дис. ... канд. юрид. наук: 12.00.01. Саратов, 2011.

4. *Гончаров И. В.* Новые векторы в развитии естественных прав человека. 2019. № 6 (74).

5. Информационная безопасность или информационная свобода? URL: /https://ok.wciom.ru/research/vciom-sputnik (дата обращения: 01.03.2024).

6. *Мухаметзянов И. Ш.* Саморазвитие информационной грамотности учащегося как основы информационной безопасности личности в рамках внеурочной деятельности: сборник статей по материалам международной научно-практической конференции, посвященной 120-летию со дня рождения А. Н. Колмогорова. Хабаровск: Тихоокеанский государственный университет, 2023.

7. Показатели преступности в России // Генеральная Прокуратура Российской Федерации. Портал правовой статистики: сайт. URL: https://epp.genproc.gov.ru/web/gprf/activity/statistics (дата обращения: 01.03.2024).

8. *Середа М. Ю.* Закрепление права на доступ в сеть Интернет в международно-правовых актах и законодательстве зарубежных стран // Международное публичное и частное право. 2013. № 5.

9. Статистика кибергугроз от «Лаборатории Касперского». URL: https: //www.kaspersky.ru/ (дата обращения: 01.03.2024).

10. *Туликов А. В.* Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): дис. ... канд. юрид. наук. Москва, 2017.

Станислав Григорьевич Семенцов,
кандидат технических наук,
доцент кафедры конструирования и технологии
производства электронной аппаратуры
Московский Государственный Технический
университет имени Н. Э. Баумана
E-mail: siemens_off@mail.ru

М. Хмиди Алхамада,
E-mail: am19ua001@student.bmstu.ru

УДК 534.843.5, 534.843.2, 681.534, 681.84.087

Использование метода изображений для расчета импульсной характеристики помещений прямоугольной формы

Аннотация

Эта статья сосредоточена на методе изображения, предложенном Алленом и Беркли в 1979 г. Метод изображения, вероятно, является одним из наиболее распространенных методов в сообществе обработки акустических сигналов и, следовательно, будет рассмотрен более подробно. Была создана наша функция, которая может использоваться в MATLAB для генерации многоканальных импульсных характеристик помещения с использованием метода изображения. Эта функция позволяет пользователю контролировать порядок отражения, размер помещения и направленность микрофона.

Ключевые слова и словосочетания: *метод изображения; уравнение Гельмгольца; импульсные отклики комнаты (ИОК); сети прямого распространения; корреляционная.*

В этой статье дается краткий обзор различных методов, которые могут быть использованы для симуляции акустики комнаты. Метод изображений [1], предложенный Алленом и Беркли в 1979 г., вероятно, является одним из наиболее распространенных методов в среде обработки акустических сигналов. Этот метод тесно связан с так называемым уравнением волн и его частотным эквивалентом, называемым уравнением Гельмгольца. Для генерации импульсные отклики комнаты (ИОК) с использованием метода изображений была создана наша функция, которую можно использовать

в MATLAB. Эта функция позволяет пользователю контролировать порядок отражения, размеры комнаты и направленность микрофона. Еще одним преимуществом этой функции по сравнению со стандартной функцией MATLAB является время вычисления. Мы обнаружили, что наша функция работает примерно в 100 раз быстрее стандартного кода MATLAB на нашем тестовом компьютере.

Волновое уравнение

В принципе, любое сложное звуковое поле можно рассматривать как суперпозицию множества простых звуковых волн (например, плоских волн), и их распространение в помещении можно считать линейным, если предположить, что свойства среды, в которой распространяются волны, однородны, находятся в состоянии покоя и не зависят от амплитуды волны [6]. В физике волновое уравнение описывает распространение волн в жидкостях (газе или жидкости).

Волновое уравнение:

$$\nabla^2 p(r,t) - \frac{1}{c^2}\frac{\partial . p(x,t)}{\partial t^2} = 0, \quad (1)$$

где

$$\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \quad (2)$$

Это лапласиан, выраженный в декартовых координатах (x; y; z), а c – скорость звука. Волновое уравнение точно описывает давление в звуковом поле при условии $|p(r,t)| \ll \rho_0 c^2$, где ρ_0 – плотность среды распространения в равновесном состоянии.

На практике в среде возникают неоднородности двух типов: 1) скалярные неоднородности и 2) векторные неоднородности. Чтобы рассчитать звуковое поле, исходящее от источника в конкретной комнате, нам нужна дополнительная функция источника в (1) и граничные условия, описывающие отражение и поглощение звука стенами. Пусть s (r; t) обозначает исходную функцию, тогда волновое уравнение задается формулой:

$$\nabla^2 p(r,t) - \frac{1}{c^2}\frac{\partial . p(x,t)}{\partial t^2} = -s(r,t) \quad (3)$$

Уравнение Гельмгольца

Уравнение Гельмгольца является дифференциальным уравнением вида:

$$\nabla^2 \psi + k^2 \psi = 0,$$

где ψ – неизвестная функция, ∇2 – оператор Лапласа, k – волновое число (или волновое число, соответствующее заданной частоте).

Уравнение Гельмгольца часто возникает в физических задачах, описывающих распространение волн, таких как звуковые, световые или электромагнитные. Решение этого уравнения позволяет определить форму и распределение этих волн в пространстве.

Давайте рассмотрим волновое уравнение в частотной области. Преобразование Фурье определяется как:

$$P\,(r;\,\omega) \triangleq F\{p(r,t)\}(\omega) = \int_{-\infty}^{+\infty} p(r,t)\,.\exp(i\omega t)\,dt, \qquad (4)$$

где $\exp(x) = e^x$, $i = \sqrt{-1}$. Применяя преобразование Фурье к (1), получаем зависящее от времени уравнение Гельмгольца:

$$\nabla^2 p(r,\omega) + k^2 p(r,\omega) = 0, \qquad (5)$$

где k обозначает волновое число, связанное с угловой частотой, и длина волны выражается через:

$$k = \frac{\omega}{\lambda} = \frac{2\pi}{\lambda}$$

Если существует гармоническое возмущение, которое порождает волны, для которых функция источника задается через $s(r,t) = S(r,\omega)e^{-j\omega t}$, то уравнение Гельмгольца задается через:

$$\nabla^2 p(r,\omega) + k^2 p(r,\omega) = -S(r,\omega) \qquad (6)$$

Оно может быть решено путем предварительного решения следующего неоднородного уравнения:

$$\nabla^2 H(r,\, r_s;\, \omega) + k^2\, H(r, r_s;\, \omega) = -\delta(r - r_s), \qquad (7)$$

где $H(r,\, r_s;\, \omega)$ – передаточная функция помещения (ПФП).

$$P(r,\omega) = \iiint_{v_s} H(r, r_s\,; \omega) S(r_s; \omega) dr_s, \qquad (8)$$

где Vs обозначает исходный объем, а $dr_s = dx_s\, dy_s\, dz_s$ – элемент дифференциального объема в позиции r_s. Звуковое давление P(r,t) теперь может быть получено с помощью обратного преобразования Фурье из (8).

Удовлетворяющая однородному уравнению $(\nabla^2 + k^2)\psi m(r;\omega) = 0$ на определенном интервале и удовлетворяющая определенным гра-

ничным условиям в конце интервала называется собственной функцией. Впоследствии, используя собственные функции, можно получить общее выражение для Зеленой функции H(r; ω) в произвольном звуковом поле:

$$H(r, r_s; \omega) = \sum_{m=0}^{\infty} C(r_s; \omega)\, \psi m(r; \omega), \tag{9}$$

где каждый коэффициент $C(r_s; \omega)$ зависит от положения источника звука. Собственные функции зависят от граничных условий, налагаемых замкнутым пространством.

Классическая прямоугольная комната

В прямоугольной комнате с физическими размерами (Lx; Ly; Lz) и жесткими идеально повторяющимися стенами собственные функции в декартовых координатах равны [6].

$$\psi_m(r) = cos\left(\frac{m_x \pi\, x}{l_x}\right) cos\left(\frac{m_y \pi\, y}{l_y}\right) cos\left(\frac{m_z \pi\, z}{l_z}\right), \tag{10}$$

где $m = \{m_x, m_y, m_z\}$ и $m_v \epsilon \{x, y, z\}$ являются неотрицательными целыми числами.

Давайте определим $k_v = \frac{m_v \pi}{l_v} : v \epsilon \{x, y, z\}$, тогда мы можем записать (10) как:

$$\psi_m(r) = \cos(k_x x)\cos(k_y y)cos(k_z z) \tag{11}$$

Соответствующие собственные значения равны: $k_m^2 = k_x^2 + k_y^2 + k_z^2$ Решением неоднородного уравнения (7) для классической прямоугольной комнаты является [6]:

$$H(r, r_s; \omega) = \sum_{m \in M} \frac{\psi_m(\mathrm{r})\psi_m^*(\mathrm{r})}{\Lambda_m(k^2 - k_m^2)}, \tag{12}$$

где Λm – константа нормализации для соответствующего собственного вектора, определяемая.

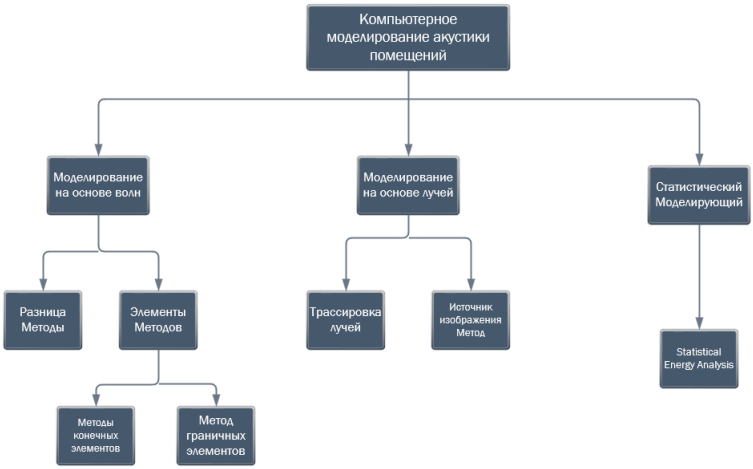

Рис. 1. Акустические модели помещений основаны на звуковых лучах (лучевой), на решении волнового уравнения (волновой) или каком-либо статистическом методе [10]

$$\iiint_v \psi_m(\mathrm{r})\psi_m^*(\mathrm{r})dr = \begin{cases} \Lambda_m, & m = n \\ 0, & \text{иначе} \end{cases} \tag{13}$$

Уравнение (13) раскрывает структуру Передаточная функция помещения. В этом случае $k_m = \frac{\omega_m}{c} + i\frac{\delta_m}{c}$, где δ_m обозначает постоянную затухания (добротность). Предполагая, что $\delta_m \ll \omega_m$, (13), приводим к виду:

$$H(r, r_s; \omega) = c^2 \sum_{m\in M} \frac{\psi_m(\mathrm{r})\psi_m^*(\mathrm{r_s})}{\Lambda_m(\omega^2 - \omega_m^2 - 2i\delta_m\omega_m)} \tag{14}$$

Обратное преобразование Фурье частотной характеристики помещения, описанной в (13), приводит к комнатной импульсной характеристики = h(r; t). Форма (13) оправдывает использование некоторых хорошо известных методов моделирования, используемых при обработке сигналов, например, модели «полюс-ноль».

Имитация акустики помещения

Математически распространение звука описывается волновым уравнением. Импульсная характеристика от источника к микрофону может быть получена путем решения волнового уравнения.

Поскольку это редко может быть выражено в аналитической форме, решение должно быть аппроксимировано. Существует три основных метода моделирования, как показано на рис. 1, а именно: волновой, лучевой и статистический [10]. Методы, основанные на лучах, такие как трассировка лучей [5] и метод источника изображения [1], являются наиболее часто используемыми. Методы, основанные на волнах, такие как метод конечных элементов (МКЭ), метод граничных элементов (МГЭ) [3; 9] и методы конечных разностей во временной области (КРВО) [2], являются более требовательными к вычислениям.

Лучевые методы

Лучевые методы основаны на геометрической акустике помещения [6]. Наиболее часто используемыми методами, основанными на лучах, являются трассировка лучей [5] и метод изображений [1]. Основное различие между этими методами заключается в способе расчета траекторий воздействия [10]. Чтобы смоделировать идеальную импульсную характеристику от источника к приемнику, необходимо обнаружить все возможные пути отражения звука, обычно называемые лучами.

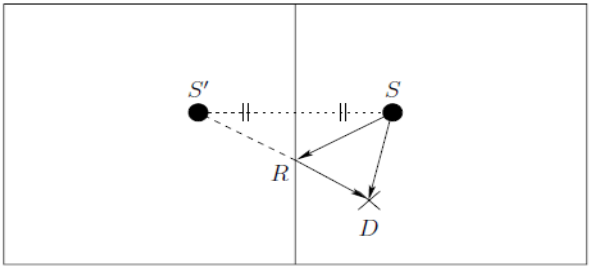

Рис. 2. Траектория, включающая одно сечение, полученное с использованием одного изображения

В методах трассировки лучей мощность звука, излучаемого источником звука, описывается конечным числом лучей. Эти лучи распространяются в пространстве и отражаются после каждого столкновения с границами помещения. Следует отметить, что все лучевые методы основаны на распространении энергии. Это означает, что всеми эффектами, связанными с разницей фаз, такими как преломление или интерференция, пренебрегают. Тогда можно предположить, что конструктивный и деструктивный фазовые эффекты компенсируют друг друга, когда две или более составляющих звуко-

вого поля накладываются в одной точке, и общая энергия в рассматриваемой точке просто получается путем сложения их энергий [4].

Метод изображения Аллена и Беркли

Рассмотрим прямоугольную комнату с длиной, шириной и высотой, заданными Lx, Ly и Lz. Пусть источник звука находится в местоположении, представленном вектором rs = [x_s; y_s; z_s], а микрофон – в местоположении, представленном вектором r = [x; y; z]. Оба вектора направлены относительно начала координат, которое находится в одном из углов комнаты. Относительные положения изображений, измеренных относительно положения приемника и полученных с использованием стенок при x = 0, y = 0 и z = 0, могут быть записаны в виде:

$$R_p = [(1-2q)x_s - x, (1-2j)y_s - y, (1-2k)z_s - z] \qquad (15)$$

Каждый из элементов в тройке p = (q; j; k) может принимать значения 0 или 1, в результате чего получается восемь различных комбинаций, которые задают множество P: $P = \{(q,j,k): q,j,k \epsilon \{0,1\}\}$. Когда значение p равно 1 в любом измерении, то рассматривается изображение источника в этом направлении. Следует отметить, что некоторые из этих изображений соответствуют отражениям более высокого порядка. Чтобы рассмотреть все изображения, мы добавляем вектор R_m к R_p, где

$$R_m = [2m_x L_x, 2m_y L_y, 2m_z L_z], \qquad (16)$$

где mx, my и mz – целочисленные значения. Каждый из элементов тройки m = (m_x; m_y; m_z) принимает значения от -N до +N. Порядок отражения, относящийся к изображению в положении Rp + Rm + r, задается формулой:

$$O_{p,m} = |2m_x - q| + |2m_y - j| + |2m_z - k| \qquad (17)$$

Расстояние между любым исходным изображением и микрофоном можно записать в виде:

$$\tau = \frac{d}{c} - \frac{\|R_p + R_m\|}{c}, \qquad (18)$$

где c обозначает скорость звука в метрах в секунду.

$$h(r,rs,t) = \sum_{p\in P}\sum_{m\in M} \beta_{x1}^{|m_x-q|}\beta_{x1}^{|m_x|}\beta_{y1}^{|m_y-j|}\beta_{y2}^{|m_y|}\beta_{z1}^{|m_z-k|}\beta_{z2}^{|m_z|}\frac{\delta(t-\tau)}{4\pi d} \qquad (19)$$

$$h(r,rs,t) = \sum_{p\in P}\sum_{m\in M}\beta_{x1}^{|m_x-q|}\beta_{x1}^{|m_x|}\beta_{y1}^{|m_y-j|}\beta_{y2}^{|m_y|}\beta_{z1}^{|m_z-k|}\beta_{z2}^{|m_z|}\frac{LPF\{\delta(n-\tau f_s)\}}{4\pi d}, \quad (20)$$

где f_s – частота дискретизации, а LPF{.} обозначает теоретически идеальный фильтр нижних частот с частотой среза $f_s/2$. В [1] время прибытия (в выборках) было сдвинуто до ближайшего целого значения. Следовательно, было сделано следующее приближение:

$$LPF\{\delta(n-\tau f_s)\} \approx \delta(n - round\{\tau f_s\}) \quad (21)$$

Хотя во многих приложениях этим искажением можно пренебречь. Один из способов уменьшить эту проблему – вычислить дискретную импульсную характеристику при гораздо более высокой частоте дискретизации, уменьшить импульсную характеристику до исходной частоты дискретизации и свернуть с ней исходный сигнал. Петерсон предложил другую модификацию метода изображений [7]. При таком подходе каждый импульс в (18) заменяется импульсной характеристикой идеального фильтра нижних частот с окном:

$$\delta_{LPF}(t) = \begin{cases} 0.5\left(1+\cos\left(\frac{2\pi t}{T_\omega}\right)\right)\sin(2\pi f_c t), & -\frac{T_\omega}{2} < t < \frac{T_\omega}{2} \\ 0, & \text{иначе} \end{cases} \quad (22)$$

Другим фактором, учитываемым при моделировании реверберации в помещении, является продолжительность реверберации или время реверберации. Формально время реверберации определяется как время, необходимое для того, чтобы интенсивность отраженных звуковых лучей снизилась на 60 дБ по сравнению с прямым звуковым лучом. Эмпирическая формула, известная как формула Сабина-Франклина [8], может быть использована для определения времени реверберации RT60:

$$RT_{60} = \frac{24\ln(10)V}{c\sum_{i=1}^{6} S_i\left(1-\beta_i^2\right)} \quad (23)$$

Решение уравнения Гельмгольца для прямоугольной комнаты было приведено в (12). Давайте примем во внимание все изображения, определив $-\infty < m_v < \infty$ для м $\in \{x,y,z\}$. Расширяя косинусы собственных функций с помощью экспонент и используя тот факт, мы можем записать (12) в виде:

$$H(r,r_s,\omega) = \frac{1}{8V}\sum_{p\in P}\sum_{m\in M}\frac{\exp(iK_m.R_p)}{k^2-\|K_m\|^2}, \quad (24)$$

$$K_m = \left[\frac{m_x\pi}{L_x}, \frac{m_y\pi}{L_y}, \frac{m_z\pi}{L_z}\right] = [k_x, k_y, k_z] \quad (25)$$

Принимая во внимание коэффициенты отражения шести стенок, мы получаем также в эквиваленте (18):

$$h(r, rs, t) = \sum_{p\in P}\sum_{m\in M} \beta_{x1}^{|m_x-q|}\beta_{x1}^{|m_x|}\beta_{y1}^{|m_y-j|}\beta_{y2}^{|m_y|}\beta_{z1}^{|m_z-k|}\beta_{z2}^{|m_z|}\frac{\delta(t-\tau)}{4\pi d} \quad (26)$$

Результаты

Метод изображения, о котором говорилось в предыдущем разделе, был реализован как функция MATLAB и тестирован в помещении (длина 480 см, ширина 400 см, высота 270 см). Коэффициент отражения равен 0,4. Нам нужно определить, где находится устройство записи (микрофон) и источник сигнала (колонки). Допустим левый угол в помещении определится нулевой точкой для начала (X Y Z). Исходя из этого, мы можем дать координаты местоположения источника сигнала или человека, который слушает сигнал. Источник сигнала (колонки) находится на расстоянии 100 см, 100 см, 100 см, устройство записи (микрофон) – 2,4; 2; 1,35.

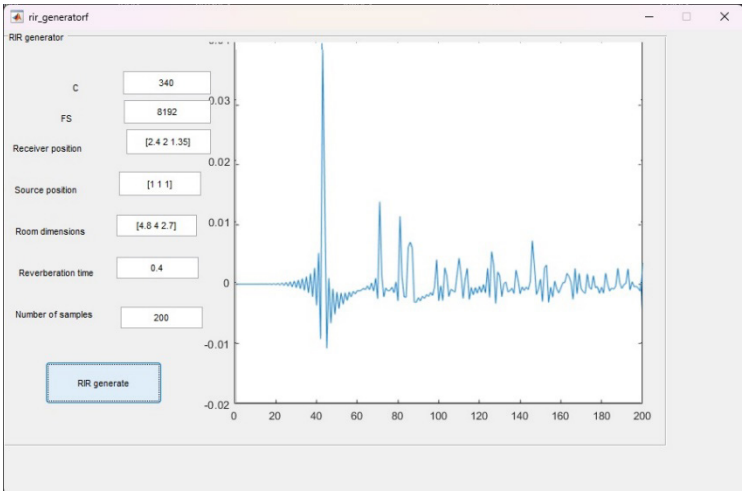

Рис. 3. Импульсный отклик помещения по изображению метода

Теперь вычислим суммарный отклик на входной сигнал X, который может быть шумом с равномерным распределением или звуком:

$$y(n) = \sum_{k=1}^{N} h(k)x(n-k) \quad (29)$$

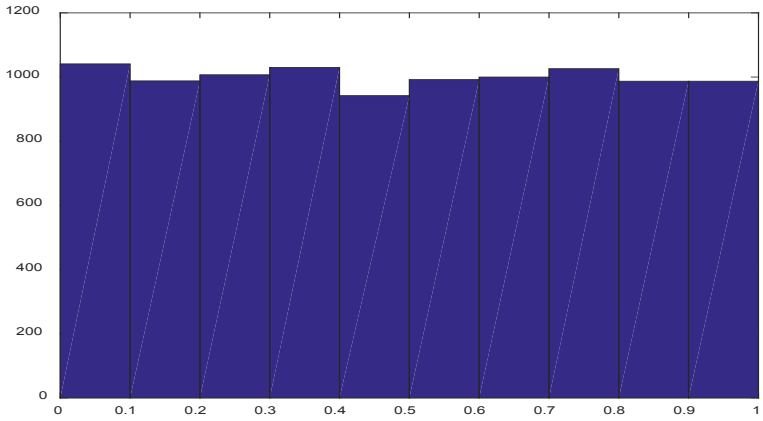

Рис. 4. Равномерное распределение сигнала до воздействия на него помещения

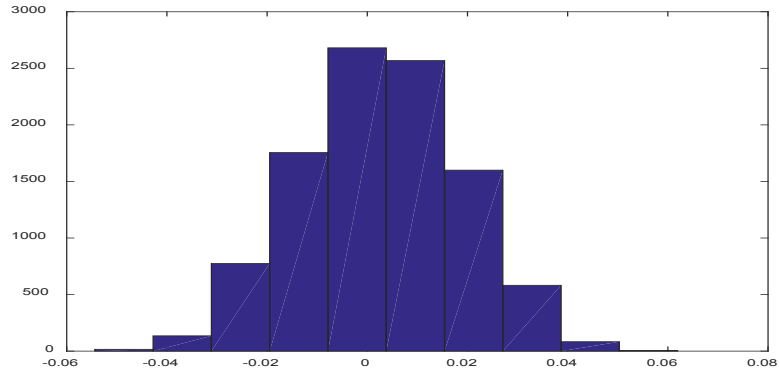

Рис. 5. Влияние помещения на распределение сигнала

Чтобы убедиться, что импульсная характеристика помещения, полученная методом изображения, правильна, мы посылали в комнату обычный белый шум, как показано на рисунке (4), и записывали диаграмму частотного распределения передаваемого сигнала. Сигнал зафиксирован после распространения в помещении (шумовой сигнал с влиянием на него помещения, показанный на рисунке (5)).

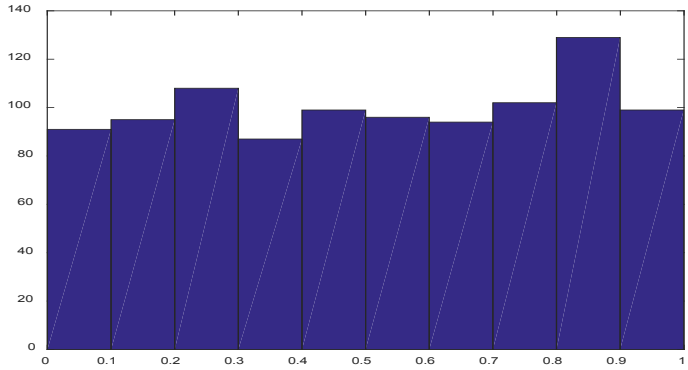

Рис. 6. Сигнал, генерируемый нейронной сетью

Для выполнения задачи по удалению эффекта помещения из записанного сигнала была сгенерирована нейронная сеть прямого распространения, после чего сравниваем полученный сигнал с переданным сигналом, следуя корреляции, и на основе результата определяем, что рекомендуемый ответ правильный или нет на рисунке (6,7).

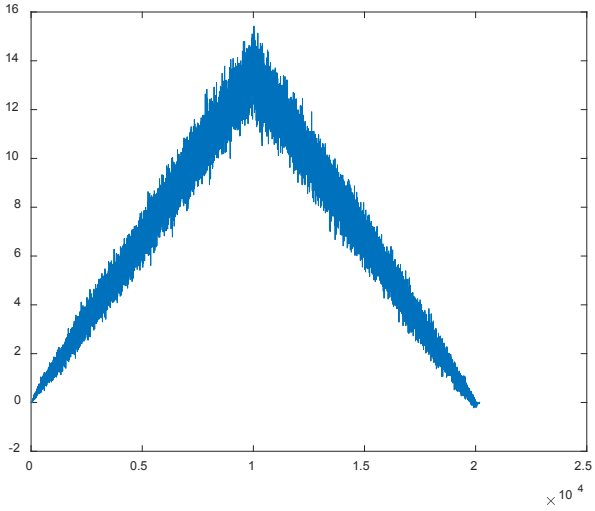

Рис. 7. Проследите корреляцию и выявите большую корреляцию между входом и выходом, которая указывает на большое сходство между ними

Заключение

Отметим, что визуальный метод обладает высокой точностью, но требует огромных вычислительных мощностей особенно при сложной форме помещения.

Следовательно, нам необходимо быстрее достичь импульсного отклика помещения менее сложным способом, чтобы снизить необходимую вычислительную мощность, сохраняя при этом достаточную точность.

Список литературы:

1. *Аллен Дж., Беркли Д.* Метод изображения для эффективного моделирования акустики небольших помещений // Журнал Американского акустического общества. 1979. № 4.
2. *Боттельдур Д.* Моделирование низкочастотных акустических задач в помещении с конечными разностями во временной области // Журнал Американского акустического общества. 1995. № 6.
3. *Кляйнер М., Даленбек Б., Свенссон П.* Аудиализация – обзор // Журнал Общества аудиотехники. 1993. № 11.
4. *Крокер М.* Справочник по акустике // Вили-Интерсайенс. 1998.
5. *Куковски А.* Алгоритмическое представление метода трассировки лучей // Прикладная акустика. 1985. № 6.
6. *Куттру Х.* Акустика помещений. Лондон, 2000.
7. *Петерсон П.* Имитация отклика нескольких микрофонов на один акустический источник в реверберационной комнате // Журнал Американского акустического общества. 1986. № 5
8. *Пирс А.* Акустика: введение в ее физические принципы и приложения // Американское акустическое общество. 1991.
9. *Пьетшик А.* Компьютерное моделирование звукового поля в небольших помещениях // Акустика и малые пространства. 1998.
10. *Савиоха Л. [и др.].* Создание интерактивных виртуальных акустических сред // Журнал Общества аудиоинженеров. 1999. № 9.

Надежда Алексеевна Солдатенкова,
научный сотрудник отдела систем связи
центра средств и систем связи
научно-исследовательского института
специальной техники
ФКУ НПО «СТиС» МВД России
E-mail: nsoldatenkova4@mvd.ru

УДК 004.451
2.2.15

Отечественные смартфоны: проблемы и пути решения

Аннотация

Актуальность исследования обозначена повсеместным распространением мобильных устройств (смартфонов), развитие которых на российском рынке претерпевает ряд проблемных вопросов. В статье рассмотрены причины, осложняющие внедрение смартфонов в деятельность органов внутренних дел Российской Федерации. Описаны подходы к решению проблем развития отечественных продуктов: операционных систем и мобильных устройств.

Ключевые слова и словосочетания: *смартфон; операционная система Аврора; радиоэлектронная промышленность; инновационный проект.*

Развитие инфокоммуникационных технологий и систем связи привело к повсеместному распространению мобильных устройств – смартфонов. Ключевые преимущества смартфонов заключаются в удобстве получения и самодостаточности при обработке информации различного рода. Таким образом, смартфоны фактически являются карманными компьютерами. Подавляющее большинство рынка современных смартфонов реализовано на операционных системах (далее – ОС) Android и IOS, принадлежащих американским компаниям Google и Apple. Развитие отечественного производства, в том числе в части радиоэлектронной промышленности, не стоит на месте, а уход с российского рынка западных компаний стимулирует спрос на российские инновационные решения [1; 5].

Одним из проектов, имеющих большой потенциал для стимулирования экономического роста и обеспечения технической суверенности государства, является разработка Российской мобильной

доверенной ОС Аврора (компания «Открытая мобильная платформа»). Как заявляют разработчики [2], ОС Аврора позволяет создавать и использовать доверенные решения, технологии защиты информации и коммуникаций для мобильных рабочих мест в компаниях и организациях. Использование ОС Аврора позволяет обезопасить чувствительные данные, так как они не собираются, не передаются на сторонние сервера. Поэтому целевой аудиторией пользователей ОС Аврора являются корпорации и государственные организации, в которых существуют высокие требования в обеспечении безопасности устройств сотрудников и внутренних данных. Например, «РЖД», «Почта России», МЧС России, органы внутренних дел Российской Федерации (далее – ОВД Российской Федерации) и т. д.

Гарантия полной безопасности устройств на базе отечественной ОС Аврора обеспечивается за счет единого центра управления, из которого дистанционным образом осуществляется контроль всех устройств корпоративного контура. ОС Аврора добавлена в реестр отечественного ПО и имеет несколько сертификатов безопасности [3]: ФСТЭК на мобильную ОС Аврора ФСТЭК А4, ФСТЭК на прикладное программное обеспечение «Аврора Центр» ФСТЭК по УД4, ФСТЭК на защищенную мобильную ОС общего назначения на базе Sailfish Mobile OS RUS ФСТЭК по А6.

Для сотрудников ОВД Российской Федерации отечественные мобильные устройства, работающие в единой закрытой системе, – решение, благодаря которому рутинные внутренние задачи могут быть упрощены, а в экстренной ситуации значительно ускорен процесс передачи и обработки информации. Тем не менее вопрос принятия на снабжение ОВД Российской Федерации средств мобильной связи на базе ОС Аврора осложняется рядом барьеров. Первым из них является отсутствие профессиональных приложений. Разработанные для ОС Аврора приложения являются базовыми (будильник, калькулятор, инструменты воспроизведения мультимедийных файлов и т. д.) и не покрывают все нужды сотрудников ОВД Российской Федерации. Большинство разработчиков создают приложения для ОС Android и iOS, так как эти платформы имеют мировую аудиторию и обширные рынки [4]. Отсутствие массового пользователя, высокие требования по обеспечению безопасности – факторы, осложняющие разработчикам приложений получение прибыли, а значит снижающие рентабельность.

Вторая причина, тесно связанная с возникновением первой, заключается в дефиците самих разработчиков ОС Аврора. Начинающий специалист мобильной разработки заинтересован в полу-

чении квалификации, которая будет востребована на всемирном рынке труда, в развитом профессиональном сообществе. Его не привлекает разработка приложений для узкой аудитории в системе, которая совместима с несколькими устройствами. Кроме того, ОС Аврора долгое время разрабатывалась в закрытом режиме, что значительно сокращает количество компетентных разработчиков.

Первая и вторая указанные причины, по сути, составляют замкнутый круг: пользователи не могут эксплуатировать мобильные устройства на базе ОС Аврора в полном объеме, так как отсутствуют специальные приложения, а разработчики не готовы их создавать, по причине ограниченного количества пользователей.

Одним из путей решения описанных барьеров является формирование собственной инженерной школы разработчиков ОС Аврора. Компания «Открытая мобильная платформа» предлагает провести бета-тестирования ОС Аврора. Программа, нацеленная на интенсивное использование софта, позволит познакомиться с новыми продуктами компании, провести собственное пользовательское тестирование и даже принять участие в разработке ОС Аврора. Пользователям предоставляется во временное пользование мобильное устройство с новой версией ОС Аврора и набором предустановленных приложений. В свою очередь, пользователь должен отправлять отзывы, по анализу которых разработчики идентифицируют проблемы с производительностью и прочими недостатками, собирают сведения о повышении удобства пользования и др. В рамках данной программы предусмотрено привлечение разработчиков к созданию приложений, а также обмен опытом с другими разработчиками. Таким образом, компания «Открытая мобильная платформа» планирует создать пласт разработчиков, ориентированных на конкретные задачи для ОС Аврора.

Что касается самих мобильных устройств, на которые ОС Аврора может быть установлена, то отечественный рынок состоит из 13 продуктов, в состав которых входят: планшетные компьютеры, смартфоны и карманные персональные компьютеры. Только четыре из этих устройств имеют защищенное исполнение корпуса. При этом мировой рынок брендов гаджетов насчитывает тысячи различных моделей, совместимых с популярными ОС Android и iOS. Другими словами, кроме развития самой российской ОС, существует потребность и в развитии отечественных мобильных устройств. Повышение популярности российской продукции у пользователей будет являться стимулом производить большее количество модификаций смартфонов. Таким образом, появится возможность расширения аудитории пользователей.

Министерство внутренних дел Российской Федерации как один из сегментов целевой аудитории ОС Аврора заинтересовано в разработке качественной, функциональной и безопасной системы, поэтому в подразделениях министерства также проводятся мероприятия по апробации отечественных мобильных устройств с целью изучения технических характеристик и оценки возможности их дальнейшего внедрения в деятельность ОВД Российской Федерации.

Таким образом, неоспоримым преимуществом ОС Аврора перед другими ОС является конфиденциальность данных и контроль системы единым центром управления. Существующий ряд барьеров возможно преодолеть при условии поддержки разработчиков целевой аудиторией и воспитанием собственной инженерной школы.

Список литературы:

1. *Азаров М. С., Махашевич Д. В.* Отечественное программное обеспечение как фактор цифрового суверенитета Российской Федерации. Москва: Вестник Российской правовой Академии, 2021.

2. Официальный сайт компании «Открытая мобильная платформа». URL: https://www.omp.ru/os-aurora/ (дата обращения: 16.03.2024).

3. Официальный сайт компании «Открытая мобильная платформа». URL: https://www.omp.ru/certificates/(дата обращения: 16.03.2024).

4. *Резванова А. Ю.* Краткий обзор российского рынка смартфонов. Петрозаводск: Сборник статей Международной научно-практической конференции, 2023. С. 34-38.

5. *Соколова Ю. А., Морева И. В., Егоров Г. И.* Научно-технический прогресс в радиоэлектронной промышленности как фактор экономического роста и развития Республики Татарстан // Инновации и инвестиции. 2023. № 4.

Вадим Алексеевич Степанов,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: stepanov13@mail.ru

УДК 349.422.234.6

Информационные технологии при решении отдельных проблем в организации и планировании служебной деятельности следователей

Аннотация

Любая деятельность требует организации, что является непременным условием эффективности решения стоящих задач. Служебная деятельность следователя подразумевает реализацию множественных функций и представлена значительным числом элементов, в связи с чем ее организация имеет важнейшее значение для оптимального решения оперативно-служебных задач. В данной статье раскрыты некоторые проблемы планирования деятельности следователей, снижающие ее эффективность, и разработаны рекомендации по их разрешению.

Ключевые слова и словосочетания: *деятельность следователей; организация деятельности следователя; планирование деятельности; контроль за деятельностью следователей; информационные технологии.*

Организация работы следователя в обязательном порядке предполагает планирование своей служебной деятельности [6]. Ему присуще несколько функций, среди которых упорядочивание работы следователей по конкретному уголовному делу и по всем уголовным делам, находящимся в его производстве; обеспечение возможности контроля за деятельностью следователей.

Нужно отметить, что нет единого подхода к решению вопроса о соотношении таких понятий, как планирование деятельности следователя и организация деятельности следователя. В частности, рядом исследователей отмечается, что понятие организации входит в понятие планирования деятельности, которое включает в себя все организационные мероприятия. Таким образом, понятие планирования более широко, чем понятие организации; последнее образует собой структурный элемент планирования следственной деятельности.

Другими исследователями отстаивается позиция о том, что, напротив, понятие организации расследования более широко и включает в себя планирование в качестве одного из структурных элементов, в основном – в качестве средства организации следственной деятельности либо в качестве ее метода. Третьи не проводят анализа соотношения данных понятий, определяя их как самостоятельные отдельные процессы и отмечая лишь их взаимосвязанность и взаимообусловленность, так как невозможно эффективно организовать деятельность следователя без ее планирования, а планирование в обязательном порядке включает в себя организационные мероприятия, т. е. невозможно без организации следственной деятельности [1].

С нашей точки зрения, наиболее верной является позиция о том, что планирование – это элемент организации работы следователя, поскольку планирование, несомненно, является мыслительной деятельностью, не способной обеспечить организованность, для которой требуется наличие деятельностного аспекта – реализации запланированных мероприятий и действий [3].

Наиболее часто понятие планирования применительно к деятельности следователя рассматривают как планирование расследования уголовных дел. Разработаны различные формы планирования, в частности – план по каждому уголовному делу, содержащий перечень необходимых следственных действий и их мероприятий, сроки их проведения, а также календарный план, предусматривающий планирование работы по всем уголовным делам, находящимся в производстве. Сочетание этих планов позволяет не допускать волокиты при расследовании, исключать ситуации, когда активная деятельность осуществляется только по какому-либо одному уголовному делу, в то время как остальные остаются без движения. Наличие таких планов обеспечивает и возможность контроля за деятельностью следователей со стороны руководителей [5].

В то же время необходимо отметить значимые проблемы, связанные с планированием деятельности следователя. Прежде всего анализ уголовных дел и анкетирование сотрудников следственных подразделений позволяет сделать вывод о том, что в большинстве случаев подход к планированию формальный. Разработанные шаблоны планов заполняются в первые дни после возбуждения уголовного дела, при этом намеченные сроки не соблюдаются, корректировки по мере продвижения расследования, получения новой информации, установления отдельных обстоятельств не вносятся [4]. Фактически планы наличествуют для того, чтобы предъявить их руководителю для осуществления контроля, а также в ходе про-

верок сотрудникам организационно-зональных или контрольно-методических отделов.

Способствует в определенной мере формальному подходу к планированию деятельности недостаточно эффективный контроль со стороны руководителя следственного органа. Как свидетельствует практика, промежуточная проверка уголовных дел на предмет исполнения намеченных мероприятий практически не осуществляется, устанавливается лишь наличие планов. Соответственно, о сложностях, возникающих в ходе производства по уголовному делу, руководителю следственного органа становится известно только когда истекает срок расследования и необходимо его продлить. Очевидно, что в случае надлежащего контроля и своевременного выявления возникающих трудностей во многих случаях удалось бы избежать необходимости продления срока предварительного следствия и нарушения принципа разумного срока уголовного судопроизводства.

Следующая проблема, которую хотелось бы отметить в свете анализа организации деятельности следователя – планирование его работы по своему содержанию существенно шире, чем планирование расследования. В графике должно быть учтено не только производство следственных действий, но и время на проводимые совещания, посещение занятий по служебной подготовке, самоподготовку. Однако зачастую эти аспекты не учитываются, что может приводить к срыву следственных действий или игнорированию следователями занятий в рамках служебной подготовки. Нередко она проводится формально, что выражается в наличии в служебных тетрадях записей по теме, когда фактически она не изучается. Это негативно влияет на профессионализм сотрудника, не позволяет ему развиваться как следователю [2]. Самоподготовкой, как свидетельствует проведенное анкетирование, занимаются единицы (20 % респондентов), что объясняется преимуществом высокой нагрузкой по уголовным делам и отсутствием свободного времени.

В то же время прослеживается закономерность, что нередко волокита по уголовным делам допускается теми следователями, которые не могут грамотно организовать свое время. Возникают накладки в связи с тем, что на одно время вызываются одновременно участники некоторых следственных действий, своевременно не направляются необходимые запросы и т. д. Эти проблемы – результат ненадлежащего отношения к планированию расследования и организации своей служебной деятельности. В некоторых случаях, при наличии формальных планов следователи составляют для себя так называемые рабочие, черновые планы – на отдельных

листках, в ежедневниках, это в определенной мере позволяет организовать работу, но не дает возможности осуществлять контроль со стороны руководителя. Есть примеры, когда даже такие планы сотрудники следственных подразделений не составляют, удерживая запланированные мероприятия и их сроки в памяти.

Полагаем, что все рассмотренные проблемы требуют комплексного подхода к их решению. Планирование работы следователя – необходимое условие эффективной организации его деятельности в том случае, когда оно осуществляется с учетом реальных потребностей, включает в себя корректировку планов и контроль за их исполнением. Представляется, что обеспечить решение таких задач возможно с помощью информационных технологий. Необходимо разработать и внедрить в практику органов расследования соответствующие программы, предоставляющие следователю возможность составления в них планов различных форм и осуществляющие проверку корректности этих планов.

Например, в случае обнаружения пересечения следственных действий по разным уголовным делам, запланированных в рамках плана по конкретному делу и календарного плана, программа должна демонстрировать ошибку и запрашивать корректировку. Аналогичным образом должна обеспечиваться реакция программы на отсутствие внесения отметок или изменений в планы более двух суток. К этой же программе должен быть обеспечен доступ руководителя следственного органа с целью осуществления контроля за деятельностью следователя, это позволит, например, при наличии в плане отметки об исполнении его определенного пункта (например, проведении следственного действия) и истребовании уголовного дела для проверки убедиться в соблюдении плана или внесении в него недостоверных данных.

Кроме того, имея возможность удаленного доступа к плану по каждому уголовному делу, руководитель следственного органа может заранее выявлять факты, свидетельствующие о затруднениях окончания производства по делу в установленные сроки, требовать корректировки плана, активизации расследования, давать указания, подлежащие обязательному исполнению.

Аналогичным образом руководитель следственного органа может контролировать самоподготовку следователей, требуя отражения ее в календарном плане с указанием темы или отдельных нормативных правовых актов, разъяснений высшей судебной инстанции, которые планирует самостоятельно изучить следователь, проверяя в последствии приобретенные знания.

Таким образом, служебная деятельность следователя может быть эффективной только при должной ее организации. Одним из важнейших ее элементов выступает планирование и использование информационных технологий. Необходимо исключить формальный подход к нему, повысить контроль со стороны руководителей следственных органов за составлением планов и их выполнением. Обеспечить это можно путем внедрения соответствующих программ с функционалом, позволяющим автоматически анализировать составленные следователями планы, отслеживать внесение в них отметок, а также иметь доступ к этим планам руководителю следственного органа со своего рабочего места. Считаем, что своевременный контроль за планированием деятельности следователя и возможность его дистанционного корректирования с использованием современных информационных технологий обеспечит и более эффективное решение следственными подразделениями стоящих перед ними задач.

Список литературы:

1. *Асланалиев С. М.* Планирование как элемент организации расследования преступлений // Научное знание современности. 2022. № 9 (69).

2. *Волохова О. В.* Тайм-менеджмент в следственной деятельности // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 3 (55).

3. *Лобунец Е. С.* Планирование в деятельности следователя: сборник научных статей по итогам работы круглого стола № 3 со Всероссийским и международным участием. Шахты, 2022.

4. *Осипов М. Е., Новичкова Е. Е.* Планирование работы следователя: организация индивидуальной работы // Правопорядок: история, теория, практика. 2020. № 2 (25).

5. *Фомина И. А.* Организация работы следователя // Сибирский юридический вестник. 2022. № 3 (98).

6. *Шувалов Н. В., Горелов М. Г.* Организация работы следователя по предупреждению уклонения обвиняемых (подозреваемых) от следствия к розыску // Вестник Волгоградской академии МВД России. 2021. № 3 (58).

Марат Кайдарович Сырлыбаев,
старший преподаватель кафедры
уголовного процесса и криминалистики
Алматинская академия МВД Республики
Казахстан имени Макана Есбулатова

Ботагоз Булатовна Сарсенбаева,
кандидат юридических наук,
профессор кафедры
уголовного процесса и криминалистики
Алматинская академия МВД Республики
Казахстан имени Макана Есбулатова

УДК 343.983

Природа возникновения цифровых следов

Аннотация

В данной статье рассматриваются основы возникновения цифровой информации и возможности использования цифровых технологий в обнаружении, изъятии, анализе доказательств в цифровом формате. Критерии доказательственной информации – относимость, допустимость и достаточность – трудно обеспечить при изъятии информации в цифровой форме. Однако при наличии знаний о природе возникновения и хранения цифровых следов имеется возможность обеспечить их неизменность в момент копирования, создать условия для точного анализа и вычленения криминалистически значимых данных.

Ключевые слова и словосочетания: *криминалистика; цифровая криминалистика; дампы памяти; накопители информации; хэш-сумма; образ информации.*

1 сентября 2023 года Президент Республики Казахстан Касым-Жомарт Кемелевич Токаев остро выделил проблему цифровизации Казахстана, сказав: «Вы знаете, я уделяю повышенное внимание вопросам цифровизации и внедрения инноваций. Перед нами стоит стратегически важная задача – превратить Казахстан в IT-страну» [5].

На сегодняшний день в Казахстане полным ходом реализуется огромное количество всевозможных проектов по внедрению цифровых технологий как в бизнес, так и госсектор. Одной из важнейших

государственных программ по внедрению IT-технологий в различные сферы жизнедеятельности казахстанцев является Государственная программа «Цифровой Казахстан», целью которой было обозначено: ускорение темпов развития экономики Республики Казахстан и улучшение качества жизни населения за счет использования цифровых технологий в среднесрочной перспективе, а также создание условий для перехода экономики Казахстана на принципиально новую траекторию развития, обеспечивающую создание цифровой экономики будущего в долгосрочной перспективе [1].

Банковский сектор пестрит различными предложениями для простых пользователей: интернет-магазинами, оплатой коммунальных услуг и другими возможностями цифровых систем.

На улицах больших городов в свободном пользовании имеется транспорт-шеринг, начиная от самокатов и велосипедов, заканчивая автомобилями. Все это возможно с использованием инновационных технологий и мобильных приложений, соединенных с банковским сектором оплаты услуг.

Однако не стоит забывать об обратной стороне медали. С развитием технологий и внедрением в массы простые пользователи становятся жертвами преступлений, связанными с информационно-коммуникационными технологиями.

Природа возникновения цифровых следов

В целях всестороннего и полного расследования уголовных дел правоохранительными органами проводится обнаружение, изъятие и фиксация всевозможных следов правонарушения с целью их дальнейшего анализа и использования.

Что касается следов правонарушения, в криминалистической науке принято разделять следы на материальные – результаты материального отражения свойств взаимодействующих в ходе преступной деятельности материальных объектов, исследование которых позволяет формировать доказательственную информацию об отдельных обстоятельствах совершенного преступления [3]; и идеальные – мысленные образы, отображенные в памяти человека [4].

По данным видам следам были написаны сотни исследований, которые рассматривали природу возникновения, критерии неизменности следов с течением времени, методики обнаружения изъятия и фиксации и многие другие аспекты. Но с развитием цифровых технологий, а также с использованием ИКТ при совершении правонарушений остро стал вопрос доказывания использования конкретного устройства конкретным лицом в целях изобличения правонарушителя. Это можно достигнуть лишь при изучении следов в цифровом пространстве.

Ранее в своих работах мы раскрывали понятие цифровых следов и следообразования в цифровом пространстве. Так, под цифровыми следами мы понимаем *криминалистически значимую информацию о любых действиях в цифровой среде, возникающих в процессе создания, обработки, хранении и передачи данных* [7].

На наш взгляд, это оптимальное определение, так как в первую очередь след должен нести в себе криминалистически значимую информацию о свойствах следообразующего объекта на разных стадиях взаимодействия с следовоспринимающим объектом, и данная информация должна сохранять свои свойства при неких манипуляциях с ней, т. е. копирование, передачу, хранение и т. д.

Для более детального рассмотрения природы цифровых следов необходимо заглянуть намного глубже в техническую часть возникновения цифровой информации. В этой связи мы рассмотрим такое явление, как компьютерный язык, историю его возникновения и практическое применение.

В 40-х годах XX в. программисты с целью настройки работы компьютеров вручную переставляли специализированные перемычки, каждая из которых отвечали на два сигнала (0-1). Данные сигналы обрабатывались центральным процессором, который занимал огромные площади. Это дало толчок развитию бинарного компьютерного языка.

Дальнейшее развитие компьютеров и машинных языков пошло в двух направлениях. Первым направлением являются языки программирования, т. е. язык, на котором специалист в области программирования вносил информацию в компьютер. К данным языкам относятся: Accembler, Frontran, Basic, COBOL, LISP, Prolog, Smalltalk, C, Objective-C, C++, Java и Python [2]. Все эти языки необходимы для создания алгоритмов программ, по которым работали и проводили вычисления компьютеры в те времена и по сей день.

Вторым направлением развития компьютерных языков является информация, воспринимаемая самой машиной, т. е. как компьютер видит и воспринимает информацию для обработки центральным процессором. К таким языкам относятся: двоичный код (BIN), восьмеричный код (OCT), десятеричный код (DEC), шестнадцатеричный код (HEX).

Изначально, как мы помним, программисты сами меняли значения переключателей для вноса информации и снимали показатели также в двоичной форме. Для восприятия информации им приходилось расшифровывать полученные результаты с машинного языка, на понятный человеку. Однако это занимало огромное количество

времени, так как шифрование одного символа могло занимать большую строку из 0 и 1, что могло приводить к искажению информации и/или неправильной дешифровки. В целях оптимизации строки шифрования были созданы языки восьмеричной, десятеричной и шестнадцатеричной систем счисления.

Эти два направления развития языков отличает лишь объект восприятия информации. В первом случае информация вносится на языке программирования, понятном человеку, состоящий из команд, символов и слов, которые в последующем обрабатываются и переносятся в систему компьютера в том языке, в котором работает компьютер с последующим ее анализом, хранением и передачей.

Так для чего мы описываем историю развития компьютерных языков в данной работе? Дело в том, что цифровой след остается только в тех местах, где имеется возможность накопления информации, так называемые файловые системы. Файловая система отвечает за то, как будет распределяться информация на запоминающем устройстве и какими способами будет группироваться в физическом плане (например, в последовательных кластерах или в произвольных) [6].

Информация в указанных системах записывается только на машинном языке, т. е. Bin, Oct, Dec, Hex, в зависимости от вида файловой системы. Таким образом, можно подытожить, что цифровая информация хранится в компьютере не в том варианте, в котором мы видим на экране, а в зашифрованной строке файловой системы и существует вероятность, что документ или фото, видео, программа могут храниться в данной файловой системе в хаотичном порядке по пустым битам.

В этой связи сразу становится понятным тот факт, что при удалении какого-то файла существует вероятность его восстановить в полном или частичном объеме.

Как это возможно? Дело в том, что каждый бит содержит информацию о местонахождении следующего бита и часть информации о самом файле. При удалении файла стираются не все биты, но компьютерная система этого не выдает. В момент сканирования файловой системы выявляются такого рода частицы удаленных файлов, и по данным крупицам восстанавливается весь файл.

Таким образом, мы приходим к выводу о том, что все цифровые следы, т. е. криминалистически значимая информация, являются частями файловой системы, содержащейся на носителях информации, и представляют собой зашифрованный код в виде компьютерного языка. Это означает, что от цифрового следа не так-то просто избавиться, но в него можно легко внести изменения.

К примеру, при включении компьютера или сотового телефона, при наличии подключения к интернету, системная программа автоматически сканирует драйверную базу и ищет обновления для корректной работы самой системы и периферийных устройств, подключенных к системе. В случае отнесения цифровой информации к доказательствам мы должны обеспечить недопущения внесения какого-то ни было изменения, так как это является критически важным фактором при определении достоверности информации изъятой у подозреваемого/потерпевшего и информации по окончании анализа и исследования.

Все это возможно обеспечить при помощи криминалистической техники, а также производством ХЭШирования, т. е. определения уникальности информации в цифровом формате.

Список литературы:

1. Информационно-правовая система нормативных правовых актов Республики Казахстан. URL: https://adilet.zan.kz/rus/docs/P1700000827 (дата обращения: 17.02.2024).

2. Контентная платформа Дзен. URL: https://dzen.ru/a/ZRwfr8vI_1lTTDVX (дата обращения: 17.02.2024).

3. Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/ponyatie-materialnye-sledy-prestupleniya#:~:text=Материальные%20следы%20преступления%20-%20это,об%20отдельных%20обстоятельствах%20совершенного%20преступления (дата обращения: 17.02.2024).

4. Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/trasologiya-idealnye-sledy/viewer (дата обращения: 17.02.2024).

5. Официальный сайт Акорда. URL: https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-ekonomicheskiy-kurs-spravedlivogo-kazahstana-18588 (дата обращения: 17.02.2024).

6. Софт-платформа BestFREE.ru. URL: https://www.bestfree.ru/article/computer/file-system.php (дата обращения: 17.02.2024).

7. *Сырлыбаев М. К., Туманшиев Р. К., Салаев А. Б.* Следообразование в цифровой среде // Ученые труды Алматинской академии МВД Республики Казахстан им. М. Есбулатова. 2023. № 2 (75).

Кристина Сергеевна Тарабрина,
адъюнкт факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: tarabrina_kristina@bk.ru

УДК 343.97

Виктимологические аспекты предупреждения сексуального насилия над несовершеннолетними, совершаемого с применением цифровых технологий

Аннотация

В статье анализируются основные виктимологические факторы, обусловливающие сексуальное насилие, совершаемое в отношении несовершеннолетних с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (далее – цифровые технологии). В ходе исследования автор приходит к выводу о том, что в условиях цифровой трансформации общества действующие российские правовые механизмы в недостаточной степени обеспечивают виктимологическую безопасность несовершеннолетних в сети Интернет, и предлагает ряд мер по предупреждению этого вида преступности.

Ключевые слова и словосочетания: *несовершеннолетние; виктимность; насилие; предупреждение; цифровые технологии; обеспечение виктимологической безопасности.*

В современном мире информационно-цифровые технологии являются неотъемлемой частью жизни людей, поэтому активно используются в различных сферах деятельности человека. Цифровые технологии помогают каждому члену общества в решении личных проблем, позволяют расширить кругозор мышления, способствуют повышению интеллектуальных способностей, предоставляют возможность легко и доступно общаться с близкими людьми по всему миру и пр.

Ускоренное развитие названных технологий не всегда приносит пользу обществу. Ежедневное применение сети Интернет, мессенджеров, социальных сетей порождает и негативные последствия. Связано это с активной цифровизацией общества и переносом большой части имеющейся информации в цифровой формат, что, несо-

мненно, увеличивает риски использования любой такой информации в преступных целях и является предпосылкой к росту преступлений, совершаемых в виртуальном пространстве.

Анализ криминальной обстановки свидетельствует о том, что количество преступлений, совершаемых в цифровой среде, ежегодно увеличивается. Результаты статистической отчетности ФКУ «ГИАЦ МВД России» о зарегистрированных преступлениях, совершенных с использованием цифровых технологий, свидетельствуют о том, что в 2023 г. зарегистрировано 676,6 тыс. преступлений, темпы прироста составили 29,6 % по отношению к аналогичному периоду предыдущего года[1]. В общем числе зарегистрированных преступлений их удельный вес составил 34,8 %. Анализ текущего состояния криминальной ситуации в данной области характеризуется сформировавшейся устойчивой тенденцией роста преступности.

Особую тревогу вызывает тот факт, что криминальные элементы в своих преступных целях активно используют цифровые технологии, обновляя при этом орудия, способы и расширяя средства совершения преступлений. В свою очередь, у правоохранительных органов возникает ряд проблемных вопросов при организации деятельности по раскрытию преступлений и расследованию уголовных дел, возбужденных по фактам совершения преступлений в цифровой среде. Высокая анонимность преступника, возможность объединения единомышленников с целью совершения противоправных деяний в сети Интернет, в том числе теневом сегменте глобальной сети, помогает ему не только скрывать свою личность, удалять следы совершения преступления, но и избегать уголовной ответственности.

Наиболее активными пользователями интернет-пространства являются несовершеннолетние. Подрастающее поколение с раннего детства повседневно пользуется современными технологиями. В XXI веке сеть Интернет стала новой реальностью для детей: общение, новые знакомства на интернет-площадках, обмен новостями, создание групп по интересам, в том числе и для обмена впечатлениями о складывающейся ситуации на интернет-площадках и прошедших событиях, а также получение полезной информации. Одними из основных средств общения несовершеннолетних в современных условиях являются социальные сети и мессенджеры. Проведенное исследование позволяет отметить, что популярными социальными сетями и мессенджерами среди несовершеннолетних являются: 85,4 % – «Вконтакте»; 78,5 % – Telegram; 58,4 %. – Tik Tok, 55,9 % –

[1] Состояние преступности в России. Ф.9 – 4 ЕГС. Москва: ГИАЦ МВД России.

WhatsApp (респондентам был задан вопрос с некоторыми вариантами ответов). Специалисты занимаются изучением влияния на развитие подростка социальных сетей и мессенджеров и отмечают, что оно неоднозначно [1; 2; 10].

Подростки размещают информацию, фотоизображения о себе в сети Интернет, в личных аккаунтах социальных сетей или мессенджеров, вступают в различные сообщества, просматривают новостные форумы города/поселка/населенного пункта и становятся потенциальной жертвой преступников. Особое внимание следует уделить росту зарегистрированных преступлений, совершенных против половой свободы и половой неприкосновенности в отношении несовершеннолетних. При этом названные посягательства всегда считались одними из самых опасных преступных деяний, так как их последствия крайне разрушительны для неокрепшей психики детей.

Объясняется это тем, что наиболее незащищенные слои нашего общества становятся уязвимыми к совершению в отношении них преступлений именно по причине размещения персональных сведений в открытой глобальной сети. Виртуальное пространство в настоящее время не контролируется и содержит огромный объем антиобщественных, незаконных и криминальных сведений. Необходимо подчеркнуть, что сеть Интернет недостаточно защищена от криминогенных лиц. Личные данные пользователей, в том числе лиц, не достигших совершеннолетия, могут быть скопированы, просмотрены или переданы в противозаконных целях третьим лицам. Тем самым криминогенная ситуация в цифровом пространстве ухудшается.

За последние пять лет (с 2019 по 2023 гг.) зарегистрировано более 19, 2 тыс. преступлений, совершенных в отношении несовершеннолетних с использованием цифровых технологий[1]. В целом за исследуемый период в России от преступлений, совершенных против половой свободы и половой неприкосновенности с использованием цифровой среды, пострадало 2,8 тыс. несовершеннолетних. В 2023 г. абсолютный рост потерпевших несовершеннолетних составил 160 (темпы роста 112 %) по отношению к аналогичному периоду 2022 г. Результаты исследования криминальной обстановки на основе статистических сведений о преступности свидетельствуют о том, что правоохранительные органы не могут в полной мере отразить масштабы сексуального насилия, сексуальной эксплуатации и домогательств, совершаемых над несовершеннолетними с применением цифровых технологий. Это обусловлено следую-

[1] Состояние преступности в России. Ф.9 – 4 ЕГС. Москва: ГИАЦ МВД России.

щим: «несовершеннолетние являются более вероятными объектами сексуального домогательства в интернете, отчасти из-за их большей мобильности, сексуального любопытства и относительной автономии, а для некоторых подростков свойственно рискованное сексуальное поведение» [8, с. 148].

Следует подчеркнуть, что названные факторы делают незащищенную категорию населения наиболее уязвимой перед криминальными лицами, поскольку подрастающее поколение реагирует на знаки внимания совершеннолетних незнакомцев в сети Интернет, социальных сетях или мессенджерах. Дети проявляют неосмотрительное виктимное поведение, общаются со взрослыми, устанавливают доверительные контакты, при этом раскрепощенно дискутируют на сексуальные темы, добровольно отправляют личные откровенные фото- и видеоизображения собеседнику, а также встречаются с незнакомцами в реальном мире [6, с. 216].

Для разработки эффективного механизма виктимологического предупреждения сексуального насилия над несовершеннолетними в цифровой среде необходимо остановиться на отдельных факторах, обусловливающих данный вид преступлений.

Первый фактор. Особую тревогу сегодня вызывает проблема обеспечения криминологической безопасности несовершеннолетних в условиях цифровизации. Это обусловлено тем, что несовершеннолетние относятся к группе повышенного риска и требуют к себе особого внимания в обеспечении защиты своих прав и интересов, в социальной поддержке. Подростки в силу возрастных и психологических особенностей, неокрепшей психики, недостаточного уровня образования, полового и правового воспитания и др. становятся потенциальной жертвой преступления в сети Интернет. Об этом свидетельствует и исследование М. В. Гусаровой, по мнению которой «некоторые виды преступлений сексуального характера получили дополнительный импульс к развитию посредством информационно-телекоммуникационной сети Интернет, составив часть киберпреступности; широкое распространение в сети получили такие явления, как секстинг и груминг» [3, с. 99].

Второй фактор. Интернет-площадка на современном этапе является общедоступной для различных членов общества. Контроль со стороны провайдеров глобальной сети находится на низком уровне. Так, сеть Интернет переполнена информацией, содержащей данные о детской порнографии (фото- и видео-), сценами жестокости и насилия, рекламой с элементами сексуальной распущенности. Несовершеннолетние, находясь в таком виртуальном мире, постепенно утрачивают нравственное и половое воспитание.

Масштабной проблемой для обеспечения криминологической безопасности несовершеннолетних в сети Интернет видится проблема отсутствия правильного восприятия традиционных духовно-нравственных ценностей.

Третий фактор. Облегчается процедура поиска несовершеннолетней жертвы. Преступники обладают профессиональным аналитическим складом ума и с легкостью выбирают жертву, не достигшую совершеннолетия. Несовершеннолетние при регистрации в различных социальных сетях указывают настоящие сведения о себе. Криминальные лица осознают то, что дети проявляют неосмотрительное виктимное поведение, охотно вступая в контакт с незнакомыми лицами. Любознательность несовершеннолетних в познании собственной сексуальности позволяет им устанавливать доверительные отношения с совершенно незнакомыми людьми. Подростки строят первые романтические отношения с помощью глобальной сети. В личных сообщениях, в том числе и при общении с незнакомцами, несовершеннолетние раскрепощенно обсуждают темы сексуального характера. Специалисты отмечают, что каждый третий несовершеннолетний, не достигший возраста шестнадцати лет, в личных сообщениях социальной сети или мессенджера получал информацию сексуального содержания от незнакомого лица. Проведенные исследования устанавливают, что «сексуальные посягательства в отношении детей способствуют развитию у них психических расстройств и заболеваний, нарушений в развитии идентичности, снижению сексуальной удовлетворенности и расстройству партнерских отношений в будущем» [9, с. 147].

Четвертый фактор. Недостаточная осведомленность детей о противоправном поведении и опасном контенте в интернет-пространстве и социальных сетях, о способах обеспечения безопасности в виртуальном пространстве приводит к разрушительным последствиям, повышая уровень виктимности несовершеннолетних. Отсутствие правовой грамотности детей, незнание общих правил использования безопасного интернета, умышленное распространение персональных данных в глобальной сети - все это делает наиболее уязвимыми несовершеннолетних при встрече в цифровой среде с преступником. Подросткам следует организовать проведение обязательных разъяснительных мероприятий по сохранению информационной безопасности в глобальной сети.

Пятый фактор. Недостаточная правовая защищенность несовершеннолетних от деструктивного воздействия криминальных лиц. В современных реалиях цифровые технологии «значительно облегчают реализацию преступной деятельности в отношении несо-

вершеннолетних, обеспечивая ее анонимность, расширяя возможности по поиску потенциальной жертвы, при этом снабжая разнообразными техническими средствами и возможностями для оказания психологического воздействия и давления» [5, с. 191]. В современных условиях уровень медиаграмотности подрастающего поколения остается низким. В соответствии с этим формирование медиаграмотности является актуальным приоритетом современного образования, так как это связано с обеспечением безопасности несовершеннолетних в сети Интернет.

Шестой фактор. Несовершенство профилактической деятельности правоохранительных органов. Информация о новых способах совершения насильственных преступлений с применением цифровых технологий должным образом не доводится до всех слоев общества, в том числе и до подрастающего поколения. Данный фактор способствует искаженному, неправильному представлению о преступной деятельности лиц, страдающих расстройством сексуального предпочтения (педофилией), сексуального удовлетворения.

Вышеизложенные факторы подтверждает и классификация основных форм криминогенного воздействия сети Интернет на несовершеннолетних, предложенная Е. В. Кузнецовой, которая является практически обоснованной и включает следующие виды воздействия:

– «контентное воздействие посредством информации, представляющей угрозу и риск для жизни, здоровья и развития несовершеннолетних (пропаганда агрессии, жестокости, насилия, экстремизма, наркотических средств, сексуальной распущенности, суицида и т. п.);

– «коммуникативное воздействие в процессе деструктивного межличностного общения (кибербуллинг, кибергруминг, секстинг, троллинг, флейминг, киберсталкинг и т. д.)» [4, с. 9].

Исходя из проведенного исследования, следует признать, что сегодня существует серьезная проблема, связанная с ростом насильственных преступлений, совершаемых в отношении несовершеннолетних с применением цифровых технологий, требующая особого внимания как со стороны государства, так и общества в целом. В первую очередь необходимо принять дополнительные меры по созданию действенных защитных барьеров в сети Интернет путем внедрения современных средств фильтрации и усиления ответственности интернет-провайдеров за публикацию запрещенного контента [7, с. 114].

Подводя итог, следует отметить, что в условиях цифровой трансформации общества действующие российские правовые меха-

низмы в недостаточной степени обеспечивают виктимологическую безопасность несовершеннолетних в сети Интернет.

Во-первых, в этой связи необходимо создать специальные интернет-площадки, на которых можно будет ознакомиться с информацией, в том числе и обучающего характера, о защите несовершеннолетних в сети Интернет. На этой базе создать информационный ресурс, который, во-первых, будет своевременно информировать сотрудников правоохранительных органов, несовершеннолетних, их родителей, педагогов о возможных рисках и угрозах совершения преступлений против половой свободы и половой неприкосновенности в глобальной сети.

Во-вторых, оказывать консультационную поддержку пострадавшим несовершеннолетним от насилия, в частности сексуального насилия, жестокости и агрессии.

В-третьих, следует включить в образовательные программы обучение безопасному поведению в глобальной сети, проводить еженедельные тренинги с детьми на рассматриваемую тему. Следует повысить «авторитет» глобальной сети, убедить родителей в том, что воздействие информационных ресурсов будет способствовать развитию нравственного, образовательного, культурного уровня.

Предложенные меры являются важными и ориентированы на обеспечение безопасности детей в условиях цифровой среды.

Список литературы:

1. *Абишева В. Т., Серкова Е. А.* Социальные сети как эффективный инструмент PR-коммуникации // Актуальные проблемы гуманитарных и естественных наук. 2015. № 11-2.

2. *Бочавер А. А [и др.].* Использование социальных сетей в интернете и депрессивная симптоматика у подростков // Клиническая и специальная психология. 2019. Т. 8. № 3.

3. *Гусарова М. В.* Личность сексуального преступника: криминологическая характеристика // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 4 (54).

4. *Кузнецова Е. В.* Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети интернет: дис. ... канд. юрид. наук. Курск, 2019.

5. *Мамаева А. Е.* Меры предупреждения вовлечения несовершеннолетних в преступления посредством социальных сетей в зарубежных странах и России // Закон и право. 2022. № 5.

6. *Михайлова Е. В.* Вовлечение несовершеннолетних в сексуальную эксплуатацию с использованием информационно-телеком-

муникационных технологий // Ученые записки Казанского юридического института МВД России. 2021. № 2 (12).

7. *Нынюк Р. Н.* Информационная безопасность детей в Российской Федерации: проблемы реализации. Иркутск: Восточно-Сибирский институт МВД России. 2023. Т. 26. № 2.

8. *Пыжиков М. А.* Роль виктимного поведения потерпевших в механизме совершения развратных действия с использованием сети Интернет // Аграрное и земельное право. 2019. № 6 (174).

9. *Скворцова О. В., Макаренко Д. Д.* Развратные действия с использованием сети Интернет // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2021. №1.

10. *Храмова М. В.* Отношение родителей к потенциальным опасностям при увлечении школьников соцсетями / М. В. Храмова, Е. Н. Пицик // Образовательные технологии и общество. 2017. Т. 20. № 3.

Айман Асанқызы Толыбаева,
докторант
Алматинская академия
Министерства внутренних дел
Республики Казахстан имени М. Есбулатова
E-mail: a.tolybaeva95@mail.ru

Гаухар Рустембековна Рустемова,
доктор юридических наук, профессор,
профессор кафедры управления
правоохранительной деятельностью
Алматинская академия
Министерства внутренних дел
Республики Казахстан имени М. Есбулатова
E-mail: g.rustemova@mail.ru

УДК: 343.13
МРНТИ:10.7951

Цифровая грамотность сотрудников правоохранительных органов при противодействии онлайн-мошенничеству

Аннотация

Статья подчеркивает важность цифровой грамотности в современном обществе особенно в контексте борьбы с онлайн-мошенничеством. Авторы анализируют, как развитие цифровой грамотности среди населения способствует повышению уровня информационной безопасности и защите от киберпреступлений. Особое внимание уделяется необходимости комплексного подхода к обучению граждан основам цифровой безопасности, развитию критического мышления и пониманию этики в цифровом пространстве. Авторы анализируют современные требования к цифровой компетентности в сфере правопорядка, выявляют основные вызовы и риски, стоящие перед правоохранителями в условиях цифровой трансформации. В статье рассматриваются методы обучения и подготовки сотрудников правоохранительных органов, направленные на повышение их цифровой грамотности, а также предлагаются практические рекомендации по эффективному внедрению цифровых навыков в рамках профессиональной деятельности.

Авторы обосновывают, что цифровая грамотность является ключевым элементом в предотвращении онлайн-мошенничества

и обеспечении общественной безопасности, а также подчеркивают роль государственной поддержки и международного сотрудничества в этой области. Приводятся примеры успешных инициатив по повышению цифровой грамотности в различных странах, включая Сингапур, Финляндию и Южную Корею. Работа имеет целью содействовать развитию современных стратегий подготовки правоохранителей к эффективному противостоянию онлайн-мошенничеству и обеспечению цифровой безопасности в сфере правопорядка.

Ключевые слова и словосочетания: *цифровая грамотность; онлайн-мошенничество; информационная безопасность; киберпреступления; стратегии противодействия.*

В современном мире, где технологии занимают все более значимое место в жизни общества, вопросы информационной безопасности и защиты от киберпреступлений становятся особенно актуальными. Среди множества факторов, способствующих повышению информационной безопасности, особое место занимает цифровая грамотность населения. Цифровая грамотность не просто обеспечивает индивиду навыки работы с цифровыми технологиями, но и вооружает его знаниями и инструментами для защиты в цифровом пространстве.

На фоне растущего числа онлайн-мошенничества, включая фишинг, мошенничество с использованием личных данных и финансовые интернет-мошенничества, становится очевидной необходимость комплексного подхода к обучению граждан основам цифровой безопасности. Целью данной статьи является исследование роли цифровой грамотности как важнейшего фактора антикриминальной безопасности и разработка стратегий противодействия онлайн-мошенничеству.

В современном дискурсе о цифровой трансформации особое место занимает концепция человеческого капитала, которая, как подчеркивает Президент Республики Казахстан Касым-Жомарт Токаев [8], одновременно является ключевым приоритетом и значительным вызовом. Важность человеческого капитала обусловлена необходимостью адаптации и управления цифровыми тенденциями, что, в свою очередь, предполагает кардинальное переосмысление и изменение существующих подходов к цифровой грамотности и образованию. Это утверждение подчеркивает сложность и многоаспектность процесса цифровой трансформации, в центре которого находится человек со своими навыками, знаниями и способностью к обучению.

Понятие цифровой грамотности начало формироваться в конце XX века, когда массовое распространение персональных компьютеров и интернета привело к необходимости развития новых знаний и навыков у пользователей. В первоначальном понимании цифровая грамотность сводилась к умению использовать компьютерные технологии для работы с информацией. Однако с развитием информационных и коммуникационных технологий (ИКТ) концепция цифровой грамотности значительно расширилась и охватила широкий спектр навыков и компетенций.

Стоит отметить, что это расширение охватывает не только технические аспекты использования ИКТ, но и развитие критического мышления, понимание этики в цифровом пространстве, а также умение безопасно и ответственно взаимодействовать в онлайн-среде. Современная цифровая грамотность требует от пользователей не только знания и понимания того, как работают цифровые инструменты и платформы, но и способности критически анализировать получаемую информацию, распознавать и предотвращать риски цифровой безопасности, а также эффективно и этично использовать цифровые технологии для общения, обучения и профессиональной деятельности.

Эволюция цифровой грамотности отражает изменения в обществе и технологиях, подчеркивая важность адаптации к новым формам информационного взаимодействия. В контексте постоянно развивающегося цифрового ландшафта, где новые инструменты и платформы появляются с беспрецедентной скоростью, цифровая грамотность становится динамичной компетенцией, требующей постоянного обновления знаний и навыков.

Важно подчеркнуть, что цифровая грамотность тесно связана с социальной инклюзией и доступом к знаниям. В условиях глобализированного мира доступ к информации и возможность ее использования играют ключевую роль в уровне жизни людей, их образовательных и профессиональных возможностях. Поэтому стратегии развития цифровой грамотности часто включают в себя меры по обеспечению равного доступа к цифровым ресурсам и технологиям для всех слоев населения, с особым вниманием к уязвимым группам.

Таким образом, цифровая грамотность в современном мире выходит за рамки простого умения пользоваться технологиями. Она представляет собой комплексное понимание и умение действовать в цифровом пространстве, что включает в себя информационную, техническую, медиа и цифровую безопасность. Развитие этих компетенций способствует формированию осознанных, ответствен-

ных и безопасных пользователей цифрового мира, способных адаптироваться к его постоянным изменениям и использовать потенциал цифровых технологий для личного и общественного блага.

Современная цифровая грамотность включает в себя несколько ключевых компонентов.

1. Информационная грамотность является основой для понимания и оценки информации, доступной в цифровом пространстве. В условиях информационного перенасыщения критически важно уметь отличать достоверную информацию от дезинформации, фейков и манипуляций. Этот навык включает в себя поиск, анализ и синтез информации из различных источников для решения задач, стоящих перед пользователем, а также этичное использование и распространение информации.

2. Компьютерная грамотность обеспечивает базовые знания и умения, необходимые для работы с компьютерной техникой и программным обеспечением. Она охватывает понимание работы операционных систем, офисных приложений, программ для обработки графики и видео, а также навыки использования интернета и различных веб-сервисов. Компьютерная грамотность служит фундаментом для более глубокого изучения ИКТ и развития специализированных навыков в этой области.

3. Медиаграмотность акцентирует внимание на критическом восприятии медиаконтента, который является неотъемлемой частью современной жизни. Развитие медиаграмотности включает в себя понимание механизмов создания медиасообщений, их целей и влияния на аудиторию. Осознанное потребление медиа помогает индивидам развивать навыки анализа и оценки информации, представленной в различных форматах, и осознавать возможные манипуляции и предвзятость.

4. Грамотность в области информационной безопасности становится все более важной в контексте увеличения числа угроз цифровой безопасности. Она включает в себя знание принципов защиты персональных данных, понимание рисков, связанных с использованием интернета, и умение использовать инструменты и методы защиты от вирусов, фишинга, мошенничества и других видов кибератак. Осведомленность в области информационной безопасности позволяет пользователям предотвращать потенциальные угрозы и защищать свою личную и профессиональную информацию в цифровом пространстве.

В совокупности эти компоненты формируют комплексную цифровую грамотность, необходимую каждому современному человеку для успешной адаптации к условиям цифровизированного

общества, обеспечения своей безопасности в интернете и эффективного использования возможностей, которые предоставляет цифровая эпоха.

В эпоху информационного общества цифровая грамотность становится не просто желаемым, а необходимым условием полноценного участия индивида в социальной, экономической и культурной жизни. Она обеспечивает личности инструменты для успешной адаптации к быстро меняющимся технологическим условиям, позволяет эффективно решать профессиональные и личные задачи в цифровой среде, защищать себя от информационных угроз и мошенничества. Цифровая грамотность способствует формированию критического мышления, повышает качество и доступность образования, укрепляет демократические процессы за счет обеспечения свободного доступа к информации и возможности участия в общественной жизни.

Среди наиболее распространенных видов онлайн-мошенничества выделяют фишинг, скимминг, фарминг, вредоносное программное обеспечение (включая троянские программы и вирусы), а также различные схемы социальной инженерии, направленные на манипуляцию поведением пользователя для получения доступа к его персональным данным и финансам. Мошенники постоянно совершенствуют свои методы, используя новейшие технологии и психологические приемы, что делает борьбу с этим явлением особенно сложной задачей [2].

Онлайн-мошенничество оказывает серьезное негативное влияние на экономику и общество. С одной стороны, оно приводит к прямым финансовым потерям для жертв, с другой — подрывает доверие к цифровым финансовым услугам, электронной коммерции и онлайн-бизнесу в целом. Долгосрочные социально-экономические последствия включают усиление социального неравенства, поскольку наиболее уязвимые слои населения часто становятся жертвами мошенников, а также угрозу устойчивому развитию цифровой экономики.

Анализируя статистические данные, можно отметить значительный рост объемов онлайн-мошенничества в последние годы. По итогам 2023 года всего по стране зарегистрировано 15 616 таких уголовных правонарушений [3]. По данным международных и национальных организаций, занимающихся вопросами кибербезопасности, ежегодно фиксируется увеличение количества жалоб на фишинг, идентификационное мошенничество и другие виды киберпреступлений. Эта тенденция коррелирует с увеличением числа пользователей интернета и объемов онлайн-транзакций, что

делает вопросы цифровой грамотности и информационной безопасности еще более актуальными.

Особенно тревожным является развитие технологий искусственного интеллекта и машинного обучения, которые мошенники используют для создания все более сложных и убедительных схем обмана [4]. В этом контексте критически важным становится не только повышение уровня цифровой грамотности населения, но и разработка комплексных мер по укреплению кибербезопасности на национальном и международном уровнях, включая законодательные инициативы, развитие технологий защиты и сотрудничество сектора информационных технологий с государственными органами и международными организациями.

Принимая во внимание динамику развития цифровых технологий и изменения в поведении пользователей, необходимо постоянно адаптировать подходы к обеспечению информационной безопасности, акцентируя внимание на предотвращении мошенничества и защите прав потребителей в цифровой среде.

В современном информационном обществе, где онлайн-мошенничество представляет собой значительную угрозу для пользователей интернета, цифровая грамотность выступает не просто как набор навыков работы с цифровыми технологиями, а как фундаментальный инструмент защиты от мошеннических схем и атак.

Образование играет ключевую роль в повышении уровня цифровой грамотности среди всех слоев населения. Осведомленность о методах и приемах, которые используют мошенники, позволяет пользователям интернета распознавать потенциальные угрозы и избегать вовлечения в мошеннические схемы. Обучение основам безопасного взаимодействия в сети, понимание принципов защиты личной информации и данных, а также знание о правах и обязанностях в цифровом пространстве становятся неотъемлемой частью современного образовательного процесса.

Многие страны и организации разработали и реализовали успешные программы и стратегии, направленные на повышение цифровой грамотности среди населения. Программа развития ООН «Цифровая стратегия на 2022–2025 годы» [5] является значимым шагом на пути к реализации глобальных целей устойчивого развития. Центральными аспектами этой стратегии являются улучшение доступа к цифровой связи и повышение цифровой грамотности населения, что направлено на сокращение цифрового разрыва между различными странами и регионами мира. Программа стремится обучить людей необходимым цифровым навыкам для успешной работы и жизни в условиях цифровой экономики. Это вклю-

чает в себя понимание основ работы с компьютером, интернетом, мобильными приложениями, а также осознание вопросов кибербезопасности и защиты личных данных.

В рамках проекта «Цифровая грамотность российских педагогов» [9] от НАФИ реализованы различные образовательные мероприятия и программы, такие как вебинары, онлайн-курсы, семинары и мастер-классы по цифровой безопасности, использованию образовательных технологий, методикам преподавания информационной грамотности и другим важным темам. Эффективность таких программ подтверждается не только повышением уровня компетенций учителей, но и улучшением качества образования в целом, а также снижением риска вовлечения учащихся в опасные ситуации в сети.

Яндекс Практикум [10] запустил бесплатную программу по развитию цифровой грамотности. Этот курс помогает людям лучше понимать современный цифровой мир и обучает навыкам работы с современными технологиями. Особое внимание уделяется вопросам безопасности в интернете, что особенно актуально в свете растущего числа киберугроз и онлайн-мошенничества.

Обучение, предлагаемое в рамках программы, позволит участникам не только приобрести практические навыки в области ИТ и интернет-технологий, но и научиться защищать свои данные и финансовую информацию от потенциальных угроз. Такие инициативы, как программа от Яндекс Практикума, играют ключевую роль в сокращении цифрового разрыва и повышении общего уровня информационной безопасности среди населения. Они не только обеспечивают доступ к знаниям и умениям, необходимым для успешной навигации в цифровом мире, но и способствуют формированию более безопасного и осознанного подхода к использованию цифровых ресурсов.

В условиях стремительного развития информационных технологий и цифровизации всех сфер жизни общества, повышение уровня цифровой грамотности населения становится одним из ключевых приоритетов государственной политики, образовательной системы, а также деятельности некоммерческих организаций и частного сектора. Рассмотрим основные стратегии и методы, направленные на решение этой задачи.

Активизация государственной политики в сфере формирования цифровой грамотности занимает центральное место в стратегии цифровой трансформации, осуществляемой на уровне национальных правительств. Примером такой политики служат меры, принимаемые в Республике Казахстан, где разработка и реализация законодательных инициатив направлены на всестороннее обеспе-

чение доступа к цифровым ресурсам, развитие необходимой инфраструктуры и поддержку образовательных программ в области ИТ. Среди ключевых мер — предоставление налоговых льгот и субсидий организациям и учебным заведениям, способствующим повышению уровня цифровой грамотности, а также разработка стандартов и требований к уровню цифровой грамотности различных категорий граждан.

В качестве конкретных примеров можно выделить следующие инициативы.

1. Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы [11], утвержденная Правительством Республики Казахстан 28 марта 2023 г. Эта концепция нацелена на формирование базовых IT-компетенций среди граждан, целевую подготовку IT-специалистов, а также междисциплинарную подготовку работников других сфер деятельности.

2. Закон Республики Казахстан от 6 февраля 2023 г. № 193-VII «О цифровых активах в Республике Казахстан» [12], регулирующий вопросы, связанные с цифровыми активами и направленный на стимулирование развития цифровой экономики страны.

Такие инициативы демонстрируют комплексный подход казахстанского правительства к вопросам цифровой грамотности и цифровизации образования, подчеркивая стратегическую ориентацию на создание условий для успешной адаптации населения к требованиям цифровой экономики.

С утверждением государственной программы «Цифровой Казахстан», реализация образовательных инициатив в этой сфере охватила все регионы страны, включая районные центры, села и поселки, предоставив населению возможность бесплатного обучения базовым навыкам цифровой грамотности. Программа обучения была структурирована вокруг четырех ключевых модулей.

1. «Базовые цифровые навыки», охватывающие компетенции в области использования персональных компьютеров, ноутбуков, мобильных устройств и интернета, а также вопросы кибербезопасности и защиты данных.

2. «Электронное правительство и электронные государственные услуги», направленные на обучение навыкам эффективного взаимодействия с порталом электронного правительства для получения государственных услуг в онлайн-формате.

3. «Открытое правительство», включающее обучение использованию компонентов портала открытого правительства, таких как

доступ к открытым данным, нормативно-правовым актам, ведению открытого диалога и осведомленности о бюджетах.

4. «Электронная торговля», предоставляющий знания и навыки для осуществления онлайн-покупок, продажи и продвижения товаров и услуг.

Обучение проводилось на базе школ, колледжей и библиотек, задействовав 2 729 учреждений по всей стране, что подчеркивает масштабность и системность подхода к повышению цифровой грамотности среди населения Казахстана [15].

Переходя от анализа инициатив по повышению цифровой грамотности в Казахстане к обзору международного опыта в этой сфере, мы обнаруживаем важные сходства и различия в подходах к противодействию онлайн-мошенничеству через образовательные программы. Как и в Казахстане, где активно развиваются цифровая грамотность и цифровизация образования через государственные инициативы и законодательные меры, многие страны мира также признают критическую важность этих элементов в создании безопасного и инклюзивного цифрового общества.

Международный опыт, особенно примеры из Сингапура, Финляндии и Южной Кореи, подчеркивает универсальность стремления к повышению уровня цифровой грамотности среди населения как ключевого элемента в борьбе с цифровыми угрозами и онлайн-мошенничеством. Эти страны демонстрируют разнообразие подходов, от школьных программ до национальных кампаний по осведомленности, что отражает многогранность задачи повышения цифровой грамотности.

Сингапур активно реализует программы цифровой грамотности в рамках национальной стратегии Smart Nation [14], включая кампании по информированию граждан о методах защиты от онлайн-мошенничества и вирусов. Ключевым элементом является сотрудничество правительства с частным сектором и образовательными учреждениями. Целью этой стратегии является создание интеллектуальной нации, где цифровые технологии и инновации используются для улучшения жизни граждан, усиления общественного взаимодействия и повышения эффективности экономики. Это включает в себя обучение граждан безопасным онлайн-практикам и методам защиты от онлайн-мошенничества и вирусов. Ключевые инициативы и меры в рамках стратегии Smart Nation выделяют следующие.

1. Сингапур внедряет образовательные программы по цифровой грамотности для всех возрастных групп, начиная с школьников и заканчивая пожилыми людьми. Эти программы направлены

на обучение основам использования интернета, пониманию цифровой безопасности и защите личных данных.

2. Правительство Сингапура активно сотрудничает с компаниями технологического сектора для создания и реализации инновационных решений, направленных на повышение цифровой грамотности. Примером такого сотрудничества может служить разработка приложений и онлайн-курсов, предоставляющих знания о кибербезопасности и цифровой этике.

3. В рамках стратегии Smart Nation проводятся обширные информационные кампании, направленные на повышение осведомленности граждан о рисках онлайн-мошенничества и способах защиты от вирусов. Эти кампании включают в себя распространение информационных материалов через СМИ, социальные сети и публичные мероприятия.

4. Сингапур инвестирует в развитие высокоскоростной интернет-инфраструктуры и создание доступных цифровых платформ, которые обеспечивают гражданам удобный доступ к образовательным ресурсам и услугам.

Эти инициативы показывают, как комплексный подход, включающий образование, сотрудничество между государством и частным сектором, а также активные кампании по повышению осведомленности, может способствовать формированию цифровой культуры среди населения. Сингапурский опыт демонстрирует, что повышение цифровой грамотности является ключевым фактором в защите граждан от онлайн-угроз и в создании основы для устойчивого развития цифрового общества.

Финляндия, признанный лидер в области образования, активно внедряет программы, направленные на повышение цифровой грамотности и медиаграмотности среди своих граждан. Особенностью финского подхода является акцент на развитии критического мышления и критического восприятия информации с раннего возраста, что ставит Финляндию в ряд стран с наиболее продвинутыми системами образования в мире в контексте подготовки к жизни в условиях цифровизации [7].

В Финляндии обучение навыкам критического анализа медиаконтента и информации начинается с начальной школы. Уроки медиаграмотности включены в общеобразовательную программу и направлены на формирование у учащихся умения критически оценивать информацию, распознавать манипулятивные техники и понимать, как медиа влияет на общественное мнение [6]. Помимо школьных программ, в Финляндии реализуются курсы и обучающие программы для взрослых и пожилых людей, направленные

на повышение уровня цифровой грамотности и безопасного использования цифровых технологий. Также Финские образовательные учреждения активно сотрудничают с СМИ и некоммерческими организациями для создания и распространения образовательных материалов по медиаграмотности и безопасности в интернете.

Финская стратегия обучения медиаграмотности и критическому восприятию информации демонстрирует, как комплексный и системный подход к образованию может эффективно повышать цифровую грамотность населения и укреплять общественную устойчивость к онлайн-мошенничеству. Этот опыт подчеркивает значимость раннего начала образовательного процесса в области критического мышления и медиаграмотности для формирования осознанного и безопасного поведения в цифровом мире.

Южная Корея, одна из ведущих стран мира в области информационных технологий, является лидером среди азиатских стран (2-е место в мире после Дании) в сфере IT-инфраструктуры, включая скорость интернета, кибербезопасность, использование цифровых технологий, активно работает над повышением цифровой грамотности своего населения через реализацию обширных образовательных программ. Особое внимание уделяется обучению граждан пониманию и эффективному использованию цифровых технологий, что является ключевым элементом стратегии страны по созданию инклюзивного и доступного цифрового общества.

Южная Корея активно внедряет программы цифрового образования в школах, начиная с начального уровня, где дети учатся основам работы с компьютером, интернетом и другими цифровыми технологиями. Программы для старших классов и студентов включают более специализированные курсы, такие как программирование, кибербезопасность и использование искусственного интеллекта [1]. Для взрослого населения и рабочей силы разработаны программы, направленные на повышение цифровых навыков в соответствии с требованиями современного рынка труда. Эти программы способствуют переходу на новые рабочие места в IT-секторе и повышению конкурентоспособности на международном уровне. Особое внимание уделяется программам цифрового образования для пожилых людей, которые помогают им адаптироваться к быстро меняющемуся технологическому миру, обеспечивая доступ к цифровым услугам и социальным сетям. По данным Samjong KPMG, консалтинговой фирмы из Сеула, уровень цифровой грамотности пожилых людей здесь вырос на 4,8 процентных пункта до 69,1 процента [13].

Эти страны демонстрируют, что инвестиции в образование и развитие навыков цифровой грамотности являются ключевыми

для подготовки населения к жизни в условиях постоянно развивающегося цифрового мира, где знания и умения в области ИТ и кибербезопасности становятся не просто важными, а абсолютно необходимыми для каждого человека.

Исследование роли цифровой грамотности в обеспечении антикриминальной безопасности и разработка стратегий противодействия онлайн-мошенничеству показали, что цифровая грамотность является неотъемлемым инструментом защиты в современном информационном обществе. Она обеспечивает не только базовые навыки работы с цифровыми технологиями, но и развивает критическое мышление, понимание этики в цифровом пространстве и умение безопасно взаимодействовать в онлайн-среде. Таким образом, цифровая грамотность выступает как фундаментальная база для повышения общественной безопасности и эффективного противодействия киберпреступлениям.

Практическая часть работы демонстрирует значимость комплексного подхода к обучению граждан основам цифровой безопасности. Анализ различных программ и стратегий, направленных на повышение цифровой грамотности в разных странах, подтверждает эффективность таких инициатив в снижении уровня онлайн-мошенничества и повышении уровня информационной безопасности населения. Это подчеркивает важность государственной поддержки и инвестиций в образовательные программы, а также необходимость активного вовлечения всех секторов общества в процесс обучения и повышения осведомленности о цифровой безопасности.

Сравнение полученных результатов с поставленной целью и задачами показывает, что цифровая грамотность эффективно способствует повышению антикриминальной безопасности, однако для достижения более значимых результатов требуется дальнейшее развитие и совершенствование стратегий обучения. Необходимо учитывать динамичность цифрового мира, постоянно обновляя и адаптируя образовательные программы к новым угрозам и вызовам.

В заключительной части следует отметить, что дальнейшее развитие исследований в данной области должно сосредоточиться на разработке инновационных методов обучения, включая использование искусственного интеллекта и машинного обучения для создания персонализированных образовательных ресурсов. Кроме того, важно углубленное изучение психологических аспектов восприятия и поведения пользователей в цифровом пространстве для эффективного противодействия социальной инженерии и манипулятивным техникам мошенников.

Авторские рекомендации включают в себя не только усиление роли образования в повышении цифровой грамотности, но и развитие стратегий международного сотрудничества и обмена лучшими практиками. Это поможет создать единую глобальную систему противодействия киберугрозам и онлайн-мошенничеству, учитывая безграничность и трансграничный характер цифрового пространства. Также следует акцентировать внимание на развитии законодательной базы, обеспечивающей защиту пользователей в интернете и ужесточение наказаний за киберпреступления.

Прогнозы развития проблемы цифровой грамотности указывают на необходимость постоянного анализа тенденций в области информационных технологий и кибербезопасности, а также гибкость в внедрении новых образовательных программ. Повышение уровня цифровой грамотности населения должно стать приоритетом в политике любого государства, стремящегося к созданию безопасного и справедливого информационного общества.

В заключение цифровая грамотность является ключевым элементом антикриминальной безопасности в современном мире. Развитие и внедрение эффективных стратегий обучения и повышения осведомленности граждан о цифровой безопасности способствует снижению рисков онлайн-мошенничества и укреплению информационной устойчивости общества. Дальнейшие исследования и практические инициативы должны сосредоточиваться на адаптации к постоянно меняющимся условиям цифрового мира, обеспечивая всестороннюю поддержку и защиту для всех пользователей интернета.

Список литературы:

1. *Абдалимова Д. О.* Актуальность цифровизации образования на примере Южной Кореи // Proceedings of MMIT'23 International Conference 25 May 2023.

2. Виды мошенничества в интернете. URL: https://journal.tinkoff.ru/wiki/fraud/#two (дата обращения: 01.02.2024).

3. Из 15 тыс. случаев интернет-мошенничества более трех тысяч совершили от имени банков. – URL: https://kz.kursiv.media/2023-10-22/dmnv-internet-moshennichestvo/(дата обращения: 01.02.2024).

4. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее. URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (дата обращения: 01.02.2024).

5. Программа развития ООН. URL: https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-ABRIDGED-VERSION-PRINT_RU_Interactive.pdf (дата обращения: 01.02.2024).

6. *Сиркку Котилайнен, Рейе Купиайнен*. Медиаобразование в Финляндии: оценка уровня медиаграмотности учащихся 9 классов: коллективная монография. Москва: РИЦ МГГУ имени М. А. Шолохова. 2014.

7. Система образования Финляндии. URL: https://www.infofinland.fi/ru/education/the-finnish-education-system (дата обращения: 01.02.2024).

8. Токаев: Нашим людям предстоит принять новые способы мышления. URL: https://yk.kz/news/politika/tokaev-nashim-lyudyam-predstoit-prinyat-novyie-sposobyi-myishleniya-313112.html (дата обращения: 01.02.2024).

9. Цифровая грамотность российских педагогов. URL: https://nafi.ru/projects/sotsialnoe-razvitie/tsifrovaya-gramotnost-rossiyskikh-pedagogov/ (дата обращения: 01.02.2024).

10. Яндекс запускает бесплатную программу по повышению цифровой грамотности. URL: https://yandex.ru/company/news/01-22-01-2024 (дата обращения: 01.02.2024).

11. «2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы» Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысы. URL: https://adilet.zan.kz/kaz/docs/P2300000269 (дата обращения: 01.02.2024).

12. «Қазақстан Республикасындағы цифрлық активтер туралы» Қазақстан Республикасының 2023 жылғы 6 ақпандағы № 193-VII Заңы (2024.11.02. берілген өзгерістермен).

13. Byun Hye-jin. Digital health care for seniors blue ocean in S.Korea: report. URL: https://www.koreaherald.com/view.php?ud=20220712000683&np=1&mp=1 (дата обращения: 01.02.2024).

14. Smart Nation Singapore: The Way Forward. URL: https://www.smartnation.gov.sg/ (дата обращения: 01.02.2024).

15. Қазақстандағы цифрлық сауаттылық. URL: https://egov.kz/cms/kk/articles/digital_literacy (дата обращения: 01.02.2024).

Борис Андреевич Торопов,
докторант факультета подготовки научных
и научно-педагогических кадров
Академия управления МВД России
E-mail: torbor@mail.ru

УДК 004.043

О некоторых аспектах планирования деятельности органов внутренних дел Российской Федерации по противодействию распространению запрещенной информации в социальных сетях

Аннотация

Рассматривается подход к планированию деятельности органов внутренних дел Российской Федерации по противодействию распространению запрещенной информации в социальных сетях, основанный на исследовании влиятельности пользователей, занимающихся противоправными деяниями, сборе дополнительной информации о их личностях и местоположении, применении к ним рациональных мер воздействия для достижения цели сокращения аудитории, которая потенциально может ознакомиться с распространяемой запрещенной информацией.

Ключевые слова и словосочетания: *социальные сети; информационное влияние; распространение информации; органы внутренних дел.*

На настоящий день российским законодателем криминализировано достаточно много разнообразных деяний, предполагающих распространение информации в цифровом пространстве.

Помимо предусмотренных Конституцией Российской Федерации норм, запрещающих порочение чести и доброго имени гражданина, пропаганду и агитацию, разжигающую межклассовую, межрелигиозную, межнациональную и иную рознь, дискриминацию групп граждан по их принадлежности к этнической, религиозной и иным характеристикам, криминальным деянием сегодня может считаться размещение информации, пропагандирующей гомосексуализм, суицидальное поведение, наркопотребление среди молодежи, информации дискредитирующей вооруженные силы Российской Федерации, призывы к пересмотру итогов Второй мировой войны, к изменению конституционного строя страны, ее территориальных границ и др.

Как видно, перечень информации, распространение которой правоохранителям следует выявлять, пресекать и профилактировать велик, а информация, попадающая в него, может классифицироваться, с одной стороны, чрезвычайно расширительно, с другой стороны, избирательно. Что ж, этот путь избран отечественным законодателем, выражающим волю народа. Органы внутренних дел в существующем правовом поле выступают лишь государственным инструментом поддержания законности. Они обязаны в соответствии с законодательством предупреждать, выявлять, пресекать рассматриваемые деяния. Необходимо учитывать, что ресурсов правоохранительной системы в целом и органов внутренних дел в частности попросту не хватит для реагирования на все факты подобного рода.

При планировании деятельности по выявлению, пресечению, предупреждению информации, криминализованной российским законодателем, следует иметь в виду следующие обстоятельства.

1. Какие именно противоправные факты распространения информации имеют место, какова их общественная опасность.

2. Массовость фактов противоправного распространения информации, выражающаяся как в количестве инициаторов и участников противоправного распространения информации, так и в охвате аудитории, которая потенциально восприняла распространяемую информацию.

3. Возможности правоохранительных органов по доступу к информационным ресурсам, размещающим названные выше виды информации, и оперированию на данных информационных ресурсах.

4. Виды мер, которые могут быть приняты в связи с фактами обнаружения рассматриваемой информации. Они зависят от ряда факторов: в юрисдикции какого государства находятся исследуемые информационные ресурсы; в каком государстве физически находятся пользователи, представляющие интерес; установлены или не установлены их личности.

5. Располагаемые ресурсы для реализации избранных мер (людские, денежные, технические и т. п.).

Таким образом, обобщенный механизм планирования мероприятий по противодействию противоправному распространению информации заключается в выполнении следующих этапов.

1. Определение круга пользователей, участвующих в распространении информации, в результате чего получается список учетных записей на различных информационных ресурсов.

2. Для каждой обнаруженной учетной записи определяется мера влиятельности соответствующего пользователя. Это может быть осуществлено разными способами, самый простой из которых

заключается в фиксации количества подписчиков, комментариев, реакций, друзей и т. п. Однако на взгляд автора целесообразно использовать иные меры, например, метрики центральности, подробнее о которых можно прочитать в работе М. О. Джексона [3]. Отечественные авторы также рассматривают подобные меры влиятельности, например, А. Н. Рабчевский и Е. А. Рабчевский предлагают свой авторский критерий потенциальный уровень влияния пользователя социальной сети [2].

3. Полученный список учетных записей ранжируется на основе ранее рассчитанной меры влиятельности.

4. Далее каждую запись в ранжированном и дополненном списке найденными сведениями списке следует рассматривать как отдельный проект, требующий усилий различных специалистов по сбору первичной информации, проведению оперативно-розыскных мероприятий, профилактических мероприятий, административно-процессуальных или уголовно-процессуальных действий.

5. Выполняется первичный сбор информации о каждой учетной записи, начиная сверху списка. По возможности необходимо дополнить список сведениями о личности каждого пользователя, его фактическом местонахождении, гражданстве. Эта информация может находиться непосредственно на интернет-странице информационного ресурса, где создана учетная запись. Если это не так, то требуется применение методов OSINT (англ. *Open Source Intelligence* разведка по открытым источникам). Эти методы чрезвычайно разнообразны, первичное знакомство с ними можно начать, например, с работы [4]. Впрочем и они могут не дать результатов. Параллельно со сбором информации из открытых источников могут направляться запросы к операторам социальных сетей и иных информационных ресурсов, где была размещена запрещенная информация. Следует учитывать, что зарубежные операторы информационных ресурсов на контакт с российскими правоохранительными органами практически не идут и сведений о пользователях от них получить не удастся. От отечественных операторов социальных сетей можно получить необходимые сведения о времени активности пользователя, географической привязке используемого IP-адреса и т. п.

6. По каждой записи (каждому проекту) принимается решение о необходимых мероприятиях, их последовательности, исполнителях. Осуществляются избранные действия в рамках компетенции правоохранительных органов.

По сути отработка каждой учетной записи осуществляется при таком подходе на основе сетевого графика, в котором отдельные

мероприятия могут выполняться только последовательно, а какие-то могут осуществляться параллельно.

Следует также учитывать, что отработка отдельных подмножеств проектов может давать синергетический эффект. Так, например, мероприятия, связанные с применением методов OSINT в отношении пользователей социальной сети, которые достаточно часто взаимодействуют друг с другом, а также направление запросов к операторам социальных сетей об их активности, возможно позволят в результате идентифицировать сразу несколько личностей пользователей, получить информацию об их местонахождении. На выполнение таких связанных синергичных проектов следует назначать одного исполнителя или одну рабочую группу (команду) исполнителей.

Что же касается оперативно-розыскных, следственных действий, административного преследования, то, на взгляд автора, на сегодняшний день принимаемые российским государством репрессивные меры в отношении пользователей социальных сетей непропорционально суровы относительно совершенных деяний. Кроме того, зачастую уголовные дела «за лайки» [1], становясь достоянием общественности, напротив, привлекают дополнительное внимание граждан к противоправной информации. В результате цель противодействия противоправному распространению запрещенной информации не только не достигается, но и достигается противоположная цель.

При решении прибегнуть к уголовному или административному преследованию необходимо учитывать тяжесть содеянного и различать, например, прямой призыв к насилию на религиозной почве и реакцию, оставленную под таким призывом. В последнем случае целесообразнее прибегнуть к профилактическим мерам: направлению так называемого предостережения о недопустимости распространения информации противоправного характера с обязательным упоминанием того, что реакции и комментарии на данную информацию способствуют ее распространению; профилактической беседе с участковым уполномоченным полиции и т. п. Скорее всего для большинства граждан, находящихся на территории России, такой профилактики будет достаточно для дальнейшего соблюдения законности.

Рассмотренный в настоящей работе подход к противодействию противоправному распространению информации, на взгляд автора, позволит повысить эффективность данной деятельности со стороны органов внутренних дел. Во-первых, в первую очередь будут отрабатываться те пользователи информационных ресурсов, занимающи-

еся противоправной деятельностью, которые имеют наибольший уровень влияния на аудиторию. Во-вторых, выполнение синергичных мероприятий в их отношении позволит более полно собрать сведения о фигурантах, а значит рационализировать правоохранительную деятельность. В-третьих, приоритетное разумное применение профилактических мер позволит достигать целей, поставленных законодательством, а именно препятствовать (а не способствовать) распространению запрещенной информации.

Список литературы:

1. *Николаев И.* Дело за лайк. Оштрафованный за реакции к антивоенным постам в «Одноклассниках» педагог обжаловал решение суда // Коммерсантъ (Новосибирск). № 134.

2. *Рабчевский А. Н., Рабчевский Е. А.* Оценка потенциального уровня информационного влияния пользователей в социальных сетях // Информационные системы и технологии. 2022. № 1 (129).

3. *Jackson M. O.* Social and Economic Networks. Princeton University Press. 2008.

4. *Laurent A.* OSINT Handbook: The Ultimate Guide to Open Source Intelligence Methods and Tools. Independently published. 2023.

Василий Юрьевич Федорович,
кандидат юридических наук, доцент,
заместитель начальника (по научной работе)
Московский университет МВД России
имени В. Я. Кикотя
E-mail: fevur@yandex.ru

УДК 343.98: 351.74

Аналитические технологии в решении экспертно-криминалистических задач

Аннотация

Для решения современных экспертно-криминалистических задач важным направлением является создание единой системы сбора, обработки, анализа и использования криминалистически значимой информации. Рассматриваются основные аналитические подходы к обработке выявляемой информации на примере исследования отдельных биометрических данных человека. Делается вывод, что развитие информационно-криминалистической поддержки решения задач органов внутренних дел связано с интеграцией криминалистических учетов различных направлений и информационно-аналитических систем, в том числе – открытого характера; основными перспективными технологиями сбора, накопления, аналитической обработки криминалистических данных выступают большие данные и методы искусственного интеллекта.

Ключевые слова и словосочетания: *аналитические технологии; криминалистические задачи; большие данные; искусственный интеллект.*

Период 60–70-х гг. прошлого века, характеризующийся революционным развитием новых естественнонаучных направлений, отразился и на деятельности по раскрытию, расследованию и предупреждению преступлений, поиске качественно новых путей совершенствования информационно-аналитического обеспечения указанных социально-правовых процессов.

Основная тенденция в этом направлении остается связанной с созданием *единой системы сбора, обработки, анализа и использования криминалистически значимой информации*.

Как известно, криминалистически значимая информация объединяет сведения (данные), позволяющие упорядочить, внести ясность в процессы раскрытия и расследования преступлений [1, с. 368; 3, с. 237]. Ее основные составляющие: отражение доказательств (*доказательственная*) и информационное представление из различных источников (*ориентирующая*).

Ориентирующая информация используется для выдвижения версий, определения направления расследования, планирования следственных действий, прогнозирования возможной линии поведения участников расследования [4, с. 31]. Важна ее роль в оценке оперативной значимости и доказательственного значения информационных связей, выявленных в процессе поиска в сети Интернет, и сопоставления их с данными криминалистических учетов.

В криминалистически значимой информации принято выделять два аспекта [2]. В первом она предстает как *актуальная* совокупность первичных данных и выводов о событии преступления, лицах, причастных к его подготовке и совершению, их мотивах, связях, орудиях преступления, способах его совершения, свидетелях и т. д.

Второй аспект имеет *потенциальное* значение. Он представляется справочной, ориентирующей, разведывательной информацией, которая может и не иметь существенных причинно-следственных связей с событием преступления, однако способствует решению диагностических, классификационных, идентификационных задач, позволяет скорректировать мнение о взаимосвязи комплекса данных о криминальном событии, причинах и условиях его возникновения.

По мнению М. В. Салтевского, содержание этого понятия в *узком смысле* охватывает теоретические основы возникновения следов преступления, практические методы и средства использования их для раскрытия, расследования, а также *предупреждения преступлений (курсив наш. – В. Ф.)* [8, с. 143].

При этом она может быть первичной – исходной, и вторичной – обработанной, проанализированной, систематизированной, обобщенной (в том числе на основе применения программных средств обработки данных, технологий искусственного интеллекта, экспертного оценивания). В процессе документирования происходит преобразование информации: она физически фиксируется на материальном носителе и тем самым обособляется от своего создателя.

Существенна роль криминалистически значимой информации в процессе доказывания, поскольку:

– она определяет предметы, факты, информационные связи, которые впоследствии могут стать доказательствами;

– включает сведения, которые, даже будучи изначально ориентирующими, разведывательными, потенциально представляют собой содержание доказательств;

– указывает на людей, события и иные объекты, находящиеся в криминалистических учетах и других информационных банках данных, а также мониторинговые сведения из социальных медиа, которые становятся источниками доказательств.

Типичными источниками криминалистически значимой информации являются:

– протоколы следственных действий (допросов, осмотров, обысков, выемок) и материалы доследственных проверок (объяснения, справки и т. д.);

– заключения судебных экспертов и специалистов;

– данные оперативно-справочных, криминалистических, розыскных и экспертно-криминалистических учетов;

– данные из источников информации в сети Интернет;

– материалы оперативно-розыскной деятельности.

Основные примеры экспертно-аналитических технологий

В последнее время особое значение приобретают данные из открытых источников, включая сеть Интернет. В частности, это данные информационных агентств, государственных органов, из многочисленных банков данных, от пресс-служб, журналистов и редакторов, а также различных общественных организаций, предоставляющих услуги мониторинга информации в сети Интернет.

Использование открытых (общедоступных) источников информации является самым емким каналом ее получения. Действительно, от 80 до 95 % всей интересующей информации можно получить из указанных источников. Исходя из этого, логично стремиться к интеграции экспертно-криминалистических учетов и открытых информационных источников, в частности сведений из социальных сетей в интересах расследования и предупреждения преступлений. Например, фотографии пользователей, содержание их аккаунтов и их друзей, структуру социальных групп, фактографические данные о местах учебы, службы, работы и многое другое.

Исследуя социальные группы и сообщества, появляется возможность определения связей между лицами и оцениваемыми объектами, которые обычно непросто выявлять в оперативном режиме. Можно также определить статус, положение и род занятий объекта оперативного интереса, что необходимо для составления его «цифрового портрета». Кроме того, проведение анализа аккаунтов может позволить получить сведения о семье, работе, геолокации объекта (путешествия, командировки, посещение определенных террито-

рий), что значительно облегчает аналитическую работу по сопоставлению фактов.

Для понимания имеющихся возможностей для сбора криминалистически значимой информации следует указать на доступные источники в виде официальных государственных органов Российской Федерации. Это налоговые инспекции, суды, аппарат судебных приставов; службы государственной регистрации, кадастра и картографии; ГИБДД МВД; нотариальная палата.

При использовании в процессе доказывания информация насыщает следствие фактами о главных и сопутствующих событиях, об источниках этих фактов, указывает на сведения, которые могут стать доказательствами, на их источники, а также на наиболее рациональные тактические приемы их получения.

Информация, зафиксированная на материальном носителе, в том числе взятая из открытых источников или полученная из криминалистических учетов, позволяет на стадии предварительного следствия или судебного рассмотрения дела не только однозначно установить происхождение, но и доказать ее достоверность. Информация в ходе следственных или судебных действий может быть подвергнута проверке на аутентичность, а материальный носитель передан для проведения соответствующей судебной экспертизы.

Развитие информационных технологий привело к тому, что некоторые ранее недоступные операции с компьютерной информацией стали осуществляться неограниченным кругом пользователей вследствие распространенности различных специализированных приложений. Так, не составляет труда проверить целостность и аутентичность файла, например, фото- и видеоизображений путем сравнения хэш-кодов (контрольных сумм) проверяемого файла и значения хэш-кода, заявленного владельцем информации.

Отмеченные особенности формирования и использования криминалистически значимой информации являлись предметом ряда исследований автора при обеспечении решения экспертно-криминалистических задач ОВД. Приведем некоторые полученные результаты методологического характера, выделив при этом их информационно-аналитическую направленность.

Дактилоскопическая информация

Вначале отметим одну из ранних авторских работ, посвященную организационным и научно-техническим основам использования автоматизированных дактилоскопических идентификационных систем в раскрытии и расследовании преступлений [8]. Особенностью решения проблем использования криминалистически значимой информации в указанной работе послужило раскрытие

возможностей моделирования, а также интеграция этого метода с новыми математическими методами и информационными технологиями.

В вопросах развития дактилоскопической идентификации автором предложен ряд новаций, методов и рекомендаций, которые подтвердили корректность выдвинутых гипотез и направлений решения научно-практических задач исследования. Результаты успешно внедрены в деятельность экспертно-криминалистических подразделений ОВД.

В методологическом плане ключевыми направлениями выступили следующие.

1. Изложены подходы для создания тестового массива, позволяющего исследовать возможности автоматизированных дактилоскопических идентификационных систем (АДИС), а также принципы создания коллекции следов (отпечатков) рук, систематизированных по криминалистически значимым признакам следообразования, хранения, изъятия, обработки дактилоскопической информации. В последнем случае на основе обобщения экспертной и судебно-следственной практики разработана методика определения уровня искажений, воспроизведения типов и степени деформации следов рук для получения статистически значимой выборки.

2. В области развития моделей для решения задач криминалистической идентификации показано два направления: первое связано с моделированием искажений папиллярных узоров в следах рук, второе – отражает работу по созданию и внедрению моделей в управленческую деятельность ОВД.

Применительно к дактилоскопической идентификации проведены исследования по созданию комплекса дактилоскопического назначения для решения поисковых и идентификационных задач на региональном и районном уровнях; осуществлено изучение статистических данных о следовоспринимающих объектах, встречающихся при осмотрах мест происшествий, механизме и условий образования на них следов рук.

Как результат внедрения таких передовых технологий применительно к дактилоскопии упрощается реализация возможности качественного анализа взаимного расположения признаков следов с наибольшим учетом индивидуальности, проведения сравнительного исследования условно-пригодных следов и оттисков; изучения без первичных источников (документов), т. е. используя только цифровые изображения дактилоскопической информации; наглядного оформления результатов для участников уголовного процесса [10].

В любом случае полученные результаты могут стать полезными многим сотрудникам ОВД, заинтересованным в них как в источнике криминалистически значимой информации. В этом автор видит основу создания технологии *криминалистической превенции* или предупреждения преступлений.

Следует особо подчеркнуть, что наличие таких технологий активизирует интеграцию применения криминалистических учетов и информационно-аналитических систем [5].

Информация о письменно-двигательном навыке человека

Данному направлению, составляющему треть всех криминалистических исследований в стране, посвящен ряд работ с участием автора. Процедуры проведения почерковедческой диагностики и идентификации связаны с применением современных математических методов и моделирования, а в последнее время – с внедрением технологических новинок, компьютерных достижений, технологий искусственного интеллекта и больших данных.

На основе систематизированного материала о зарубежном и отечественном становлении почерковедения и почерковедческой экспертизы обозначены организационно-правовые основы применения интеллектуальных систем в этих смежных научных сферах, что расширило представление о научно-прикладном понимании криминалистической идентификации почерка человека. Это нашло отражение в работе [12].

История указанных научных дисциплин в разные периоды своего развития связана с теоретическими и практическими достижениями каллиграфии, приметоописания (сигналитики), графометрии, графологии, методами моделирования, вероятностно-статистическими методиками распознавания образов.

Важной тенденцией стало поддержание идей интеграции перспективных методов и подходов, отражающих результаты различных наук, в том числе медицины, психологии и физиологии. Одним из революционных шагов стало обращение к компьютерным технологиям обработки почерка человека.

Естественно, что поиск путей совершенствования продолжается. Наиболее перспективным видится применение технологий искусственного интеллекта. К сегодняшнему дню подробно рассмотрены возможности использования в судебном почерковедении *ДСМ-метода* (в честь английского ученого Джона Стюарта Милля), связанного с автоматическим порождением гипотез [7]. Развитие ДСМ-метода позволило проводить интеллектуальный анализ данных, использующий алгоритмический принцип – «структурное сходство объектов влечет сходство их свойств». Указанный

подход позволил не только выдвигать гипотезу об авторе почерка, но и давать объяснение процессу ее формирования [6].

Для расширения теоретических представлений о судебно-почерковедческих экспертизах рукописей иноязычного состава, которые недостаточно разработаны в научном и практическом аспектах криминалистических исследований, изучены графические особенности систем этнического письма и подготовлены соответствующие методические рекомендации.

Для решения данной проблемы использован комплекс современных достижений судебной экспертологии и языкознания, а также математических методов определения тесноты связей анализируемых почерковедческих явлений. В работе обращено внимание на экспертную трактовку понятия «письмо» с учетом особенностей судебно-почерковедческого исследования рукописей иноязычного состава, внедрения в криминалистическую сферу лингвистических данных о национальных языках и письменных явлениях, установление их корреляционной связи со структурой и механизмом функционирования письменного функционально-динамического комплекса [11].

Информация о внешности человека

Сегодня следственно-оперативная деятельность связана с разнообразием информации о внешности человека, размещенной в информационных системах. Появление объектов, содержащих информацию о внешности человека в различных форматах представления, вызывает необходимость новых решений и в криминалистической практике.

Интеграция многих научно-технических направлений позволяет в полной мере реализовать принципы судебно-экспертной деятельности. При этом, наряду с соблюдением прав и свобод человека и гражданина, необходима объективность, всесторонность и полнота исследований, проводимых с использованием современных достижений науки и техники. Интеграция в криминалистике предполагает объединение знаний из различных областей науки и техники. Оно нацелено на решение главной задачи – создания и применения передовой методики судебно-портретных экспертиз и исследований. Интеграция в габитоскопии как научном познании внешности человека также рассмотрены в статье, посвященной этой проблематике [9].

Объектами портретных исследований являются объективные отображения внешнего облика человека (фото- и видеоизображения, зафиксированные на различных носителях информации). Для решения вопросов, поставленных перед экспертом по существу, необходимо владеть навыками фото- и видеофиксации объектов,

которые, в свою очередь, основаны на оптике, проективной геометрии, физике электромагнитных колебаний и других областях научного знания.

В портретной идентификации традиционно применяются следующие методы исследования: визуальный, линейных и угловых измерений, графический, совмещения изображений, фото-аппликация, координатных сеток. Сейчас находят все большее применение технологии, направленные на распознавание лиц. Эти технологии можно разделить на два класса.

Первые способны распознавать лица в автоматическом режиме и как результаты экспертиз могут ориентировать на выдвижение экспертной гипотезы. Эксперт далее только подтверждает или опровергает решение, предложенное системой. Результат распознавания в этом случае зависит от качества исходных фото- и видеоматериалов; выбора исходных биометрических признаков лица; методов и критериев, используемых для распознавания. К числу применяемых математических моделей относят методы корреляционного анализа, дискриминантного анализа, нейронных сетей, машинного обучения.

Второй класс систем объединяет аппаратно-технические комплексы, имеющие измерительный 3D-модуль и модуль обработки и сравнения с помощью систем искусственного интеллекта. В их работе используются принципиально другие программно-технологические решения к выделению идентификационных признаков. Они воспроизводят по своему внешнему представлению мыслительную деятельность человека.

Приведенные примеры выявления криминалистически значимой информации в ходе расследования и предупреждения преступлений свидетельствуют о необходимости развития теоретических и прикладных аспектов аналитических технологий, применяемых в решении экспертно-криминалистических задач.

В качестве общего вывода статьи выступают два положения.

1. Развитие информационно-криминалистической поддержки решения задач, направленных на раскрытие, расследование и предупреждение преступлений, связано с интеграцией криминалистических учетов различных направлений и информационно-аналитических систем, в том числе открытого характера.

2. Основными перспективными технологиями сбора, накопления, аналитической обработки криминалистической информации в задачах уголовного судопроизводства выступают большие данные и методы искусственного интеллекта.

Список литературы:

1. *Аверьянова Т. В. [и др.].* Криминалистика: учебник для вузов / под ред. проф. Р. С. Белкина. 2-е изд. перераб. и доп. Москва: НОРМА, 2003. 992 с.

2. *Белкин Р. С. [и др.].* Криминалистика: учебник для вузов / под. ред. Р. С. Белкина. Москва,1999. 928 с.

3. *Белкин Р. С.* Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Москва: Норма, 2001. 240 с.

4. Криминалистика: учебник / отв. ред. Н. П. Яблоков. Москва: Юристъ, 2000. 371 с.

5. *Минаев В. А. [и др.].* Противодействие экстремистской идеологии в социальных медиа: монография / под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: ДВЮИ МВД России, 2023. 232 с.

6. *Охлупина А. Н., Федорович В. Ю.* Подготовка базы данных для проведения идентификационных почерковедческих исследований с применением ДСМ-метода автоматического порождения гипотез // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы. Москва: Московский университет МВД России имени В. Я. Кикотя, 2017.

7. *Проткин А. А., Федорович В. Ю., Устинов В. В.* Организационно-правовые основы применение интеллектуальных систем в почерковедении и почерковедческой экспертизе: учебное пособие. Москва: Московский университет МВД России имени В. Я. Кикотя, 2015. 84 с.

8. *Салтевский М. В.* Криминалистика. В современном изложении юристов. 1996. 432 с.

9. *Федорович В. Ю.* Интеграция в габитоскопии // Вестник экономической безопасности. 2020. № 2.

10. *Федорович В. Ю.* Организационные и научно-технические основы использования автоматизированных дактилоскопических идентификационных систем в раскрытии и расследовании преступлений: дис. ... канд. юрид. наук. Москва, 2000. 24 с.

11. *Федорович В. Ю., Бобовкин А. М.* Языковая обусловленность структуры письменного функционально-динамического комплекса навыков // Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Москва: Московский университет МВД России имени В. Я. Кикотя, 2022.

12. *Федорович В. Ю., Химичева О. В., Андреев А. В.* Внедрение технологий информатизации и искусственного интеллекта как перспективных направлений развития современного уголовного судопроизводства // Вестник МОСУ МВД России. 2021. № 2.

Андрей Владимирович Шипулин,
начальник ФКУ «НИЦ «Охрана» Росгвардии
E-mail: anshipulin@yandex.ru

УДК 342.723

Перспективы использования современных технических средств безопасности в правоохранительной деятельности

Аннотация

В статье рассмотрены перспективы использования современных технических систем безопасности, в том числе с использованием технологий искусственного интеллекта, в правоохранительной деятельности по обеспечению имущественной безопасности граждан и охраны общественного порядка.

Ключевые слова и словосочетания: *системы безопасности; технические средства охраны; видеоаналитика; аудиоаналитика; безопасность; искусственный интеллект.*

Ощущение безопасности – одна из основных человеческих потребностей, которая формируется в обществе на грани инстинктивного и сознательного. Любой контакт или возможную угрозу, связанную с природными или социальными явлениями, каждый человек сознательно или интуитивно оценивает с точки зрения возможных опасностей и обеспечения безопасности [1–3].

При этом безопасность в современных условиях зависит от конкретного человека все меньше и меньше, и все больше прослеживается ее зависимость от системы безопасности социального субъекта и системы управления ею. Уменьшение вероятности воздействия криминальных вызовов и угроз разного рода, опасных факторов на общество и граждан должно обеспечиваться совершенствованием системы управления безопасностью.

С точки зрения обеспечения безопасности, очевидно, что главным будет являться достижение и сохранение как в государстве, так и в его субъектах, территорий (республики, края, области) устойчивого социального порядка, социальной и политической стабильности, развития духовного потенциала и поддержания приемлемого экономического состояния общества. В этом процессе система безопасности общества от вызовов и угроз преступности будет играть существенную роль. При этом, говоря о системе борьбы с преступ-

ностью и соблюдения принципа неотвратимости ответственности за совершенные деяния, нельзя забывать о компонентах профилактики и предупреждения преступных проявлений, что на современном этапе выступает ключевым фактором в правоохранительной деятельности.

Бесспорно, что в настоящий момент одними из основных компонентов в этой сфере являются меры профилактики и предупреждения преступных проявлений с использованием современных технических средств безопасности. При этом, наряду с уже ставшими традиционными техническими средствами охраны (средства обнаружения проникновения в охраняемые зоны), системами централизованной охраны (использующими различные каналы связи для передачи информации от охраняемых объектов на единый центр управления), находят применение системы с использованием технологий искусственного интеллекта, виртуальной и дополненной реальности, раннего обнаружения противоправных действий, аудио- и видео- аналитики окружающей обстановки.

При этом в системы управления на различных уровнях внедряются средства ситуационного прогнозирования. Происходит интеграция элементов технических средств обнаружения робототехнических комплексов и средств противодействия им в структуру современных систем обеспечения безопасности.

С учетом новых угроз безопасности в нашей стране одной из актуальных проблем является проблема противодействия беспилотным воздушным судам и иным робототехническим комплексам (далее – РТК) [4].

Несмотря на разработку большого количества систем противодействия, основными проблемами остаются:

– высокая стоимость развертывания и эксплуатации данных систем;

– малая эффективность по отношению к вновь разрабатываемым РТК (сложно достижимая и практически невыполнимая задача по созданию универсальных систем противодействия);

– недостаточная проработка вопросов способов противодействия РТК (правовая (кто может и где) и организационная (кто принимает решение о противодействии).

При этом несмотря на то что в соответствии с Федеральным законом от 4 августа 2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» определены субъекты, имеющие полномочия для осуществления противодействия РТК, эти полномочия могут быть использованы только при охране объектов, для которых установлены требования по анти-

террористической защищенности. Кроме того, в настоящее время до конца не проработан вопрос о территориальных границах зон безопасности, в которых допускается оказывать противодействие РТК. Противодействие, осуществляемое непосредственно в зоне размещения объекта, недостаточно эффективно и несет дополнительные риски.

Выскажу мнение, что основной проблемой противодействия РТК является отсутствие единой государственной системы противодействия данной угрозе. Системы противодействия устанавливаются хаотично, бессистемно и никаким образом не взаимодействуют между собой. Представляется очевидным, что если это проблема системная и актуальная для государства, то нужно применять комплексные меры, разрабатывать правила взаимодействия существующих систем, определять концепцию построения единой системы с учетом территориального распределения ее компонентов. При этом должны быть определены уровни применения; оптимизирована система управления и принятия решений.

Важным проблемным вопросом является отсутствие единого координирующего органа власти, отвечающего за государственную политику в отрасли технического регулирования современных технологий, применяемых в системах безопасности. Здесь уже имеется опыт белорусских коллег.

В соответствии с законом от 8 декабря 2006 г. № 175-З «Об охранной деятельности в Республике Беларусь» при Министерстве внутренних дел Республики Беларусь создан специальный орган охраны в сфере охранной деятельности.

В соответствии с данным Законом специальный орган охраны в сфере охранной деятельности:

– разрабатывает и осуществляет меры, направленные на реализацию государственной политики;

– обеспечивает соблюдение технических требований в сфере проектирования и производства средств и систем охраны, а также осуществляет контроль за их внедрением и эксплуатацией.

Кроме того, помимо имеющихся в настоящий момент организационных проблем, существуют проблемы отсутствия правовой регламентации использования и применения всех вышеобозначенных современных технических средств безопасности в правоохранительной деятельности.

Современные технологии привнесли в нашу жизнь как несомненные преимущества, так и дополнительные угрозы безопасности, противостоять которым возможно, только используя те же самые технологии в правоохранительной деятельности.

Поэтому в настоящее время для повышения эффективности деятельности правоохранительных органов необходимо[1]:

– использовать новые подходы и современные технологии в технических средствах безопасности (в том числе с использованием технологий искусственного интеллекта), осуществлять проработку алгоритмов их использования, в целях повышения ответственности руководителей за действия или бездействие при их применении;

– внедрять аналитические системы оптимизации принятия управленческих решений при управлении системами безопасности различного уровня, в том числе обеспечивать передачу информации и функций управления на вышестоящие уровни, сохраняя при этом оперативность получения информации и управляемость сил и средств;

– формировать необходимые нормативные правовые акты, разрабатывать и принимать целевые программы, новые формы взаимодействия между государственными организациями и субъектами негосударственных форм собственности, имеющих технические средства безопасности.

Современный механизм управления должен учитывать два основных базовых положения для единства системы безопасности. С одной стороны, это использование возможностей имеющихся систем безопасности негосударственных субъектов в рамках социально-политической консолидации общества, с другой – использование эффективных механизмов государственного управления в правоохранительной деятельности. Только партнерство государства, общества и предпринимательских структур способно обеспечить желаемый уровень безопасности от угроз преступности в стране. При этом создание на государственном уровне системы управления, включающей в себя интеграцию всех технических средств безопасности, применяемых всеми субъектами, позволит более эффективно использовать их и поднимет на новый уровень безопасность общества и граждан.

Список литературы:

1. *Амельчакова В. Н., Суслова Г. Н.* Общественная безопасность как составляющая национальной безопасности государства: сбор-

[1] Перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта», состоявшейся 24 ноября 2023 г. URL: http://www. http://www.kremlin.ru/acts/assignments/orders/73282 (дата обращения: 02.04.2024).

ник по материалам II Международной научной конференции. Краснодар, 2018.

2. *Безруков А. В.* Конституция российской федерации как ценность общественно-правового развития. Москва, 2014. № 4.

3. *Гиммельрейх О. В.* Республиканская система мониторинга общественной безопасности в системе организационных средств охраны общественного порядка и безопасности // Вестник Академии МВД Республики Беларусь. 2020. № 1 (39).

4. *Прошутинский Д. А.* Основные направления развития технологий искусственного интеллекта в технических средствах обнаружения: сборник по материалам Международной научно-технической конференции «Системы безопасности». Воронеж, 2021. № 30.

ДЛЯ ЗАМЕТОК

Научное издание

ИНФОРМАТИЗАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник трудов
Международной научно-практической конференции

Статьи публикуются в авторской редакции
Корректура: *А. А. Трегубова*
Верстка *С. Н. Портновой*

Подписано в печать 15.07.2024. Формат 60×84 $^{1}/_{16}$.
Усл. печ. л. 19,3. Уч.-изд. л. 15,3. Тираж 98 экз. Заказ № 27у.

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России
125171, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907721-31-9