Министерство внутренних дел Российской Федерации
Академия управления

Искусственный интеллект (большие данные) на службе полиции

Сборник статей
международной научно-практической конференции
(28 ноября 2019 г.)

Москва • 2020

Об издании 1, 2, 3

ISBN 978-5-907187-42-9

Содержание

Одобрено редакционно-издательским советом
Академии управления МВД России

УДК 351.754.1:519.715
ББК 67.4/67.9стд1-5:16.632
И86

Рецензенты: *Н. М. Дубинина,* начальник кафедры информатики и математики Московского университета МВД России им. В. Я. Кикотя, кандидат юридических наук, доцент; *К. Х. Асланов,* заместитель начальника СУ УМВД России по г. Тольятти.

Искусственный интеллект (большие данные) на службе полиции [Электронный ресурс]: сборник статей международной научно-практической конференции. Электронные текстовые данные (3,66 Мб). М. : Академия управления МВД России, 2020. 1 электр. опт. диск (DVD-R): 12 см. Систем. требования: процессор Intel с частотой не менее 1,3 ГГц; ОЗУ 512 Мб; операц. система семейства Windows; Adobe Reader v. 4.0 и выше; дисковод, мышь. Загл. с экрана.

И86 ISBN 978-5-907187-42-9

Стремительная цифровизация практически всех сфер человеческой деятельности в последние годы сопряжена с развитием и внедрением в эту деятельность различных информационных технологий и систем, способных частично или полностью реализовывать когнитивные и аналитические функции, ранее присущие исключительно людям, а также с ростом количества данных, которые характеризуют результаты деятельности людей и требуют анализа для принятия своевременных и взвешенных управленческих решений. Перед человечеством сегодня стоит проблема больших данных, связанная с необходимостью выработки подходов к их анализу, создания методов, технологий и систем обработки данных. Такие технологии и системы сегодня принято обобщенно относить к искусственному интеллекту.

Не подлежит сомнению, что в деятельности МВД России существует большое количество задач, при решении которых применение технологий и систем искусственного интеллекта не только оправдано огромными объемами подлежащих обработке данных, но и необходимо, позволяя существенно повысить эффективность и качество получаемых результатов.

Вместе с тем на сегодняшний день применение в деятельности МВД России технологий и систем, относящихся к искусственному интеллекту, носит фрагментарный, несистематизированный характер. Не вполне проработанными остаются правовая база и основные направления развития систем искусственного интеллекта в деятельности МВД России, равно как и общие вопросы информатизации правоохранительной деятельности.

Работы, включенные в настоящий сборник, преимущественно направлены на решение проблем концептуализации внедрения информационных технологий в правоохранительную деятельность, на решение вопросов использования искусственного интеллекта в деятельности МВД России.

Систем. требования: процессор Intel с частотой не менее 1,3 ГГц; ОЗУ 512 Мб; операц. система семейства Windows; Adobe Reader v. 4.0 и выше; дисковод, мышь. Загл. с экрана.

УДК 351.754.1:519.715
ББК 67.4/67.9стд1-5:16.632

Об издании 1, 2, 3

Содержание

Электронное издание создано при использовании программного обеспечения:
Adobe Acrobat Reader
Объем издания 3,66 Мб

Дата подписания к использованию: 03.12.2020
Тираж 10 эл. опт. дисков.

Редактор *Э. А. Циткилова*

Федеральное государственное казенное образовательное учреждение высшего образования
«Академия управления МВД России»
125993, ул. З. и А. Космодемьянских, д. 8
Тел. 8 (499) 745-82-55

E-mail: mvd.akademy@yandex.ru; press_akadem@mvd.gov.ru; https://а.мвд.рф

ISBN 978-5-907187-42-9

Содержание

В. А. АПУЛЬЦИН,
доцент кафедры информационных технологий,
кандидат физико-математических наук
(Академия управления МВД России)

М. В. СМИРНОВ,
старший преподаватель кафедры информационных технологий,
кандидат технических наук
(Академия управления МВД России)

Методы интеллектуального анализа данных трансграничных пассажиропотоков в интересах борьбы с противоправной деятельностью

Интенсивный трансграничный пассажиропоток является характерной особенностью современного мира и поддерживается такими условиями, как мобильность населения и развитая транспортная инфраструктура. Однако в России присутствует еще несколько немаловажных факторов, способствующих этому явлению. Россия имеет границы с 18 странами, это наибольшее число в мире. Протяженность государственной границы России составляет более 60,9 тыс. километров. Другим фактором является низкая в последние годы рождаемость и восполнение возникшей естественной убыли населения за счет интенсивного притока мигрантов. Основные причины такой миграции – экономические, так как мигранты, выгодно предлагая себя на рынке труда, занимают оставленные коренным населением рабочие места.

Факторами миграционной привлекательности России на протяжении последнего десятилетия остаются устойчивое социально-экономическое положение, сохранение исторических и культурных связей народов государств – участников Содружества Независимых Государств, взаимные безвизовые поездки, учреждение Евразийского экономического союза.

В 2012−2017 гг. миграционный приток в Российскую Федерацию компенсировал естественную убыль населения и стал источником дополнительных трудовых ресурсов для национальной экономики [1]. По оценкам Росстата, численность постоянного населения России в 2018 г. по сравнению с 2017 г. уменьшилась на 99 тыс. и на 1 января 2019 г. составила 146 781 тыс. В то же время миграционный прирост в 2018 г. составил 101 267 человек [2]. Ожидается, что в ближайшие годы приток мигрантов в Россию будет только усиливаться, что, в свою очередь, станет причиной увеличения трансграничного пассажиропотока.

К сожалению, высокий уровень миграции представляет собой определенную опасность для государства. Обостряются угрозы, связанные

с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности [3].

В этих условиях возрастает роль органов государственной власти по управлению миграционными потоками, профилактике правонарушений и преступлений, борьбе с преступностью. Обеспечить такое управление возможно с помощью применения современных методов и моделей анализа данных о трансграничном пассажиропотоке. Учитывая высокий уровень автоматизации и информационного обеспечения современных пунктов пограничного контроля, можно с уверенностью отнести эти данные к «большим».

Миграционный учет иностранных граждан осуществляется при въезде и выезде, транзитном проезде, выборе и изменении места пребывания или жительства. Фиксация этих фактов проводится в электронном виде с использованием Государственной информационной системы миграционного учета (ГИСМУ). Ежегодно в ГИСМУ выполняется до 70 млн регистрационных действий при осуществлении миграционного учета иностранных граждан и лиц без гражданства.

Данные о трансграничном пассажиропотоке разнородны, так как хранятся в различных информационных системах. Для анализа данных, как правило, используются специализированные информационные системы, способные работать с данными разного формата (текстом, электронными таблицами, базами данных), однако предъявляющие свои требования к организации данных и преобразующие их к собственному формату.

Таким образом, процесс анализа данных в самом общем виде состоит из двух этапов – сбора и предварительной обработки данных из разнородных источников, анализа в специализированном программном обеспечении.

На этапе сбора и предварительной обработки определяются источники данных, изучается их структура и возможность выгрузки данных в требуемом для аналитической системы формате. Затем данные очищаются от всего ненужного для анализа, например дублирующих записей, при необходимости приводятся к нужному формату и виду, подходящему для загрузки в аналитическую систему, подбираются модели, наилучшим образом подходящие для полезного представления данных.

На этапе анализа осуществляется импорт данных в аналитическую систему, к реальным данным применяются аналитические модели, позволяющие наилучшим образом представить результат импорта, рассчитываются параметры аналитических схем и их объектов (число объектов, наиболее важные объекты, связи объектов и т. д.).

Наиболее популярным форматом обмена данными в современных информационных системах является XML-формат. Кроме того, информационные системы могут обмениваться данными в формализованном текстовом формате. Примером обмена данными между приложениями является обмен формализованными сообщениями о результатах проверки паспортов

пассажиров по базам данных Интерпола, возникающий в ходе взаимодействия информационных систем программно-технического комплекса «Розыск-Магистраль», сервиса информационно-аналитического обеспечения деятельности Интерпола (СОДИ), единой системы информационно-аналитического обеспечения деятельности МВД России и информационной системы Генерального секретариата Интерпола «Ай-Линк» (I-Link).

Анализ содержащихся в упомянутых и других информационных системах разнородных данных авторами предлагается осуществлять в несколько этапов. На первом этапе предлагается привести данные к единому виду посредством получения выгрузки в формализованном текстовом или XML-формате. На втором этапе используется логико-аналитическое программное обеспечение с применением моделей данных, разработанных для целей криминального анализа и позволяющих наглядно отображать табличные данные о пассажиропотоке и отражать динамику анализируемых событий.

Авторами использовалось логико-аналитическое программное обеспечение в составе модуля «Лис-М» производства российского разработчика НТЦ «Вулкан» [4].

Для анализа имеющихся тестовых данных применялись два основных типа моделей данных – графовая модель и модель с использованием временных диаграмм «лента событий».

Графовые модели используются в криминальном анализе [5] и позволяют применить различные варианты размещения вершин и связей, например размещение с минимальным числом пересечений связей. В графовых моделях возможно также применение алгоритмов расчета важности вершин и связей, поиска кратчайших путей между объектами и т. д. (рис. 1).

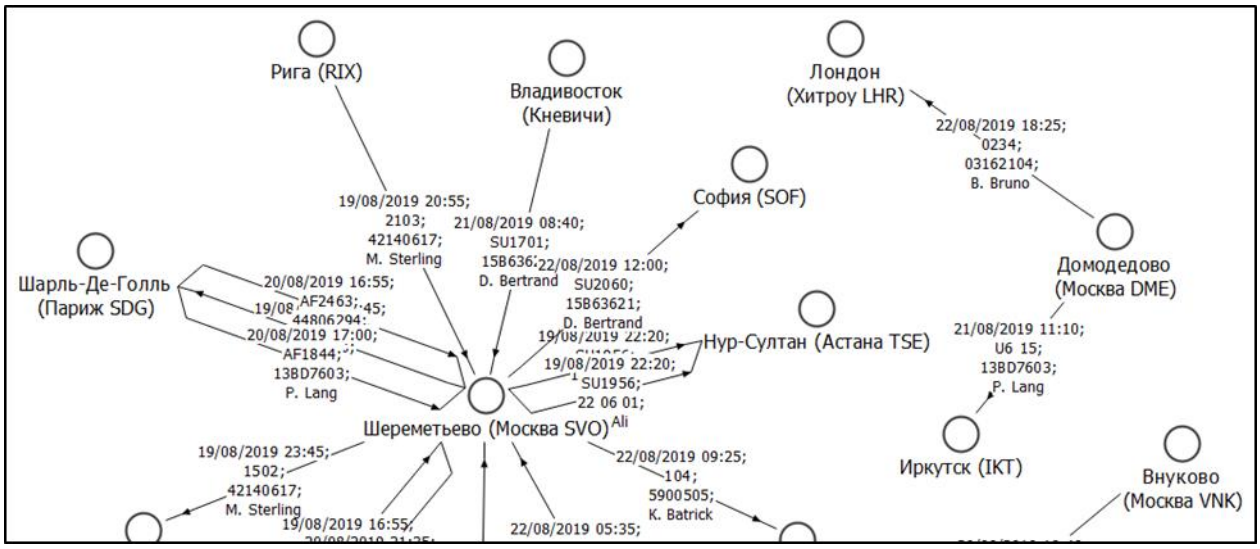

Рис. 1. Пример применения графовой модели для анализа данных о трансграничном пассажиропотоке

Временная диаграмма «лента событий» состоит из тематических линий, каждой из которых назначается своя роль, и объектов анализа, размещаемых на этих линиях со связями. Вверху временной диаграммы, как правило, располагается шкала времени (рис. 2).

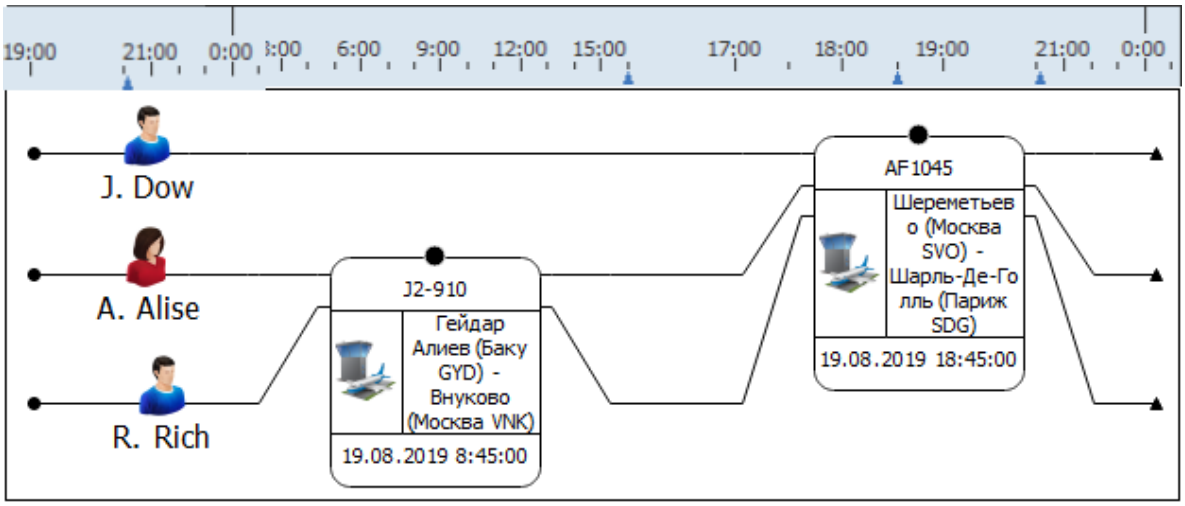

Рис. 2. Анализ динамики исследуемых событий на временной диаграмме

С изменением качественных характеристик преступности, возникновением транснациональных преступных групп возрастает значение аналитической работы. На современном этапе развития информационных технологий такую работу невозможно представить без специальных аналитических инструментов, уверенного владения методами обработки и наглядного представления результатов. Все это в полной мере относится и к задачам анализа данных о трансграничных пассажиропотоках.

Руководителям аналитических подразделений МВД России необходимо четко представлять выполняемый специалистами процесс сбора и анализа данных для решения конкретных задач. Рассмотрим кратко этапы проведения криминалистического исследования данных о пассажиропотоке с использованием современного логико-аналитического программного обеспечения.

1. Получение обращения инициатора исследования и прилагаемых носителей информации, содержащих массивы с данными о пассажиропотоке.

2. Изучение обращения инициатора, содержания следственных версий, излагаемых в нем.

3. Изучение структуры и оценка объема массивов данных на представленных носителях информации, решение вопроса о пригодности и достаточности данных для проведения исследования.

4. Запрос дополнительной информации, в случае если массивы данных в имеющемся виде непригодны к исследованию (например, отсутствует описание структуры данных) либо объем их недостаточен.

5. Техническая подготовка массивов информации к обработке с учетом требований, предъявляемых специализированным обеспечением к выходным данным.

6. Автоматизированный анализ информационных массивов с помощью специализированных логико-аналитических систем.

7. Визуализация результатов анализа в виде схем, диаграмм, таблиц. Оценка результатов анализа специалистом и принятие решения о завершении его расчетной части.

8. Подготовка отчетного документа (справки об исследовании, заключения эксперта).

Применение моделей данных о трансграничном пассажиропотоке, формируемых в разнородных информационных системах МВД России и других российских и зарубежных правоохранительных органов, позволяет использовать современные специализированные логико-аналитические системы для анализа «больших данных» трансграничных пассажиропотоков сотрудниками подразделений ОВД при осуществлении поисковой деятельности.

Список литературы

1. О Концепции государственной миграционной политики Российской Федерации на 2019–2025 годы: Указ Президента РФ от 31 октября 2018 г. № 622 // СПС «Гарант».

2. Государственная статистика. URL: www.gks.ru (дата обращения: 30.08.2019).

3. О стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 декабря 2015 г. № 683 // СПС «Гарант».

4. *Яковлев А. Н., Грачев М. Н., Шухнин М. Н. и др.* Информационно-аналитическое исследование больших массивов цифровой информации с помощью IBM i2 Analyst’s Notebook: учеб.-метод. пособие. М., 2016.

5. *Денисов В. В. и др.* Организация информационно-аналитического обеспечения оперативно-разыскной деятельности органов внутренних дел: учеб. пособие. М., 2017.

В. В. БАРАНОВ,
старший преподаватель кафедры информационных технологий
(Академия управления МВД России)

Б. А. ТОРОПОВ,
доцент кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

Технологии выявления преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации

Научно-технический прогресс, сопровождающий современное общество, стал одной из причин развития преступности, которая распространилась не только на сферу реальной жизни, но и на так называемое киберпространство. Киберпреступность обретает все новые формы и масштабы, постоянно расширяя свои границы.

В то же время преступления, совершаемые с использованием сферы телекоммуникаций и компьютерной информации, имеют высокую степень опасности, причем не только для отдельных граждан и организаций, но и для национальной безопасности любого государства в целом. Преступники, используя сеть Интернет, способны не только совершать преступления в сфере компьютерной информации, предусмотренные главой 28 УК РФ, но и получать доступ к данным, составляющим сведения, охраняемые действующим законодательством, способствовать совершению опаснейших преступлений, в том числе террористическим посягательствам на объекты жизнеобеспечения, транспорта, атомной энергетики.

Так, в ходе расследования всемирно известного теракта в центре Нью-Йорка 11 сентября 2001 г. в США был принят Закон о борьбе с терроризмом, было установлено, что разрушение башен-близнецов – лишь видимая часть теракта, в его разработке были задействованы десятки тысяч людей, находившихся в разных точках мира, а их взаимодействие осуществлялось с использованием сети Интернет [11, с. 146].

Ежегодный ущерб от киберпреступлений, по подсчетам ООН, составляет около 500 млрд дол. В России ежедневно совершается 44 хищения из банковских систем, с банковских карт и счетов. Кроме того, согласно статистике Европола большинство хакеров проживают на территории России и СНГ и не привлекаются к уголовной ответственности, так как законы данных стран об ответственности за совершение киберпреступлений недостаточно проработаны, в связи с чем применить в отношении них меры уголовно-правового характера не представляется возможным [12].

По статистическим данным, на территории Европейского союза обезврежено 3 600 преступных группировок, которые осуществляли свою деятельность в сети Интернет, однако это лишь 30 % от общего количества всех выявленных преступлений в данной сфере [13].

В настоящее время информационные системы и сети связи глубоко проникли в различные сферы общества. Сформировалось глобальное информационное пространство, без которого люди уже не представляют своей жизни [1, с. 44], а потому необходимо обеспечить безопасные условия пользования киберпространством, определить технологию выявления преступлений, совершаемых с использованием сферы телекоммуникаций и компьютерной информации.

*Под **технологией выявления киберпреступлений** необходимо понимать совокупность методов и инструментов, необходимых для выявления преступлений, совершаемых в киберпространстве.*

Основными особенностями современных информационных сетей, используемых преступниками для совершения преступления, являются:

– доступность и простота использования для практически любого пользователя;

– возможность обмениваться информацией непосредственно с конкретным человеком независимо от его местоположения;

– интернациональный характер информационного обмена, практически устранивший границы для общения, когда получение услуг осуществляется независимо от государственной принадлежности и расположения как поставщика услуг, так и их получателя [2, с. 288].

Свобода проявлений в информационном пространстве позволяет действовать дерзко и безбоязненно преступникам различных специализаций, в связи с чем возможно утверждать, что информатизация общества, обладая, несомненно, множеством позитивных качеств, привела и к информатизации криминальной среды, придала ей ярко выраженный интернациональный и высокотехнологичный характер.

Лица, склонные к совершению вышеуказанных преступлений, используют возможности информационно-телекоммуникационных систем, что способствует расширению транснационального масштаба, и в конечном итоге создают угрозу национальной безопасности. События, произошедшие в таких странах, как Грузия, Ирак, Иран, Ливия, Сирия, Турция, Украина, показали эффективность использования информационных технологий для организации массовых беспорядков, агитационного воздействия на сознание людей, что в ряде случаев обеспечило переворот и захват власти радикальными силами.

Преступления, совершаемые в сети Интернет, с каждым годом становятся все более опасными, приобретая организованную форму и международный характер. Явно просматривается возможность ее использования в целях реализации международных преступлений, в том числе и террористической и экстремистской направленности.

Организованными преступными структурами широко применяются методы конспирации, информационно-телекоммуникационные системы для организации и управления преступной деятельностью, сокрытия следов преступлений.

В то же время глобальная сеть Интернет содержит значительные объемы разнообразной информации, которая может представлять интерес для оперативных подразделений ОВД. Данная информация успешно используется для решения задач ОРД, в том числе для противодействия экстремистским и террористическим проявлениям, особо опасным видам преступности, для выявления каналов движения денежных средств, полученных противоправным путем, и криминальных источников финансирования международных преступных группировок, экстремистских и террористических организаций [3, с. 240].

Необходимо отметить, что действующая законодательная и нормативная база, включая и теоретические основы ОРД, позволяет с успехом выявлять перечисленные категории преступлений в сети Интернет, осуществлять документирование преступных действий. При этом, как показывает практика, противодействие таким видам преступности, как терроризм и экстремизм, в том числе совершаемым с использованием киберпространства, невозможно без применения оперативно-разыскных сил, средств и методов [4].

Форумы, блоги и социальные сети для значительной части населения большинства стран мира стали основным способом массового общения, самоидентификации и самореализации в многоуровневой и разветвленной информационной среде пользователей и реальной жизни [5, с. 352], а также являются средой совершения преступлений, местом возможного «обитания» преступников. В зависимости от складывающейся оперативно-следственной ситуации сотрудники правоохранительных органов должны грамотно определить конкретный вид оперативно-разыскных мероприятий (далее – ОРМ), которые необходимо провести при раскрытии конкретного преступления.

Использование понятия сетевого информационного пространства дает возможность расценивать глобальные информационно-телекоммуникационные сети и как место осуществления ОРД. Однако необходимо учитывать, что место преступления как место осуществления ОРД в киберпространстве лишено пространственно-временных рамок. Действующее законодательство в принципе не предусматривает дефиниции «место совершения преступления», «место проведения ОРД», хотя законодателем четко определено понятие «время совершения преступления» [14, с. 55–56].

Вид и тактика проведения ОРМ зачастую зависят от местонахождения субъекта преступления в сетевом информационном пространстве, которое определить порой весьма затруднительно. В то же время остается открытым вопрос о юрисдикции правоохранительных органов, особенно в тех случаях, когда преступление совершается человеком, находящимся в другом государстве. Используя прокси-серверы, можно выйти в Интернет через IP

пользователя, находящегося в другом государстве. Мессенджеры «Телеграм», «Дарнет» позволяют пользователю анонимно общаться с другими соучастниками преступлений и затрудняют их раскрытие правоохранительными органами.

Таким образом, информационные технологии создают предпосылки и условия для совершения преступлений в сфере сети Интернет или с ее использованием, устойчивые предпосылки для структурной оптимизации криминальных формирований [6, с. 219]. Анализ показывает, что именно в сети Интернет формируются преступные группы, экстремистские и террористические организации [7, с. 616].

Расследование киберпреступлений предусматривает в качестве необходимого следственного действия осмотр места происшествия, т. е. рабочего места, информационных носителей. Следовательно, местом совершения преступления стоит считать физическое местонахождение компьютера, ноутбука, телефона или планшета, с которого осуществляет выход подозреваемый. Однако для киберпреступлений такой подход не применим. Они могут иметь трансграничный характер, быть совершенными посредством удаленного доступа. Информационное право, существующее как отдельная отрасль права, определяет информационное пространство как единство технической и социальной стороны (техники и пользователей), не связывая их с какой-либо территорией.

Это и определяют специфику организационно-тактических форм проведения ОРМ в борьбе как с общеуголовной преступностью в Интернете, так и с сетевыми криминальными явлениями. Особый интерес представляют ОРМ, проводимые при раскрытии террористических и экстремистских преступлений, совершенных с использованием телекоммуникаций и компьютерной информации.

Под ОРМ, проводимым в ходе раскрытия преступлений, совершенных с использованием телекоммуникаций и компьютерной информации, понимают, в соответствии с Федеральным законом «Об оперативно-розыскной деятельности», деятельность уполномоченных сотрудников оперативных подразделений, целью которых является обнаружение, документирование, соответствующее хранение и последующая реализация оперативно значимой информации, по своевременному пресечению, предупреждению, выявлению, раскрытию и успешному расследованию преступлений в киберпространстве [8].

При расследовании преступлений экстремистской и террористической направленности ОРМ могут проводиться с целью выявления в сети Интернет следующих криминогенных объектов:

– следов противоправной деятельности;

– сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений;

– ссылок на материалы, запрещенные к распространению, и т. п.

Лица, совершающие преступления экстремистской и террористической направленности, а также иные преступления с использованием возможностей

современных информационных систем, осуществляют подготовку данной категории преступлений более тщательно, так как используют в своем арсенале информационные технологии, что значительно облегчает совершение преступления, например общение между членами группы.

Пример. *Первое убийство, совершенное с использованием телекоммуникационных технологий, зарегистрировано в США в феврале 2008 г.*

Проводимые спецоперации позволили выявить организованную преступную группу террористической и экстремистской направленности, однако в ходе реализации мероприятий было совершено покушение на жизнь важного свидетеля, показания которого являлись одним из наиболее важных доказательств террористической операции выявленной группы. Принимая меры по защите жизни данного свидетеля и обеспечению его безопасности, сотрудники спецподразделений поместили его в закрытый госпиталь на территории военной базы. Однако принятые меры безопасности не увенчались успехом, поскольку преступники, получив несанкционированный доступ к телекоммуникационной сети военного госпиталя, внесли изменения в установленные временные режимы работы кардиостимулятора и аппарата вентиляции легких, к которым был подключен свидетель, что привело к его гибели.

Данный факт наглядно демонстрирует возможности использования организованной преступностью телекоммуникационных сетей не только для облегчения совершения преступления, но и для противодействия раскрытию и расследованию таких деяний.

При раскрытии и расследовании преступлений в киберпространстве у правоприменителей возникает огромное количество различных трудностей, обусловленных как объективными, так и субъективными причинами. В первую очередь это необходимость обладания достаточно высоким уровнем знаний в сфере компьютерных и информационных технологий, в сфере уголовно-процессуального законодательства, умением грамотно применять существующие законодательные нормы в практической деятельности.

Несмотря на достаточно широкое разнообразие преступных действий, которые могут иметь место в сфере телекоммуникаций и компьютерной информации, все они обладают определенными сходными чертами, что позволяет выделить некоторые **типичные следственные ситуации**:

1) нарушение целостности информационной системы либо конфиденциальности информации выявлено непосредственно ее собственником, виновный установлен;

2) нарушение целостности информационной системы либо конфиденциальности информации выявлено непосредственно ее собственником, виновный не установлен;

3) нарушение целостности информационной системы либо конфиденциальности информации выявлено правоохранительными органами либо стало общеизвестным;

4) размещение на странице пользователей, в группе или на форуме, где они зарегистрированы, аудио-, видео- и текстовых файлов, содержащих материалы экстремистского и террористического характера;

5) распространение по различным сайтам идей, пропагандирующих терроризм, экстремизм, сепаратизм и религиозную нетерпимость;

6) совершение преступлений с использованием интернет-технологий, в том числе мошенничеств, краж, грабежей и т. д.

Без сомнений, наиболее благоприятными для раскрытия и расследования преступлений являются ситуации, в которых лицо, виновное в совершении преступления, установлено. В таком случае деятельность сотрудников следственного и оперативного аппарата в основном направлена на установление обстоятельств содеянного, поиск возможных источников доказательств вины лица. Необходимыми обстоятельствами, подлежащими установлению и доказыванию, будут являться данные:

– о нарушении целостности или конфиденциальности информации в системе;

– размере ущерба, причиненного указанным преступным деянием;

– механизме преступного действия;

– об отношении виновного к совершенным действиям и наступившим последствиям;

– попытках противодействия расследованию.

При задержании виновных непосредственно после совершения преступления возможно предложить следующий алгоритм производства первоначальных следственных действий:

– личный обыск;

– допрос задержанного;

– обыски по месту жительства, работы, задержания, в иных местах пребывания;

– осмотр изъятого имущества, в том числе компьютера, смартфона, планшета и т. д.

Отметим, что по рассматриваемой категории преступлений поисковые следственные действия, к коим относятся осмотр, обыск и в определенной степени выемка, – это важнейшие инструменты получения сведений об обстоятельствах совершенного преступления, имеющих доказательственное значение, а также средства обнаружения и изъятия документов, впоследствии получающих статус вещественных доказательств. При этом следует учитывать и тот факт, что по рассматриваемой категории преступлений именно вещественные доказательства обладают наиболее важным значением, поскольку именно наличие определенных следов и предметов, раскрывающих непосредственный способ совершения преступления, позволяет наиболее полно установить обстоятельства содеянного. Однако

информационные данные не являются вещественными доказательствами, осмотру подлежат их материальные носители, а также само содержание информации.

Ведя речь о вышеуказанных следственных действиях, необходимо охарактеризовать их содержание. Так, **осмотр** – это непосредственное обнаружение, восприятие и исследование уполномоченным лицом материальных объектов, имеющих отношение к исследуемому событию. **Обыск** – следственное действие, содержание которого образует поиск и принудительное изъятие объектов, имеющих значение для расследуемого события. **Выемка** – следственное действие, направленное на изъятие значимых для расследуемого деяния объектов в случае наличия точной информации о местонахождении искомого (ст. 176, 182, 183 УПК РФ) [9].

Планируя производство поисковых следственных действий при расследовании киберпреступлений, необходимо рассмотреть вопрос о привлечении к участию в производстве следственного действия специалиста (ст. 58 УПК РФ), поскольку специфика осмотра и изъятия компьютерной техники, носителей информации нередко приводит к возникновению определенных проблем, а в ряде случаев – к допущению ошибок, ведущих к невосполнимой утрате информации, имеющей доказательственное значение.

Производя следственные действия по таким преступлениям, всегда следует учитывать возможность оказания противодействия со стороны преступников, заключающегося, в частности, и в попытках уничтожения вещественных доказательств, к примеру – с использованием специального оборудования с сильным магнитным полем, уничтожающим информацию. Путем грамотной совместной подготовки следователей и оперативных сотрудников возможно просчитать вероятность оказания такого противодействия и разработать необходимые предупредительные меры, не позволяющие злоумышленникам уничтожить следы преступления.

Также необходимо учитывать и возможности принятия преступником иных мер по перекрытию доступа к информации, способной иметь доказательственное значение по рассматриваемой категории преступлений, например установление программы, требующей введения пароля в определенное время и автоматически уничтожающей данные на магнитных носителях при невыполнении этого требования.

Все вышеуказанное свидетельствует о том, что успех поисковых следственных действий по анализируемой категории преступлений зависит не только от включения в состав их участников специалиста, но также и от оснащения сотрудников правоохранительных органов необходимым оборудованием – в частности, устройством для определения наличия и измерения магнитных полей.

При расследовании киберпреступлений необходимо не только учитывать механизм следообразования, но и осуществлять поиск иных

следов, свойственных для преступлений любой категории, в том числе следов пальцев рук на клавиатуре, иных частях компьютерной системы.

Осмотру подлежат все компьютерные устройства, средства телекоммуникационной связи.

Первоочередная задача поискового следственного действия – обеспечение сохранности всей информации, содержащейся в компьютерах и на электронных носителях, для чего необходимо:

– не допускать никого, кроме специалиста, к компьютерам и носителям информации;

– не выполнять самостоятельно никаких действий с компьютером, не будучи уверенным в том, что они не повредят информацию;

– в случае обнаружения в месте нахождения компьютерной техники и носителей информации взрывчатых, токсичных, легковоспламеняющихся и иных опасных веществ принять незамедлительные меры к их удалению из данного помещения.

Осмотры и обыски по рассматриваемому виду преступлений обладают существенной спецификой, которая в обязательном порядке должна учитываться при производстве вышеуказанных следственных действий.

Если компьютер работает, то изъятие непосредственно самого компьютерного оборудования либо имеющейся в нем информации сопряжено с существенными трудностями, в особенности если следственное действие происходит без участия специалиста. Однако, несмотря на определенные затруднения, следователем все же должны быть приняты все возможные меры с целью изъятия имеющей значение для расследования информации при соблюдении ряда рекомендаций, позволяющих предотвратить уничтожение доказательственной информации [10, с. 750].

Здесь рекомендуется использовать данный алгоритм деятельности следователя.

1. Определить программу, выполняемую компьютером, исследуя изображение на экране, детально зафиксировав его описание в протоколе.

Также целесообразно с помощью диспетчера задач (одновременное нажатие клавиш «Ctrl»-«Alt»-«Del») определить запущенные процессы на компьютере (за исключением скрытых), учитывая возможность работы программ с функцией экстренного уничтожения информации в скрытом режиме.

В ряде случаев, остановив программу и осуществив выход в операционную систему, возможно установление программы, вызывавшейся последней, с помощью функциональной клавиши «F3».

2. Остановить запущенный процесс с помощью диспетчера задач или одновременного нажатия клавиш «Ctrl»-«C» либо «Ctrl»-«Break» (для консольных приложений, поддерживающих управление командной строкой).

3. Определить наличие у компьютера внешних устройств, накопителей информации на жестких магнитных дисках и картах памяти, виртуального диска.

4. Проверить наличие внешних устройств удаленного доступа к системе, установить и зафиксировать их состояние, произвести отключение устройств, позволяющих принять меры к уничтожению информации.

5. Произвести копирование программ и файлов с помощью стандартных средств операционной системы.

6. Отключить электропитание компьютера, после чего выполнять действия в соответствии с алгоритмом, предлагаемым для неработающего компьютера.

Все перечисленные действия, производимые в ходе осмотра либо обыска, надлежит тщательно фиксировать в протоколе.

Особые меры предосторожности при изъятии носителей информации и компьютерной техники надлежит соблюдать не только при упаковке, но также и при транспортировке и хранении, не допуская возможности их механического повреждения в силу бросков, ударов, а также исключая наличие иных условий, способных нанести вред носителям информации и оборудованию, таких как излишняя влажность, перепады температуры.

Поиск информации в компьютерных устройствах, следов воздействия на нее, а также изъятие информации и следов достаточно специфичны, информация может содержаться в **оперативном запоминающем устройстве** (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и во **внешних запоминающих устройствах** (ВЗУ).

Данные из ОЗУ могут быть сохранены путем распечатки на бумагу либо фиксации специального программного обеспечения для сохранения и последующей визуализации дампа памяти.

Дамп памяти – это копия содержимого оперативной памяти, находящаяся на жестком диске или другом энергонезависимом устройстве памяти [11, с. 642].

Следует учитывать, что при создании компьютерных программ изготовителями могут быть допущены некоторые ошибки, облегчающие преступникам доступ к ПК. Порой также небрежное отношение к хранению информации может облегчить преступникам доступ к ней.

Совершая некоторые преступления, преступник может выдавать себя за законного пользователя. Такие деяния характерны при посягательстве на системы, у которых отсутствуют средства аутентичной идентификации (например, по физиологическим характеристикам, отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.). При отсутствии серьезных способов идентификации личности преступник может совершить преступление без особого сопротивления, например следующими способами:

– приобретения путем подкупа персонала списка пользователей со всей необходимой информацией;

– обнаружения данного списка в организациях, не имеющих должного контроля за его хранением;

– незаконного, несанкционированного подслушивания через телефонные линии.

Пример. *В 2014 г. в Сочи проводились зимние Олимпийские игры. Как и во всех массовых спортивных мероприятиях, была выполнена соответствующая работа по защите телекоммуникационных ресурсов, используемых в процессе проведения всех видов спортивных соревнований, оперативными подразделениями силовых структур и сотрудниками АО «Лаборатория Касперского». Телекоммуникационные ресурсы Олимпийских игр на протяжении всего периода проведения данного массового международного спортивного мероприятия ежедневно подвергались кибератакам со стороны некоторых иностранных государств. Вирусы, направленные на их срыв, своевременно выявлялись, блокировались, дробно пакетировались и отправлялись обратно злоумышленникам. В результате слаженной совместной работы соответствующих оперативных структур и сотрудников АО «Лаборатория Касперского» были предотвращены все попытки дестабилизации проведения зимних Олимпийских игр в Сочи.*

Пользователи сети Интернет нередко сталкиваются с кибермошенничеством и киберкражами, которые совершаются с использованием так называемых «бомб» – вредоносных программ. Так, «логическая бомба» при наличии определенных условий способна полностью или частично повредить систему компьютерной сети. Ее разновидностью является «временная бомба», начинающая разрушительное действие с момента достижения определенного временного периода. Суть данного метода состоит в несанкционированном проникновении вредоносных программ в уже имеющиеся и порождении абсолютно новых функций, владельцем не запланированных, но при этом не вредящих работе старых.

Таким образом, лица криминальной направленности, используя возможности вредоносных программ, перечисляют денежные суммы на свои временно открытые банковские счета.

В связи с тем, что содержание вирусной программы **в** своем текстовом обличии весьма многогранно и имеет огромное количество команд, их определение, естественно, требует большого профессионализма лиц, имеющих навыки в данной области.

Нередко преступники также используют определенные команды, которые способны при внедрении в определенные файлы (в виде текста, символов и т. д.) сформировать команду на уничтожение определенной информации. Для обнаружения вредоносных файлов необходимо найти не программу, а конкретную команду, что необходимо учитывать при осмотре устройств.

Мошенники при совершении преступлений в киберпространстве иногда используют рабочее выражение «воздушный змей». Рассмотрим конкретный пример, который визуализирует суть данного понятия.

Пример. *В нескольких банках открываются счета на небольшие суммы, осуществляются переводы из одного банка в другой и обратно с постепенным увеличением сумм. Цель такой махинации – в доставке*

информации о сумме перевода в первый банк быстрее, чем платежного поручения из другого банка, т. е. до обнаружения факта необеспечения перевода необходимой денежной суммой. Данные денежные манипуляции осуществляются неоднократно, с каждым разом увеличивая конечную сумму («воздушный змей» поднимается все выше и выше), пока на счете не оказывается приличная сумма денежных переводов, устраивающая преступников. В результате достижения преступной цели деньги с конечного счета быстро снимаются и присваиваются мошенниками, которые впоследствии скрываются.

Чем больше количество задействованных в данной афере банков, тем больше и быстрее накапливается желаемая денежная сумма, и число поручений о переводе не достигает подозрительных значений. Такой вид совершения преступления возможен только при осуществлении операций с помощью компьютера.

Далее рассмотрим основные средства совершения киберпреступлений.

1. **Вирус** – компьютерная программа, находящаяся на компьютере пользователя без его ведома и выполняющая какое-либо действие, чаще всего деструктивное (удаление, перемещение, изменение файлов).

2. **Adware** – компьютерная программа, находящаяся на компьютере пользователя без его ведома, вред которой выражается в навязчивом показе пользователю рекламы путем изменения стандартной страницы браузера, всплывающих окон, баннеров, переадресации на другие сайты.

3. **Spyware** – компьютерная программа, находящаяся на компьютере пользователя без его ведома, вред которой выражается в шпионских действиях против пользователя с целью получения паролей и иной личной информации.

4. **Удаленная атака** – это программа, осуществляющая сканирование системы на предмет открытых портов с последующим захватом контроля над вашим компьютером, что грозит финансовыми потерями, приведением в негодность операционной системы (компьютер будет под управлением других машин рассылать «спам», а трафик будет оплачиваться его пользователем).

Разновидностью являются DDoS-атаки, задача которых в том, чтобы компьютер или компьютерная сеть были недоступны пользователю этого компьютера или сети. Примером может являться одна из самых глобальных в истории DDoS атак от группы Anonymous *в* 2002 г., которая повлекла выход из строя 7 корневых DNS-серверов.

В более поздние годы такие атаки все более распространены. Так, например, 30 сентября 2013 г. хакерской группировкой Anonymous Caucasus на видеосервисе YouTube был опубликован ролик, в котором говорилось о том, что начинается новая операция против российских банков «в отместку за геноцид кавказских народов». После этого 1 октября 2013 г. совершена DDoS-атака на сайт Сбербанка, 2 октября – на сайт Альфа-банка, 3 октября – на сайты Банка России, Альфа-банка и Газпромбанка.

Нападение имело своей целью ограничить доступ к публичным сайтам банков, но данные атаки удалось отразить в кратчайшие сроки, так, например, сайт ЦБ РФ не работал лишь 7 минут [15].

24 марта 2014 г. совершена DDoS-атака на сайт Банка России, в результате чего сайт не работал с 09:45 до 11:00. Мощность данной атаки превышала пропускную способность каналов связи сайта в десять раз. 17 марта 2014 г. DDoS-атака вывела из строя сайт и интернет-сервисы банка «ВТБ-24» и интернет-сервис Альфа-банка. 2 октября 2015 г. была зафиксирована крупнейшая волна продолжительных DDoS-атак на сайты и системы онлайн-банкинга восьми крупных российских банков, при этом половине из них были направлены сообщения с требованиями заплатить выкуп в криптовалюте биткоин за прекращение атак. 8 ноября 2016 г. Сбербанком была отражена серия мощных DDoS-атак, организованных из нескольких десятков стран [16].

5. **Скимминг** – снятие информации с финансового инструмента пользователя с целью последующего хищения денежных средств и других противоправных действий.

К наиболее активным видам киберпреступлений необходимо отнести стремительно развивающийся **фишинг** – поддельные письма якобы от имени банков или платежных интернет-систем с просьбой к клиентам сообщить данные для авторизации и доступа к их персональной информации. В случае если пользователь оставляет свои данные, то они используются мошенниками для немедленного снятия с его счета имеющихся денежных средств. Данный вид мошенничества активно внедрен и применяется преступниками в сетях операторов сотовой связи.

Основными средствами идентификации и разоблачения пользователя, в том числе и киберпреступника, в сети Интернет являются его IP-адрес (уникальный адрес регистрации абонента в сети Интернет, который может быть как статическим, так и динамическим) и MAC-адрес (уникальный номер сетевого аппаратного средства – идентификационный номер, который «прошивается» в память данного устройства). Информацию об указанных данных можно получить посредством СОРМ либо напрямую у провайдера.

Так, для совершения преступлений террористической направленности необходимо значительное количество финансов. Поэтому злоумышленники используют все возможности хищения денежных средств с помощью телекоммуникаций и компьютерной информации. Таким образом, при расследовании преступлений террористической направленности необходимо проводить обыски, тщательно изучать устройства, используемые преступниками, с целью изобличения всех соучастников, поиска канала хищения и реализации денежных средств и т. д.

Таким образом, можно выделить следующие меры, направленные на **предупреждение преступлений в** сфере телекоммуникаций и компьютерной информации:

– технические;

– правовые;

– организационные.

К техническим мерам относят:

– защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем;

– организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

– установку оборудования обнаружения и тушения пожара, обнаружения утечек воды;

– принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов;

– установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Правовые меры включают:

– разработку норм, устанавливающих ответственность за преступления экстремистского и террористического характера с использованием сферы телекоммуникаций и компьютерной информации;

– введение в уголовное законодательство ряда понятий – «киберпреступление», «киберпреступность», «кибербуллинг», «кибертерроризм», пересмотр теоретиками понятия «место преступления» с учетом характеристик киберпреступлений;

– совершенствование уголовного и гражданского законодательства, а также судопроизводства. В настоящее время отсутствует документ о взаимодействии по вопросам совершения киберпреступлений. Необходимо принятие документа, регламентирующего вопросы частичного или всестороннего сотрудничества, причем не только внутригосударственного уровня, но и международного.

Организационные меры включают:

– конкретизацию целей ОРМ при расследовании преступлений в киберпространстве;

– разработку методических рекомендаций по расследованию киберпреступлений;

– оснащение правоохранительных органов специализированной материально-технической базой, обучение по профилю «противодействие киберпреступности» в вузах МВД России.

Список литературы

1. *Мельников Д. А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. М., 2015.
2. *Мирошников Б. Н.* Сетевой фактор: Интернет и общество. М., 2015.
3. *Сундиев И. Ю., Смирнов А. А., Кундетов А. И., Федотов В. П.* Теория и практика информационного противодействия экстремистской и террористической деятельности: монография. М., 2014.
4. *Потупчик К., Федорова А.* Власть над Сетью. Как государство действует в Интернете. М., 2014.
5. *Сейджман М.* Сетевые структуры терроризма / пер. с англ. И. Данилина. М., 2008.
6. Эффективные меры борьбы с транснациональной организованной преступностью // XI Конгресс ООН по предупреждению преступности и уголовному правосудию (Бангкок, 18–25 апреля 2005 г.): сборник документов / сост. А. Н. Сухаренко. М., 2008.
7. Об оперативно-розыскной деятельности: федер. закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп.) // СПС «КонсультантПлюс».
8. Уголовно-процессуальный кодекс РФ: федер. закон от 18 декабря 2001 г. № 174-ФЗ (с изм. и доп.) // СПС «КонсультантПлюс».
9. *Филиппов А. Г.* Криминалистика: учебник. 3-е изд., перераб. и доп. М., 2004.
10. *Матвеев М. Д., Юдин М. В., Прокди Р. Г.* Windows 7. Полное руководство // Наука и техника. 2012.
11. *Жестеров П. В.* Границы национального суверенитета и преступления в сфере киберпространства // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. 2018.
12. URL: https://www.mcafee.com/enterprise/de-de/assets/executive-summaries/es-economic-impact-cybercrime.pdf (дата обращения: 01.12.2019).
13. URL: https://www.europol.europa.eu/sites/default/ files/publications/ socta2013.pdf (дата обращения: 01.12.2019).
14. *Искевич И. С., Кочеткова М. Н., Попов А. М.* Актуальные проблемы определения юрисдикции при расследовании преступлений в информационном пространстве: международно-правовой аспект // Проблемы правоохранительной деятельности. 2016. № 4.
15. *Повышев В.* Борьба с киберпреступностью и кибертерроризмом. URL: http://tmun.utmn.ru/wp-content/uploads/SPChKiber.pdf (дата обращения: 01.12.2019).

16. *Дубинина Н. М.* Совершенствование управленческой деятельности органов внутренних дел на основе разработки и реализации целевых программ: методологические, методические, организационно-правовые аспекты: автореф. дис. ... канд. юрид. наук. М., 2000.

17. *Дубинин М. П., Дубинина Н. М.* Методологические аспекты постановки задачи анализа результатов деятельности органов внутренних дел // Вестник Московского университета МВД России. 2013. № 11.

18. *Егорченко И. В.* Кибертерроризм: феномен, анализ ситуации, особенности противодействия // Национальная безопасность в современной России: стратегия противодействия экстремизму и терроризму и перспективы преодоления глобальных проблем: материалы всероссийской научной конференции: в 2 т. М., 2016.

Б. О. БАТОРОВ,
слушатель 2-го факультета
(Академия управления МВД России)

Применение нейросети в интересах оценки эффективности социотехнических систем

Введение. С позиции теории менеджмента *социотехническая система* понимается как научный подход к проектированию трудового процесса в аспекте взаимодействия социума и технико-технологических факторов труда. Общество, социальные институты и их подструктуры образуют сложные социотехнические системы.

Иными словами, любая организация – это социотехническая система, состоящая из социальных и технических подсистем. Техническая подсистема включает устройства, инструменты и технологии, преобразующие вход в выход способом, который улучшает экономическую эффективность организации. Социальная подсистема включает занятых в организации служащих (знания, умения, настрой, ценностные установки, отношение к выполняемым функциям), управленческую структуру, систему поощрений.

Достичь высокой эффективности функционирования организации возможно, оптимизируя ее подсистемы и их взаимодействие – гармонизируя их работу. Взаимодействие элементов, т. е. формирование социотехнической системы как целостности, начинается тогда, когда в системе возникает неопределенность, источником которой является непредсказуемость индивидуального поведения людей и их социальной деятельности.

В своем стремлении снизить уровень этой неопределенности люди вырабатывают правила взаимодействия, и пока неопределенность относительно мала, индивидуумы регулируют взаимодействие на локальном уровне, не создавая каких-либо глобальных структур. Если же неопределенность превышает некоторое критическое значение и выходит за рамки локального взаимодействия, то урегулирование неопределенности происходит на глобальном уровне. И поэтому оценка эффективности функционирования социотехнических систем невозможна без теории экспертных систем, рассмотрение которой является целью настоящей статьи.

Современная теория экспертных систем. В последнее время наблюдается все более полное взаимное проникновение способов представления информации, методов и алгоритмов ее обработки (системы искусственного интеллекта и системы статистической обработки информации). Однако подлинным водоразделом между классической и современной теорией экспертных систем следует считать применение

интеллектуальных способов обработки данных (Data Mining). Основу методов Data Mining составляют всевозможные методы классификации, моделирования и прогнозирования, основанные на применении нейронных сетей, генетических алгоритмов, методов кластеризации, метода анализа иерархий, ассоциативной памяти, нечетких множеств. Среди статистических методов к категории Data Mining относят многомерный регрессионный анализ, факторный анализ, анализ главных компонент, дисперсионный анализ, дискриминантный анализ, анализ временных рядов. Теория нейронных сетей в последнее время интенсивно развивается благодаря универсальности общего методологического подхода к решению самых разнообразных научных и технических задач: аппроксимации кривых, классификации, кластеризации, фильтрации, идентификации, управления, распознавания образов, сжатия информации и т. д.

К числу основоположников теории нейронных сетей относят ряд ученых, среди которых D. O. Hebb, J. J. Hopfield, T. Kohonen, F. Rosenblatt, W. W. McCulloch, W. Pitts, S. Grossberg, B. Widrow, M. E. Hoff и др. Среди наиболее известных следует отметить публикации следующих иностранных специалистов: С. Хайкина [1], Р. Каллана [2], Т. Кохонена[3], С. Осовского[4], Д. Рутковской[5], Ф. Уоссермена[6] и др.

Реальная нейронная сеть может содержать один или несколько слоев и, соответственно, называется однослойной или многослойной. Приведем для примера схему однослойной сети с m-нейронами (рис. 1).

Каждый элемент вектора входа соединен со всеми входами нейронов, и это соединение задается матрицей синаптических весов W, при этом i-нейрон включает суммирующий элемент, который формирует скалярный выход z_i. Совокупность скалярных величин z_i объединяется в S-элементный вектор входа z для функции активации f-слоя. Особенностью нейронных сетей является то, что для обеспечения большей гибкости и универсальности модели к входам каждого нейрона могут добавляться сигналы смещения $b_1, b_2, ..., b_S$.

[1] *Хайкин С.* Нейронные сети: полный курс. 2-е изд. М., СПб., 2006.
[2] *Каллан Р.* Основные концепции нейронных сетей. М., 2001.
[3] *Кохонен Т.* Самоорганизующиеся карты. 3-е изд. М., 2008.
[4] *Осовский С.* Нейронные сети для обработки информации. М., 2004.
[5] *Рутковская Д.* Нейронные сети, генетические алгоритмы и нечеткие системы. М., 2006.
[6] *Уоссермен Ф.* Нейрокомпьютерная техника. М., 1992.

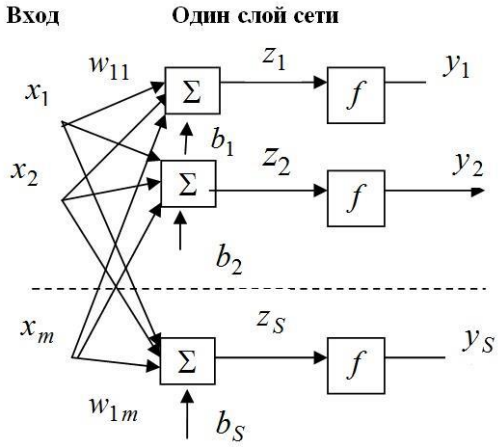

Рис. 1. Развернутая схема однослойной нейронной сети

Выходы слоя нейронов формируют вектор-столбец *Y*, и тогда описание слоя имеет вид:

$Y= f(Wx+b),$

где W – матрица синаптических весов, f – нелинейная функция активации.

Мощность и универсальность аппарата нейронного моделирования объясняется тем, что отдельные однослойные сети могут объединяться в многослойные, кроме того, между ними могут образовываться обратные связи. Принято называть структуру такой сложной сети архитектурой [5].

Обозначим весовую матрицу, связанную с входами, через IW^{11}, верхние индексы которой указывают, что источником входов является первый слой (второй индекс) и адресатом является также первый слой (первый индекс) (см. рис. 2). Элементы этого слоя, такие как число нейронов в слое S^1, смещение b^1, вход функции активации z^1 и выход слоя y^1, имеют верхний индекс 1, чтобы обозначить, что они связаны с первым слоем. Черный прямоугольник в левой части рис. 2 обозначает вектор входов.

Символическое описание первого слоя выглядит как: $y^1= f^1(IW^{11}X+b^1).$

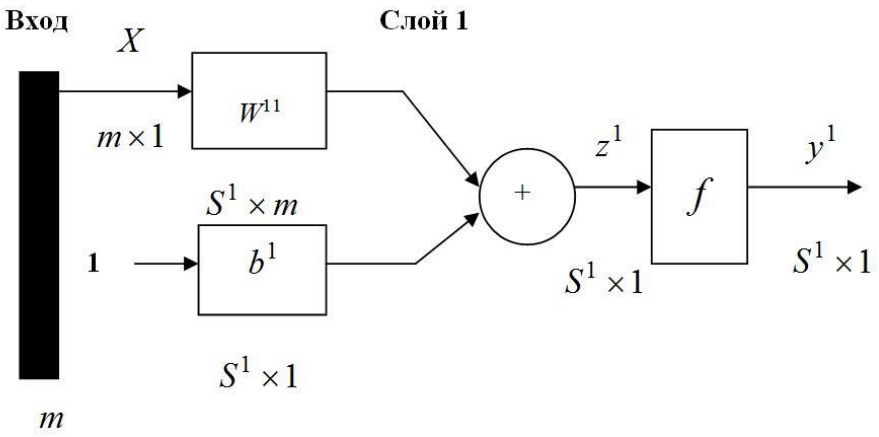

Рис. 2. Первый слой многослойной нейронной сети

Когда сеть имеет несколько слоев, то каждый слой имеет свою матрицу весов *W*, вектор смещения *b*, функцию активации *f* и вектор выхода *y* . Чтобы различать весовые матрицы, векторы выхода для каждого из этих слоев, вводится номер слоя как верхний индекс для каждой переменной.

Альтернативный подход к экспертизе. Специфическим видом нейронных сетей являются так называемые ассоциативные машины [7] , основанные на вероятностной модели ассоциативного обучения. Среди них выделяются динамические структуры, подразумевающие объединение оценок, полученных «экспертами» (отдельными нейронами).

Рассмотрим вначале модульную нейронную сеть, в которой процесс обучения происходит при неявном объединении самоорганизующейся формы обучения и формы обучения с учителем. Эксперты (нейроны) в целом осуществляют обучение с учителем, поскольку их отдельные выходы объединяются для получения требуемого отклика. Однако раздельно эксперты осуществляют самоорганизующееся обучение, т. е. они самоорганизуются с целью нахождения наилучшего разбиения пространства входов, причем каждый из них в своем подпространстве имеет оптимальную производительность.

В работах [1, 2] была детально описана методика решения прямой задачи оценки (экспертизы), целью которой являлось выделение среди множества сравниваемых объектов одного наилучшего объекта по ***критерию максимума обобщенного показателя J.***

В практике применения нейронных сетей такой методике соответствует встроенная функция *compet* пакета *nntool* языка MATLAB, реализующая принцип «победитель получает все». Для иллюстрации результатов экспертизы рассмотрим применение функции активации *compet* к тестовому множеству обобщенных показателей качества:

$J=(0.00;\ 1{,}00;\ -0{,}50;\ 0{,}50)^T$

и представим полученные результаты графически (см. рис. 3).

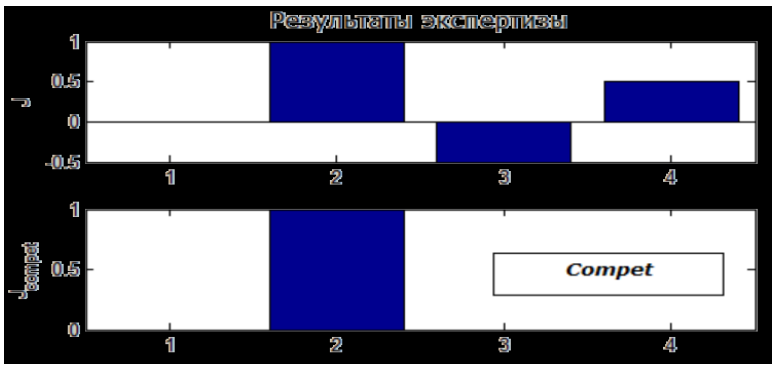

Рис. 3. Исходное множество показателей качества J и выходы нейронной сети при функции активации compet

[7] *Хайкин С.* Указ. соч.

В верхней части рис. 3 приведены исходные значения показателя *J*, соответствующие формуле, в нижней части – выходной сигнал нейронной сети при использовании функции активации *compet*. Как и следовало ожидать, только один (второй) нейрон «выиграл» в процессе конкурентной борьбы. Выходы сети, соответствующие другим нейронам, равны нулю, т. е. информация о показателях других объектов экспертизы оказалась утерянной. В целом, это соответствует принятой ранее в работах [1, 2] методике решения прямой задачи экспертизы, поскольку целью ее было выявление единственного объекта с наилучшими показателями. Однако известно, что «жесткие решения при экспертизе приводят к потере информации, в то время как мягкие решения ее сохраняют».

Поэтому при формировании нейронной сети представляется целесообразным перейти от жесткой конкурирующей функции активации *compet* к конкурирующей функции активации с мягким максимумом – *softmax*.

Вывод. Таким образом, проведенный выше анализ теории экспертных систем показывает, что решение задачи оценки эффективности функционирования социотехнической системы заключается в погружении численной задачи оценки в экспертную оболочку в классе DMS (Data Mining System) для определения эффективности.

Список литературы

1. *Бухарин С. В., Мельникова А. В.* Кластерно-иерархические методы экспертизы экономических объектов: монография. Воронеж, 2012.
2. *Бухарин С. В., Навоев В. В.* Методы теории нейронных сетей в экспертизе технических и экономических объектов. Воронеж, 2015.
3. *Дюк В. А.* Компьютерная психодиагностика: монография. СПб., 1994.
4. *Дюк В. А., Самойленко А.* Data Mining: учебный курс. СПб., 2001.
5. *Медведев В. С., Потемкин В. Г.* Нейронные сети. Matlab 6. М., 2002.
6. *Барсегян А. А. и др.* Технология анализа данных: Data Mining, Text Mining, OLAP. 2-е изд. СПб., 2007.

А. В. БЕЦКОВ,
начальник кафедры информационных технологий,
доктор технических наук, доцент
(Академия управления МВД России)

О математическом моделировании вероятности совершения террористического акта

В настоящее время можно обозначить три основных направления научного исследования проблем современного терроризма [1, 3]:

– исторические взаимосвязи, причины и условия развития;

– современное состояние терроризма;

– прогнозирование, меры предупреждения и активная борьба с терроризмом.

Причины и условия возникновения терроризма могут быть: региональные, экономические, политические, религиозные, этнические, исторические. При раскрытии причин и условий терроризма необходимо придерживаться основополагающей идеи о том, что, до тех пор пока человечество не определится в них, не выяснит онтологию этого феномена, оно все время будет запаздывать в своих мерах воздействия. Нельзя не принимать во внимание и то, что террор для большинства экстремистских групп по-прежнему является главным средством побуждения властей удовлетворять их требования.

Ко второму направлению относятся региональные и национальные стратегии борьбы с терроризмом; основные методы борьбы с международным терроризмом; особенности полицейских и силовых мер, специальных операций как эффективных форм борьбы с международным терроризмом и др. В процессе научных исследований проблем современного состояния терроризма важное значение должно придаваться не только раскрытию его отдельных проявлений, но и изменению самого характера преступления. Из сугубо криминального терроризм превратился в социально-политическое явление, содержащее в себе определенные социальные противоречия. Его питательной средой являются:

– глубинные противоречия в политике и экономике;

– ослабление защитных механизмов в сфере нравственности, морали и патриотизма;

– низкая эффективность деятельности государственного аппарата.

Без осознания, особенно на высшем уровне государства, указанных процессов и принятия жестких мер, а также анализа и исследования феномена терроризма сложно и даже невозможно оценить и победить этот феномен.

Третье направление должно включать анализ и исследование разработки научной технологии в таких областях, как:

– прогнозирование дальнейшего возможного развития терроризма; проблемы создания антитеррористического международного фонда; национальные и международные доктрины по координации усилий международного сообщества в борьбе с терроризмом;

– правовое и организационное, техническое и ресурсное (в широком понимании) обеспечение международных и собственных сил быстрого реагирования на проявления терроризма.

Терроризм эволюционирует в результате недооценки его опасности международным сообществом и процветает там, где имеется соответствующая среда, отсутствуют скоординированные, целенаправленные, решительные и высокопрофессиональные действия по борьбе с этим международным злом. По числу и характеру совершаемых в настоящее время террористических актов можно сделать вывод: терроризм перешел в активное наступление, им брошен вызов всему цивилизованному миру. Это отрицательно характеризует международное сообщество и его государственные институты.

В связи с отмеченным выше, по нашему мнению, являются актуальными исследования, направленные на создание технологических научных основ противодействия современному терроризму на базе фундаментально-прикладных основ и технических достижений, реализуемых с помощью быстродействующих информационных технологий [5]. Вначале рассмотрим задачу о проникновении террориста на объект для совершения преступления [1, 2] (рис. 1). Пусть на оси слева из ∞ движется бесконечная последовательность точек, которые будем называть целями.

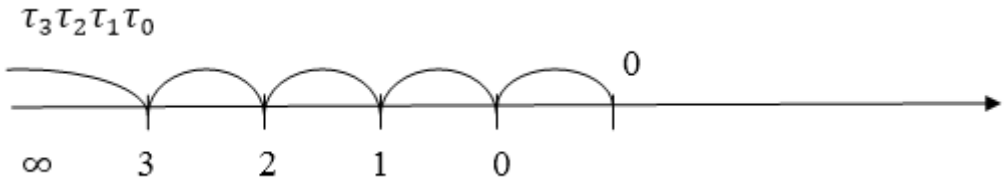

Рис.1

Самую правую цель назовем головной. Предположим, что все цели движутся вправо с постоянной скоростью, равной единице, а расстояние между соседними целями – $\tau_к$ ($к = 1,2$). Суть – независимые случайные величины, каждая из которых распределена по закону:

$$P=\{\tau_к < x\}=\begin{cases} f(x) \text{ при } x > 0 \\ 0 \text{ при } x \le 0 \end{cases}$$

Допустим, что существует среднее значение этой величины $h= \int_0^\infty x dF(x)$. Когда головная цель (выбранная террористом) приходит в точку τ_0, террорист начинает действовать. Случайная величина (выбранная цель) τ_0 имеет распределение $P =\{ \tau_0 < x\} = \begin{cases} G(x) \text{при } x > 0 \\ 0 \text{ при } x \le 0 \end{cases}$ со средним

$h_0 = \int_0^\infty x dG(x)$. Предположим, что террорист воздействует всегда только на выбранную (для себя) головную цель, т. е. самую правую на рис. 1, а в действительности – на вагон в Петербургском метро на станции «Технологический институт».

Характер воздействия на цель таков, что независимо от предшествующего воздействия, номера выбранной цели и ее расположения вероятность поражения цели на участке длины Δx равна

$$1-\lambda\Delta x + 0(\Delta x). \quad (1)$$

Отсюда следует, что длительность воздействия на цель подчинена экспоненциальному закону и $\frac{1}{x}$ – есть среднее время воздействия террориста на данную выбранную цель. Для дальнейшего исследования предположим, что начальная головная цель имеет нулевой номер, а остальные цели (в нашем случае вагоны поезда в метро) нумеруются по порядку. Обозначим через p_n вероятность того, что цель с номером n первой достигла начала координат [3]. В этом случае

$$P = \sum_{n=0}^{\infty} p_n - \text{ есть вероятность прорыва террориста к цели.}$$

Задача заключается в определении этой вероятности P_n. Пусть головная цель для террориста в какой-то момент t_0 находится в точке x_0. Обозначим через $v(x)$ число возможных пораженных целей, начиная с момента t_0 и до момента, когда головная цель (намеченная террористом) впервые после момента t_0 придет в точку x_0+x. Тогда случайная величина (СВ) $v(x)$ не зависит ни от номера головной цели, пришедшей в точку x_0, ни от времени воздействия террориста на нее до момента t_0, ни от положения отрезка $[x_0, x_0+x]$. Для двух соседних участков длины x и y имеем

$$v(x+y)=v(x)+v(y), \quad (2)$$

причем в силу вышеизложенного величины $v(x)$ и $v(y)$ независимы. Сделаем обозначение

$$P(X_1 Z) = M\left[Z^{v(x)}\right] = \sum_{n=0}^{\infty} P_n(x) Z^n.$$

$$P(Z) = \sum_{n=0}^{\infty} P_n Z^n \quad (3)$$

$$P(Z) = \int_0^\infty P(X_1 Z) dG(x) \quad (4)$$

Для решения задачи достаточно найти производящую функцию

$$P(X_1 Z).$$

Из (2) получим

$P(Xx+Y,Z)=M[Z^{v(x+y)}]=M[Z^{v(x)+v(y)}]=M[Z^{v(x)}]MM[Z^{v(y)}]=P(X,Z)P(Y,Z)$.

Отсюда следует [1], что функция $P(X_1 Z)$ имеет вид

$$P(X_1 Z)=e^{-xy(z)}. \quad (5)$$

На бесконечно малом участке длины Δx выбранная головная цель будет либо поражена, либо нет. Если же головная цель поражена, то начинается (террористом) воздействие на следующую цель, отстоящую от данной точки на случайное расстояние $\tau_к$, и в этом случае $v(\Delta x)$ будет равно $v(\tau_к)+1$. Таким образом, $M[Z^{v(\Delta x)}]=1-e^{-\Delta x y(z)} = 1-\Delta x y(z)+0(\Delta x) = (1-\lambda\Delta x)M(Z^0)++\lambda\Delta x M\left[Z^{v(\tau_к)+1}\right]+0(\Delta x) = 1-\lambda\Delta x+\lambda\Delta x Z\int_0^\infty e^{-ty(z)}dF(t)+0(\Delta x)$.

В пределе при $\Delta x \longrightarrow 0$ получим уравнение

$$y(z)=\lambda-\lambda Z\int_0^\infty e^{-ty(z)}dF(t) \text{ или}$$

$$y(z)=\lambda-\lambda Z\varrho[y(z)], \quad (6)$$

где $\varrho(P)=\int_0^\infty P^{-Pt}dF(t)$. Искомая производящая функция P(Z) из (4) равна

$$P(Z)=\int_0^\infty e^{xy(z)}dG(X)=b[y(z)], \quad (7)$$

где $b(p)=\int_0^\infty e^{-Pt}dG(t)$. Используя (3), (6), (7), определим искомые вероятности P_n-прорыва террориста для поражения выбранной цели.

Рассмотрим уравнение (6). Так как функция $Z=Z(y)=\frac{\lambda-y}{\lambda a(y)}$ регулярна в окрестности y=x, то обратная ей функция y(z) будет регулярна и однозначна в окрестности точки z=0.

Поэтому при $n>0$

$P_n=\frac{1}{2\pi i}\int_C\frac{P(Z)}{Z^{n+1}}dZ=\frac{1}{2\pi i}\int_c\frac{b[y(Z)]}{Z^{n+1}}dZ$, где c-контур охватывает начала координат. Последний интеграл преобразуем интегрированием по частям.

$P_n=\frac{1}{2\pi i}\int_C\frac{b'[y(Z)]}{nz^n}dy(z)$. Сделаем в интеграле замену переменного, положив $\mathcal{E}=y(z)$

$$P_n=\frac{1}{2\pi i}\int_{C_\lambda}\frac{b'(\varepsilon)d\varepsilon}{h\left[\frac{\lambda-\varepsilon}{\lambda\varrho(\varepsilon)}\right]^n}=\frac{x^n(-1)^n}{2\pi i}\int_{C_\lambda}\frac{b'(\varepsilon)\varrho^n(\varepsilon)}{h(\varepsilon-\lambda)^n}0/\varepsilon.$$

Контур C_λ охватывает точку $\varepsilon=\lambda$. Отсюда конечная формула для вероятностей прорыва террориста к цели:

$$P_n=\frac{\lambda_n(-1)^n}{n!}[\varrho^n(\varepsilon)b'(\varepsilon)]_{\varepsilon=\lambda}^{(n-1)} \quad (8)$$

Определим теперь оценку вероятности прорыва. Выше определено

$$P=\sum_{n=0}^{\infty}P_n=b[y(1)]=b(\alpha),$$

$\alpha=y(1)$ и определяется из уравнения

$$\alpha=\lambda-\lambda\varrho(\alpha) \text{ или } 1-\frac{\alpha}{\lambda}=\varrho(\alpha) \quad (9)$$

Используя выпуклость функции ϙ(x) (рис. 2), можно получить такой результат. Если $\lambda h \leq 1$, то $\alpha = 0$, и в этом случае вероятность прорыва террориста к цели P=b(0)=1. Если $\lambda h >$, то $0 < \alpha < \lambda$, и, следовательно, вероятность прорыва – меньше единицы.

Тогда возникает задача, каков должен быть закон распределения расстояния между целями F(x) при фиксированном среднем расстоянии $h > \frac{1}{\lambda}$, чтобы вероятность прорыва была наименьшей. Для этого будем иметь в виду следующее [1, 5]:

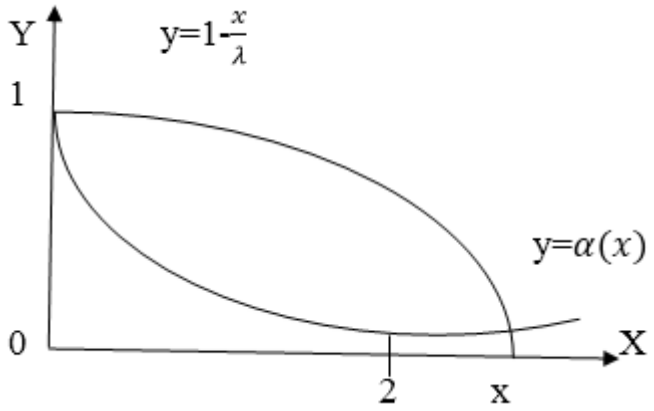

Рис. 2

$$\alpha(P)\ell^{Ph} = \int_0^\infty \ell^{-P(x-h)}\, dF(x) \geq \int_0^\infty [1 - P(x-h)]\, dF(x) = 1,$$

или $\alpha(P) \geq \ell^{-Ph}$, на ℓ^{-Ph} есть преобразование Лапласа для закона

$$F_0(x) = \begin{cases} 0, & x \leq h \\ 1, & x > h \end{cases}$$

Отсюда геометрически очевидно (рис. 2), что наибольшее значение корня уравнения (9) будет в том случае, когда $\alpha(P) = \ell^{-Ph}$, т. е. когда все расстояния между соседними целями равны n. Этот наибольший корень α_0 определяется рядом:

$$\alpha_0 = \lambda\left[1 - \sum_{n=1}^{\infty} \frac{(nh\lambda)^{n-1}}{n!}\ell^{-nh\lambda}\right], \qquad (10)$$

что легко получается тем же методом, которым была получена формула (8).

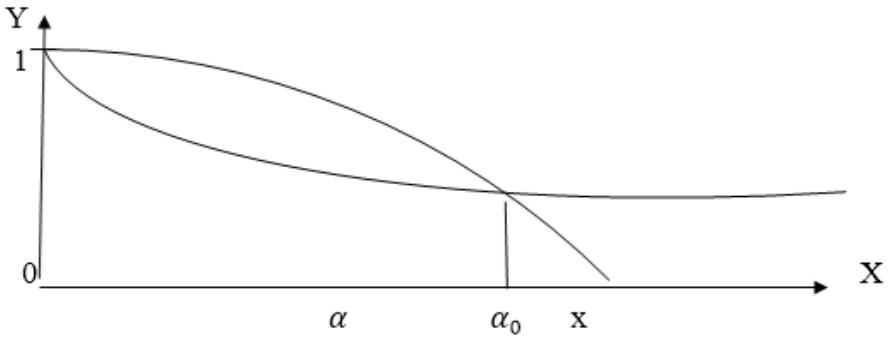

Рис. 3

Но очевидно, что при этом наибольшем α_0 вероятность прорыва террориста к цели $P=b(\alpha_0)$ будет наименьшей, так как функция b(x) монотонно убывает.

Итак, для движущихся целей типа поездов в метро и др. наименее выгодным будет регулярный порядок, при котором все расстояния между соседними целями равны. Возникает вопрос: при каком $F(x)$ со средним h вероятность прорыва террориста к цели будет наибольшей? Ответ: надо найти такие законы, для которых вероятность прорыва сколь угодно будет близка к единице. Например, если

$$\alpha(P) = \frac{1}{\sqrt[m]{1+mhp}};\ (m>0),\ \text{то при } m\longrightarrow\infty\alpha(p)\longrightarrow 1$$

при любом фиксированном P. Следовательно, корень α при этом стремится к нулю, а вероятность прорыва $b(\alpha)$ – к единице.

Демонстрация данного подхода к определению вероятности террористического акта не исключает, а, скорее, ангажирует массу иных научных взглядов на решение этой проблемы. Моделирование можно считать успешным направлением формирования учебных задач для обучения специалистов в области противодействия преступности, в т. ч. терроризму.

Список литературы

1. *Северцев Н. А., Шмалько Е. Ю.* Эффективность стратегий обеспечения безопасности автотранспортного движения в мегаполисе // Наукоемкие технологии. 2015. № 2. С. 11–14.

2. *Северцев Н. А.* Моделирование оценки математического ожидания дисперсии случайных функций, характеристик сложной технической системы // Надежность и качество сложных систем. 2014. № 3. С. 16–21.

3. *Северцев Н. А., Бецков А. В.* Системный анализ теории безопасности. М., 2018.

4. *Северцев Н. А., Бецков А. В.* Введение в безопасность. М., 2018.

5. *Бецков А. В., Дарьина А. Н.* Возможный вариант оценки требований безопасности полетов при ограниченной статистике тяжелых летных происшествий // Наукоемкие технологии. 2015. № 2. С. 34–38.

А. В. БЕЦКОВ,
начальник кафедры информационных технологий,
доктор технических наук, доцент
(Академия управления МВД России)

Н. А. СЕВЕРЦЕВ,
заведующий отделом,
доктор технических наук, профессор
(ВЦ РАН им. А. А. Дородницина)

И. В. ПРОКОПЬЕВ,
старший научный сотрудник,
кандидат технических наук
(ВЦ РАН им. А. А. Дородницина)

О системном представлении методологии безопасности

Необходимо признать, что до сих пор обобщенной терминологии безопасности для различных отраслей науки и техники нет, особенно в формализованной постановке. Есть понятие безопасности систем для каждой отрасли научных знаний, хозяйствования и в философском понимании – вербальном представлении, которое трактуется применительно к какому-либо объекту (системе), принадлежащему той или иной отрасли. Данная статья посвящена обобщенному понятию безопасности независимо от принадлежности исследуемой системы (объекта).

Пусть имеется система, на которую действуют внешние и внутренние возмущения при управлении данной системой. Весь спектр этих случайных воздействий может привести систему к разрушению. Задача состоит в том, чтобы построить оценки, позволяющие в процессе работы системы численно определить угрозу распада системы для своевременного принятия мер к недопущению этого. Очевидно, такая оценка должна быть построена на движении системы, т. е. представлять функционал, так как изменяющееся состояние системы может нести в себе информацию о приближении опасного порога функционирования системы.

Принципиальная схема формирования показателя безопасности $J_б$ на основе всех информационных потоков представляется следующим образом.

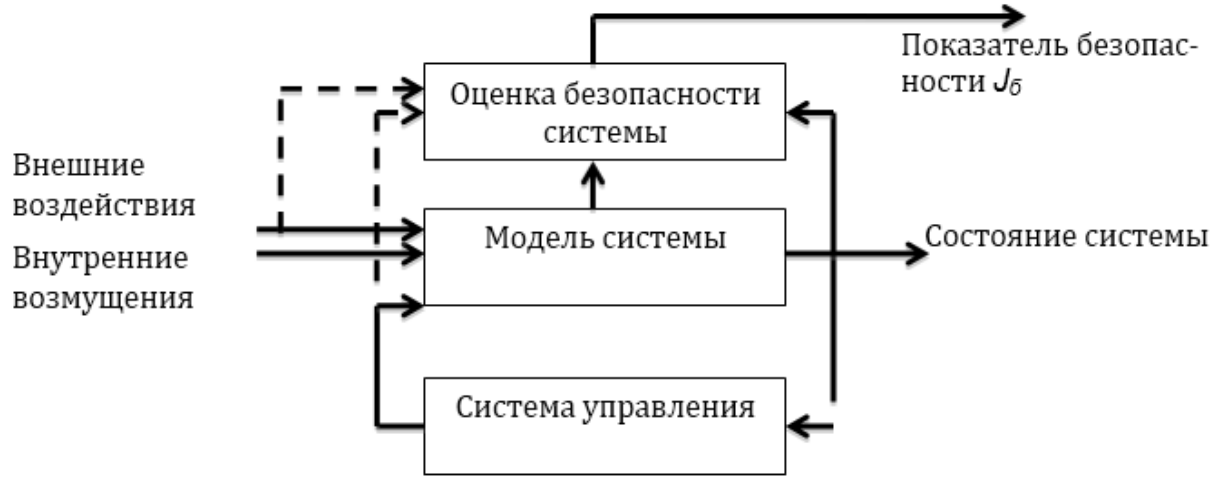

Рис. 1. Схема формирования оценки безопасности на основе информации

Например, увеличивающаяся амплитуда колебаний (качки) водного судна выше пределов остойчивости позволяет судить об угрозе его оверкиля, т. е. когда центр тяжести (центр масс) окажется выше центра величины, т. е. центра гидростатического давления. В этом примере катастрофа (оверкиль водного судна) будет являться результатом изменения его состояния, а не причиной, его вызвавшей.

Следовательно, все пространство состояний системы можно разделить на две области: одна будет составлять множество опасных для существования системы состояний – C_o, а другой будут принадлежать все безопасные состояния – $C_б$. Объединение этих множеств опишет все возможные состояния системы $(C = C_o \cap C_б)$. Надо выделить две противоречивые тенденции при построении $C_б$. С одной стороны, чтобы гарантировать безопасность системы, из этого множества следует исключить все режимы, которые могли бы приводить к ее деструкции, что означает – множество надо сужать. Но ограничение допустимых состояний стесняет возможности функционирования, а следовательно, уменьшает возможности достижения целевого множества. Преодоление противоречия осуществляется поиском компромисса. В этом случае его следует искать в удалении от границы безопасности, т. е. уменьшать область безопасности и предоставить ЛПР время на парирование угроз, а также повысить уровень защищенности. Такой подход можно определить следующим образом: объективную оценку безопасности системы можно произвести, наблюдая ее состояние. Для этого следует построить подмножество безопасных состояний, выделив все режимы, приводящие к разрушению (потере гомеостаза) системы. Строго говоря, область безопасности может быть сформирована на основе полномасштабного моделирования работы системы с управлением в реальных условиях и действия на нее всевозможных возмущений. Для сохранения гомеостаза системы необходимо создать запас безопасности, введение которого обеспечивает уменьшение области безопасности.

Однако даже если построена модифицированная граница области безопасности с учетом запаса $Г_{бм}$, то находить в пространстве C кратчайшее расстояние от текущего состояния системы, задаваемого вектором C, до границы $Г_{бм}$ представляется затруднительным.

Во-первых, наличие модифицированной области $C_{бм}$ в пространстве состояний наиболее объективно свидетельствует об удаленности текущего режима работы системы от состояния, угрожающего его целостности. Однако для повышения временного ресурса для устранения неполадок в системе, для повышения оперативности и качества управления было бы желательно располагать информацией о причинах, обусловливающих приближение состояния системы к опасной границе. Для этого рассмотрим факторы, определяющие появление опасных для системы режимов, т. е. требуется сделать анализ угроз, проникающих через единственный канал – через воздействие на систему. Например, лучше сделать профилактику судна «Булгария», выяснить все причины неполадок и устранить их, чем выходить в плавание с этими неустраненными неполадками (а их было много), дожидаться оверкиля судна с большими жертвами.

Во-вторых, необходимо определить показатели безопасности, имеющие большую физическую наглядность и меньшую сложность вычислений, нежели определение в пространстве состояний расстояния до границы (рис. 2).

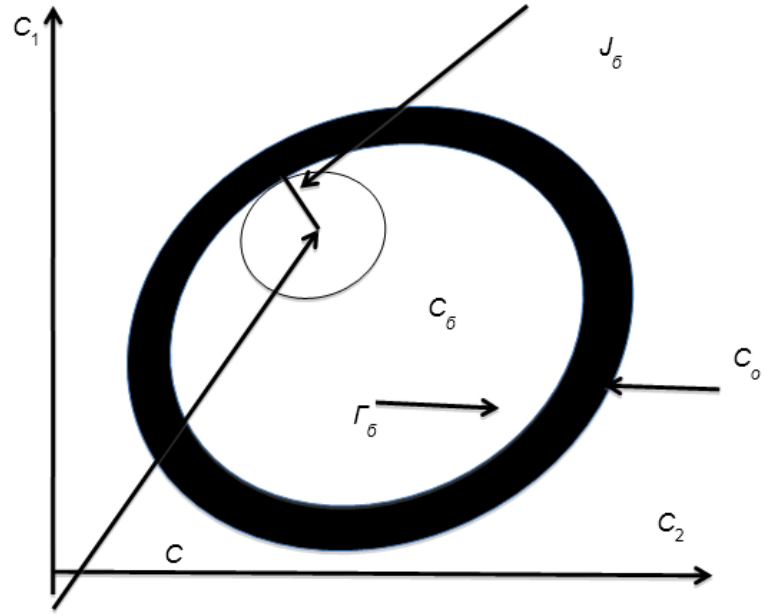

Рис. 2. Показатель безопасности в пространстве состояний

Решение первой задачи базируется на рис. 1. Если раньше область безопасности строилась на основе информации о состоянии (выход модели), то теперь следует привлекать сведения о входных воздействиях, т. е. использовать каналы, изображенные пунктирными линиями. Это воздействия управления, внешние и внутренние воздействия. Итак, внутренние возмущения включают в себя изменения каналов передачи

информации (структурные трансформации) и отклонения параметров от номинальных значений (параметрические возмущения). Неожиданная реорганизация структуры является самой опасной, так как особенно сильно влияет на динамическое состояние системы. Предвидеть подобные преобразования в самоорганизующихся системах весьма сложно в силу их многоальтернативности и малой предсказуемости; такая задача имеет характер бифуркационных изменений. В искусственно созданных системах структура мало подвержена внезапным преобразованиям, так как они есть результат синтеза системы, воплощенного в реальность совокупностью технических решений, направленных именно на поддержание целостности системы. Что касается управлений как целенаправленных воздействий на динамику системы, то в искусственных системах они идентифицируются просто. В естественных системах понятие управления часто размыто. Тогда напрашивается вывод о том, что основную проблему при построении оценки безопасности доставляют параметрические возмущения и внешние воздействия среды. Итак, будем исходить из предположения, что область безопасности $C_{бм}$ построена. Тогда задача заключается в пересчете этого подпространства пространства состояний в пространство входных воздействий – параметрических $C^{П}_{бм}$ и внешних $C^{В}_{бм}$ возмущений. Однако такое решение затруднительно, так как из реакций системы трудно выделить их причинную обусловленность, т. е. установить вклад каждого возмущения в результат – состояние. Поэтому приходится обойтись без процедуры общего пересчета, а по отдельности строить области для каждого входного воздействия. Методически это заключается в нахождении соответствия границы $\Gamma_{бм}$ множества $C_{бм}$ границам в пространствах параметров и воздействия внешней среды – соответственно $\Gamma^{В}_{бм}$ и $\Gamma^{П}_{бм}$. Перебирается весь спектр воздействий, например, методом Монте-Карло, и находится реакция системы на каждый входной сигнал. Те сигналы, которые приводят к распаду системы, и признаются опасными.

Сложность процедуры усугубляется еще одним обстоятельством: в общем случае динамических нелинейных систем существует взаимная корреляционная зависимость области нормального функционирования системы от параметрических и внешних возмущений. Грубо говоря, для каждого уровня внешних воздействий имеется свое множество допустимых значений параметров системы (рис. 3).

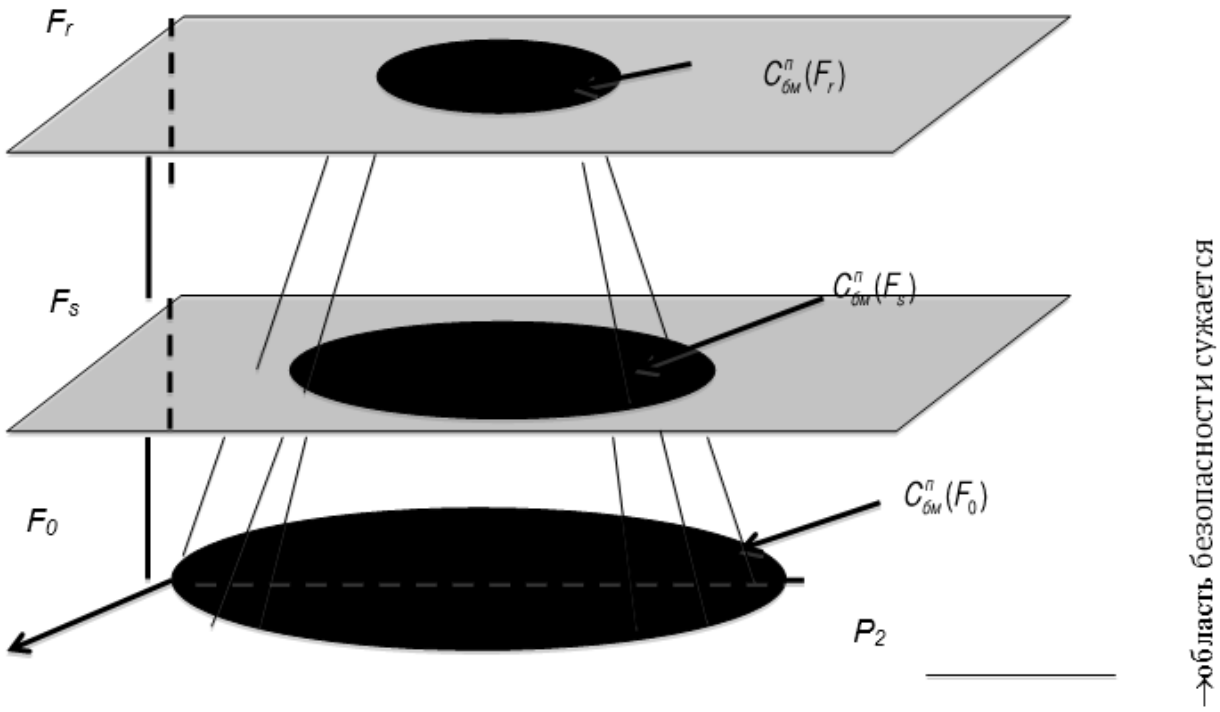

Рис. 3. Деформация параметрической области безопасности при различных возмущениях

Горизонтальная плоскость рис. 3 есть множество параметров $P=\{P_i\}$, $i=1,2$, где выделена область безопасности $C^{п}_{бм}$. По ординате отложена величина уровня внешних возмущений F с тремя координатами-воздействиями – F_0,F_s,F_r. Для разных уровней возмущений область $C^{п}_{бм}$ меняется, т. е. становится их функцией. Можно предположить, что по мере роста воздействий на систему параметрическая область безопасности сужается. Таким образом, в результате построений мы располагаем двумя наборами взаимосвязанных множеств: областями безопасности $C^{в}_{бм}$ и $C^{п}_{бм}$, построенными в пространстве входных воздействий и флуктуирующих параметров соответственно. Тем самым при оценке безопасности можно перейти от изучения состояний системы к наблюдению за выходными сигналами, а значит, заменить анализ следствия анализом причин. Обращение непосредственно к угрозам, исходящим от среды и нарушений в системе, привело к размножению областей безопасности. Вместо итоговой области в пространстве состояний мы вынуждены иметь дело с несколькими областями по числу каналов проникновения угроз в систему, к тому же области связаны функционально. Конечно, это делает алгоритмы обеспечения безопасности более сложными.

Мы рассмотрели решение первой задачи. Теперь перейдем ко второй.

1. Нарушение устойчивости системы означает появление в ней расходящихся процессов, которые не поддаются управлению и немедленно приводят к дезинтеграции системы. Существует общий подход к исследованию устойчивости на результатах А. М. Ляпунова, от которого трудно ожидать непосредственной применимости к проблеме безопасности

в силу отсутствия возможности получения конкретных оценок. Развитие метода показало, что его эффективное использование требует разбиения общей задачи на классы, а наиболее продвинутыми оказались решения частных задач с вполне конкретными видами нелинейностей.

Нарушение устойчивости не столь очевидно, но имеет губительные последствия. Поэтому при определении безопасности режимов работы системы следует уделять внимание и устойчивости. Тогда границы $\Gamma_{б}^{в}$ и $\Gamma_{б}^{п}$ областей безопасности будут описывать нарушение условий устойчивости системы при превышении уровня допустимых внешних воздействий и запредельном отклонении параметров системы. Мера безопасности как гарантия устойчивости определяется посредством оценки удаления текущего состояния системы от границы, описывающей переход в неустойчивое состояние (рис. 2). Однако в настоящее время не существует общих методов построения областей устойчивости в пространствах воздействий и параметров, которые были бы адекватными областями безопасности. Это обстоятельство ставит под сомнение возможность разработки общей конструктивной теории безопасности, по крайней мере при современном уровне теории устойчивости в безопасности функционирования системы. Выход из указанного затруднения лежит на пути декомпозиции проблемы, разбиения общей задачи на ряд частных. Иначе, если не удается построить теорию безопасности для всех типов систем, то необходимо решать задачи для систем отдельных классов или в худшем случае ограничиться отысканием частных решений для конкретного вида систем, оценка устойчивости которых известна. Действительно, при изучении системы на безопасность всегда можно выстроить приоритеты факторов по их влиянию на ее безопасность. Тогда в последующих исследованиях устойчивости можно принимать во внимание только наиболее критичные, для которых и вычислять области допустимых значений.

2. Управляемость системы по своей содержательности сходна с понятием области достижимости. Оба характеризуют достижение цели. Для линейных систем условие управляемости известно. Для нелинейных систем это условие сопряжено с большими трудностями. С практической точки зрения достижение цели требует:

а) того, чтобы управляющие органы могли воздействовать на параметры состояния, в которых фиксируется цель;

б) того, чтобы было достаточно ресурсов для движения по траектории, проходящей через цель. Эти соображения имеют ясную физическую наглядность, что позволяет выполнить их при создании системы;

в) наблюдаемости системы – доступности измерений степеней свободы, информация о которых необходима для управления системой. Выполнение этого требования на практике осуществляется путем создания измерителей, достаточных для идентификации состояний и управления движением системы.

Выводы

1. Для построения оперативной системы мер по недопущению превращения угроз в катастрофические (аварийные) для системы целесообразно использовать информацию о входных воздействиях со стороны среды и отклонениях параметров системы. Это позволяет подвергнуть анализу не следствия (опасные изменения состояния), а причины появления угрожающих состояний. Однако такой путь связан с усложнением системы как в алгоритмическом смысле, так и информационном – требуются сведения об угрозах существованию системы. Можно ожидать, что объединение информационных потоков о состоянии систем и причинах его изменения даст наилучшие результаты.

2. Из числа доступных анализу характеристик динамики системы пригодны для оценки безопасности показатели управляемости, наблюдаемости и устойчивости, а также энергетические ресурсы. Большинство из них достаточно просто удовлетворяется при проектировании или подготовке системы к работе, поэтому их можно не учитывать при анализе безопасности системы. Исключением можно считать устойчивость, оценка которой изменяется при воздействиях со стороны внешней среды и внутренних возмущениях. Эту характеристику следует использовать при построении области безопасности.

3. Применение оценки устойчивости в качестве показателя безопасности в общем случае затруднительно, что приводит к необходимости подвергать анализу на безопасность отдельные классы или только конкретные системы. Для построения области безопасности по критерию устойчивости и ее использования при контроле целесообразно применять упрощение модели системы. Упрощение рационально проводить путем: выявления критических угроз и/или их объединения в эталонные группы; отказа от непрерывной модели системы и перехода к конечным зависимостям между воздействиями и реакциями системы.

Список литературы

1. *Могилевский В. Д.* Основы теории систем. М., 1997.
2. *Северцев Н. А., Бецков А. В.* Введение в безопасность. М., 2018.
3. *Северцев Н. А., Бецков А. В.* Системный анализ теории безопасности. М., 2018.

Д. Ю. БУЛГАКОВ,
заместитель начальника
ФКУ «ГИАЦ МВД России»

Современные подходы к тестированию систем биометрической идентификации по изображению лица

Типовая биометрическая система, как она представляется в соответствии с ГОСТ [1] и международным стандартом [2], состоит из следующих модулей: 1) биометрический сканер; 2) предобработка (фильтрация); 3) извлечение особенностей; 4) создание биометрического шаблона; 5) поиск совпадений по базе данных; 6) показ рекомендательного списка.

Концептуальные компоненты биометрической системы, в соответствии с теми же стандартами, состоят из следующих подсистем: 1) сбора данных; 2) передачи данных; 3) обработки сигнала; 4) хранения данных (базы данных); 5) сравнения данных; 6) принятия решений; 7) администрирования; 8) взаимодействия с внешними приложениями (API – англ. Application Programming Interface).

Современные биометрические системы, основанные на распознавании изображения лица и использующие в своей основе сверточные нейронные сети (далее – СНС), укладываются в данную концепцию. В качестве их структурных компонентов и этапов обработки изображения можно выделить следующие:

1) захват фотоизображения с фотоаппарата или в виде кадра из видеопотока;

2) выявление лица (Face Detection) – определение наличия лица (лиц) на фотографии в виде прямоугольных областей;

3) выделение признаков (Landmarks Localization), чтобы определить, как именно расположено (ориентировано) лицо в прямоугольной области;

4) нормализация или выпрямление лица (Face Alignment). С помощью аффинных преобразований лицо приводится к заранее определенному масштабу, глаза располагаются горизонтально;

5) распознавание или кодирование лица (Face Recognition). На данной стадии из нормализованного лица извлекается биометрический шаблон. Именно здесь происходит работа СНС;

6) сравнение лиц (Face Matching). Поиск в массиве известных нам лиц наиболее похожих лиц путем сопоставления их биометрических шаблонов.

По мнению исследователей из Национального института стандартов и технологий США [3], алгоритмы идентификации, использующие распознавание лиц, применяются в следующих трех целях.

1. *Расследование преступлений*. Допустим, на месте преступления были сфотографированы подозреваемый или его жертва, и их личности нам

не известны. Используя алгоритм распознания лиц и некоторое множество фотографий лиц, личности которых нам известны, следователи сопоставляют фотографию, сделанную на месте преступления, с данным множеством. Обычно нет никакой гарантии, что фотография искомой личности находится в известном нам множестве. Алгоритм распознавания лиц настроен таким образом, чтобы в качестве результата поиска предлагать рекомендательный список, состоящий из постоянного числа кандидатов из искомого множества, или список из кандидатов, процент схожести которых выше определенного критерия. Рекомендательный список просматривает человек, который сопоставляет поисковую фотографию (объект) с фотографиями предлагаемых кандидатов. Если он решает, что один из кандидатов – это и есть искомая личность, то считается, что объект может быть идентифицирован – по имени или другой биографической информации, содержащейся в базе данных. Данное применение характеризуется очень низкими объемами поиска (возможно, только одной входной фотографией) и наличием рабочей силы, чтобы отсмотреть рекомендательный список.

2. *Отрицательная идентификация.* Представим сотрудника, выдающего водительские удостоверения, который ежедневно получает десятки тысяч фотографий. Его задача состоит в том, чтобы обнаружить, присутствует ли претендент на получение водительского удостоверения в базе данных под другим именем, например чтобы уклониться от запрета на управление транспортным средством. Эта задача рассматривается как отрицательная идентификация, потому что предположение по умолчанию – это то, что объекты не находятся в базе данных. Система распознавания лиц искала бы представленные фотографии в ссылочной базе данных и произвела бы сопоставление кандидата. В этом случае, учитывая большие объемы поиска и ограниченную рабочую силу, только то подмножество поисковых запросов, которые находят очень похожего кандидата, будет отправлено для принятия решения человеком. Системный оператор устанавливает пороговое значение, которое зависит от объема найденных кандидатов и трудовых ресурсов. Кандидаты, степень схожести которых находится ниже заданного порога, не возвращаются.

При видеонаблюдении количество кандидатов для просмотра, возвращаемое в рекомендательных списках, также может быть гораздо выше доступной рабочей силы.

3. *Положительная идентификация.* В условиях, когда большая часть объектов исследования содержится в базе данных, например в системе контроля и управления доступом (СКУД), распознавание лиц могло бы использоваться, чтобы реализовать аутентификацию на основе всего лишь одного фактора. К объектам не предъявляется требование в отношении их идентификационных данных, вместо этого простое предъявление их лица системе – это требование, которое должно быть выполнено, чтобы они получили необходимый доступ, если их лицо соответствует любому из предварительно зарегистрированных лиц. Решение вопроса безопасности такой системы определяется почти таким же

способом, как решение задачи верификации – т. е. ограничением, чтобы порог ложноположительных срабатываний был ниже определенного уровня. Это сложнее, чем верификация, так как сравнение обычно происходит не один-к одному, а один-ко-многим.

Чтобы обеспечивать данные сценарии, точность работы алгоритма устанавливается двумя способами: метрика на основе ранга (места в рекомендательном списке) – для задачи расследования преступлений; и метрика на основе порогового значения меры «похожести» – для задачи идентификации.

Обе метрики допускают компромиссы. Например, при расследовании преступлений общая точность будет снижена, если сил сотрудников будет достаточно только для того, чтобы рассмотреть небольшое количество кандидатов из рекомендательного списка.

Для оценки качества систем распознавания лиц проводятся различные тесты и организуются конкурсы.

К трем наиболее популярным в мире тестам систем биометрической идентификации по изображению лица можно отнести следующие.

1. Тестирование на основе открытого датасета «Labeled Faces in the Wild» (LFW), созданного в 2007 г. Университетом Массачусетса в Амхерсте (США). Наименование датасета можно перевести как «Известные личности в естественной обстановке». Данный датасет содержит 13 233 фотографии в отношении 5 749 личностей. Фотографии собраны из открытых источников в Интернете. Для 1 680 личностей содержится 2 и более различных фотографий. В датасете присутствует несколько ошибок, когда фотографии от разных лиц приписаны одному лицу.

К *достоинствам* тестирования на основе данного датасета можно отнести его большую популярность и доступность, вследствие чего, как правило, он используется в качестве базового теста для алгоритмов распознавания лиц. К *недостаткам* можно отнести небольшой объем выборки, на которой производится тестирование, а также то, что фотографии из данного датасета умышленно или неумышленно могли входить в состав датасетов, использованных для обучения тестируемых алгоритмов, вследствие чего эти алгоритмы будут показывать идеальный результат на данном датасете.

2. Тестирование на основе датасетов «Megaface», созданных Университетом Вашингтона (США). Представлены открытые датасеты для тренировки (объемом 910 ГБ) и для проверки правильности соответствия (1 млн фотографий). Датасеты содержат фотографии более 672 тыс. личностей.

К *достоинствам* такого тестирования можно отнести большой объем выборки, на которой производится тестирование, к *недостаткам* – то, что фотографии из данного датасета могли умышленно включаться в состав датасетов, использованных для обучения тестируемых алгоритмов, с целью показа алгоритмами более высоких показателей в конкурсе.

3. Тестирование «Ongoing Face Recognition Vendor Test» (FRVT), проводимое Национальным институтом стандартов и технологий США (НИСТ). Данное тестирование состоит из двух частей – верификация и идентификация. Для тестирования используются закрытые датасеты, неизвестные участникам тестирования. Тестирование в таком виде проводится на постоянной основе с 2010 г.

К его *достоинствам* можно отнести закрытость датасетов, на основе которых проводится тестирование, всестороннее изучение точности и скорости работы алгоритмов распознавания лиц на датасетах различного качества и объема. К *недостаткам* – то, что для тестирования алгоритмы должны соответствовать определенным стандартам, быть оформлены в виде монолитного модуля и взаимодействовать с тестирующим программным обеспечением через интерфейс API C++.

Остановимся более подробно на тесте «FRVT 1:N Identification», к особенностям данного теста можно отнести следующее:

1) участникам тестирования неизвестны датасеты, на которых проводится тестирование;

2) при этом известно, что датасеты, на которых проводится тестирование биометрических систем, включают в себя основной датасет, состоящий из 26,6 млн портретных фотографий в отношении 12,3 млн личностей, сделанных в естественных условиях при умеренном контроле фотографируемых людей (из них 86 % – это фотографии лиц, доставленных в полицейский участок), и дополнительные датасеты, содержащие более «репортажные» фотографии, в том числе: 3,2 млн фотографий с веб-камер; 2,5 млн фото от фотожурналистов и фотолюбителей; 90 тыс. фотографий, вырезанных из видеопотоков;

3) тестирование биометрических систем производится по принципу «черного ящика» таким образом, что алгоритмы построения биометрических шаблонов и поиска и интеллектуальная собственность, связанная с ними, скрыты в предварительно скомпилированных библиотеках. Исходные тексты алгоритмов и программ не предоставляются участникам тестирования в НИСТ.

Участникам доступны следующие документы и программное обеспечение (далее – ПО): документированный API для взаимодействия с тестирующим ПО НИСТ на языке C++; ПО от НИСТ с исходными кодами на языке программирования C++ для проверки того, что биометрическая система, направляемая на тестирование, отвечает требованиям API; инструкции по шифрованию и подписыванию ПО биометрической системы с помощью электронной подписи перед его отправкой в НИСТ; инструкции по отправке ПО.

К биометрической системе, направляемой на тестирование, предъявляются следующие квалификационные требования:

– ПО должно быть скомпилировано для работы под управлением операционной системы Linux CentOS 7.6.1810 x86-64 (C++11 compiler, g++ version 4.8.5), операционная система Microsoft Windows не используется;

– размер биометрического шаблона должен быть не более 32 КБ;

– среднее время создания биометрического шаблона для изображения 640*480 на 1 ядре Xeon CPU E5-2630 v4 @ 2.20GHz должно составлять не более 1 секунды;

– среднее время поиска по галерее в 1 млн фото с выдачей рекомендательного списка размером 100 кандидатов должно составлять не более 10 секунд;

– с 2018 г. работа программного обеспечения на GPU не используется – только CPU;

– специфичные для процессоров семейства Intel инструкции (AVX2 и т. п.) можно использовать при компиляции «движка».

Отчет НИСТ [4] с приложением (далее – отчет NIST.IR.8271), подготовленный в сентябре 2019 г., включает в себя показатели производительности и точности для 203 прототипов алгоритмов (биометрических систем) от научно-исследовательских лабораторий 50 коммерческих разработчиков и одного университета из Китая, направленных в НИСТ в 2018 г. Российские разработчики представлены такими компаниями, как «НТехЛаб» (N-Tech Lab), «Вижнлабс» (VisionLabs), «Вокорд» (Vocord), «Синезис» (Synesys), «Тевиан» (Tevian).

Данное тестирование позволяет охватить большинство коммерческой индустрии распознавания лиц, но охват академического сообщества очень незначительный. Несмотря на то, что участие в тестировании бесплатное, разработчикам приходится приложить значительные усилия для того, чтобы адаптировать алгоритмы к единому программному интерфейсу (API) НИСТ.

В процессе тестирования, среди прочего, оценивается: размер исполняемых файлов биометрической системы; размер биометрического шаблона; время создания шаблона; время поиска с выдачей рекомендательных списков по галереям различной длины; точность поиска по датасетам различного качества с попаданием искомой фотографии в рекомендательные списки различной длины (ТОП-1, ТОП-20).

Как отмечают исследователи в отчете NIST.IR.8271, точность распознавания лиц значительно улучшилась за последние два десятилетия. НИСТ отслеживал данные улучшения путем проведения регулярных и общедоступных тестирований алгоритмов, что способствовало их совершенствованию в соответствии с современным развитием науки.

При этом отмечается, что несмотря на миграцию технологий распознавания лиц к СНС, до сих пор не достигнуто согласия по поводу оптимальных размеров биометрических шаблонов, указывая, таким образом, на разнообразие используемых подходов. Все еще нет перспективы получения стандартного биометрического шаблона, который предъявлял бы типовые требования к особенностям, извлекаемым из лиц. Функциональная совместимость в системах автоматизированного распознавания лиц остается целиком основанной на изображениях.

В отчете NIST.IR.8009 содержатся сведения о точности распознавания лиц для алгоритмов, представленных в НИСТ в октябре 2013 г., на основе набора данных «полицейских» фотографий задержанных лиц. В отчете NIST.IR.8271 отмечается, что при точном повторении того же испытания – поиск фотографий по галерее (списку) из 1,6 млн фотографий – самый точный алгоритм от июня 2018 г. делает в 20 раз меньше промахов[8], чем самый точный алгоритм 2013 г. «NEC E30C». Это означает, что примерно 95 % поисковых запросов, которые раньше заканчивались неудачей, теперь выдают корректный результат с рангом 1[9].

Отмечается, что для самых точных алгоритмов 2018 г. процент поисков, которые не выдают искомые объекты в ТОП-50, близок к нулю (или, что более точно, близок к тому проценту, который так или иначе существует из-за ошибок, служащих при разметке тестовых данных). Более того, корректный ответ (искомая сущность) почти всегда находится в самом начале рекомендательного списка. Таким образом, например, для самого точного алгоритма 2018 г. «Microsoft-4» при выполнении поиска по базе данных из 12 млн лиц процент поисков, которые не выдают искомое лицо на первом месте (ТОП-1), составляет всего 0,45.

Анализируя результаты тестов «Megaface Challenge 1», «Megaface Challenge 2», отчеты NIST.IR.8009 и NIST.IR.8271, можно согласиться с исследователями из НИСТ, что значительное сокращение числа промахов в последние пять лет (2014–2018 гг.) происходит за счет массовой замены старых алгоритмов, не использующих в своей работе нейронные сети, на алгоритмы, основанные на глубоких СНС. В этом состоит революция, а не эволюция алгоритмов, которая имела место в 2010–2013 гг. Последние инновации в данной области включают в себя такие достижения, как архитектуры сверточных нейронных сетей Resnet [6], Inception [7], «очень глубокие сети» [8], разработанные соответственно группами исследователей из Microsoft, Google, Оксфордского университета.

Реализация этих и других архитектур СНС на базе свободных библиотек машинного обучения, таких как PyTorch, TensorFlow, Keras и других, а также наличие все большего количества открытых датасетов, на которых возможно проводить обучение и тестирование алгоритмов распознавания лиц, способствуют стремительному развитию данной отрасли.

[8] Под промахом здесь подразумевается, что искомое лицо из галереи не попадает в рекомендательный список «ТОП-20».

[9] Под рангом 1 здесь подразумевается, что правильно найденное лицо присутствует в рекомендательном списке на 1-м месте.

Список литературы

1. ГОСТ ISO/IEC 19794-1–2015.
2. ISO/IEC 19794-1:2011, IDT.
3. *Grother P., Ngan M., Hanaoka K.* Ongoing Face Recognition Vendor Test (FRVT). Part 2: Identification // Technical Report 8238, National Institute of Standards and Technology (NIST). November 2018. DOI: 10.6028/NIST.IR.8238.
4. *Grother P., Ngan M., Hanaoka K.* Face Recognition Vendor Test (FRVT). Part 2: Identification // Technical Report 8271, National Institute of Standards and Technology (NIST). September 2019. DOI: 10.6028/NIST.IR.8271.
5. *Grother P., Ngan M.* Face Recognition Vendor Test (FRVT). Performance of Face Identification Algorithms // NIST Interagency Report 8009. May 2014. DOI: 10.6028/NIST.IR.8009.
6. *He K., Zhang X., Ren S., Sun J.* Deep residual learning for image recognition // Conference on Computer Vision and Pattern Recognition (CVPR). June 2016.
7. *Szegedy C., Liu W., Jia Y. et al.* Going deeper with convolutions. 2014.
8. *Simonyan K. and Zisserman A.* Very deep convolutional networks for large-scale image recognition. 2014.

А. О. БУРЦЕВ,
начальник отделения научно-исследовательского центра,
кандидат психологических наук
(Академия управления МВД России)

Н. В. ЕФИМКИНА,
старший преподаватель кафедры юридической психологии,
кандидат психологических наук
(УНК ПСД МосУ МВД России имени В. Я. Кикотя)

Л. Н. КИСЕЛЕВА,
слушатель факультета психологии служебной деятельности
органов внутренних дел
(МосУ МВД России имени В. Я. Кикотя)

Влияние социально-психологического климата на успешность обучения курсантов образовательных организаций системы МВД России

Обеспечение и поддержание благоприятного социально-психологического климата любого служебного коллектива является одной из основных задач деятельности ОВД. Социально-психологический климат является фактором, через который, преломляясь, опосредуется любая деятельность коллектива, в том числе и служебного. При этом преобладает настрой коллектива, определяющий не только меру включенности каждого курсанта [1] образовательной организации МВД России в деятельность, но и характер ее направленности, ее эффективность.

Группа всегда занимает особое место в системе общественных отношений, а в ее сознании отражаются элементы общественного сознания.

Цель нашего исследования состояла в изучении влияния социально-психологического климата на успешность обучения курсантов образовательных организаций системы МВД России.

Этой теме посвящено немалое количество публикаций, в которых рассматриваются как общие вопросы, связанные с характеристикой природы, роли и факторов социально-психологического климата, так и специальные вопросы данной проблемы. В их числе – регулирование и управление, формирование и совершенствование, особенности функционирования социально-психологического климата учебного коллектива [2].

Чтобы научить владеть способами общения с людьми, в том числе для создания благоприятного климата в служебном коллективе, необходима системная работа начальника курса, педагога, психолога и младших командиров учебных групп. От социально-психологического климата коллектива зависит не только результативность совместной деятельности,

но и отношение к труду, эмоциональный настрой, а также удовлетворенность деятельностью в целом.

Под социально-психологическим климатом в коллективе понимается тот психологический настрой, который существует в учебной группе.

К основным факторам психологического климата в коллективе следует отнести:

– уровень сложившихся в нем взаимоотношений по горизонтали и по вертикали;

– стиль руководства коллективом;

– сложившиеся внутриколлективные нормы взаимоотношений;

– хорошо организованная производственная обстановка (условия, в которых протекает деятельность, система морального стимулирования).

Характерологические особенности социально-психологического климата коллектива определяет степень его развитости. Социально-психологический климат внутриколлективных отношений положительно связан с эффективной совместной деятельностью членов этого коллектива и их межличностным взаимодействием. Он проявляется в коллективных мнениях, настроениях, индивидуальном самочувствии и оценках жизнедеятельности личности в коллективе.

Психологическое своеобразие личности может способствовать либо мешать становлению чувства коллективной общности, то есть является важным фактором формирования благоприятного социально-психологического климата внутригрупповых отношений.

Для эффективного управления служебными коллективами необходимо опираться на данные, получаемые психологом в процессе социально-психологических обследований подразделений.

Эмпирической базой исследования послужило изучение результатов экзаменационных сессий курсантов, социально-психологического климата в данных учебных взводах. В исследовании приняли участие курсанты одной из образовательных организаций МВД России.

С помощью программы «Социально-психологический мониторинг», разработанной доктором психологических наук М. И. Марьиным, было произведено исследование СПК и МПС курсантов образовательных организаций МВД России. Полученные данные могут использоваться для совершенствования работы со служебными коллективами. Данная программа предназначена для проведения СПО служебных коллективов.

На I этапе было проведено исследование социально-психологического климата курсантов 3-го и 4-го курсов.

На II этапе был проведен анализ весенне-летней сессии 2017/2018 учебного года, а также зимней сессии 2018/2019 учебного года.

На III этапе проводился сравнительный анализ результатов СПК и учебной успеваемости.

На диаграммах мы видим, что чем благоприятней социально-психологический климат в коллективе, тем выше показатели экзаменационной сессии.

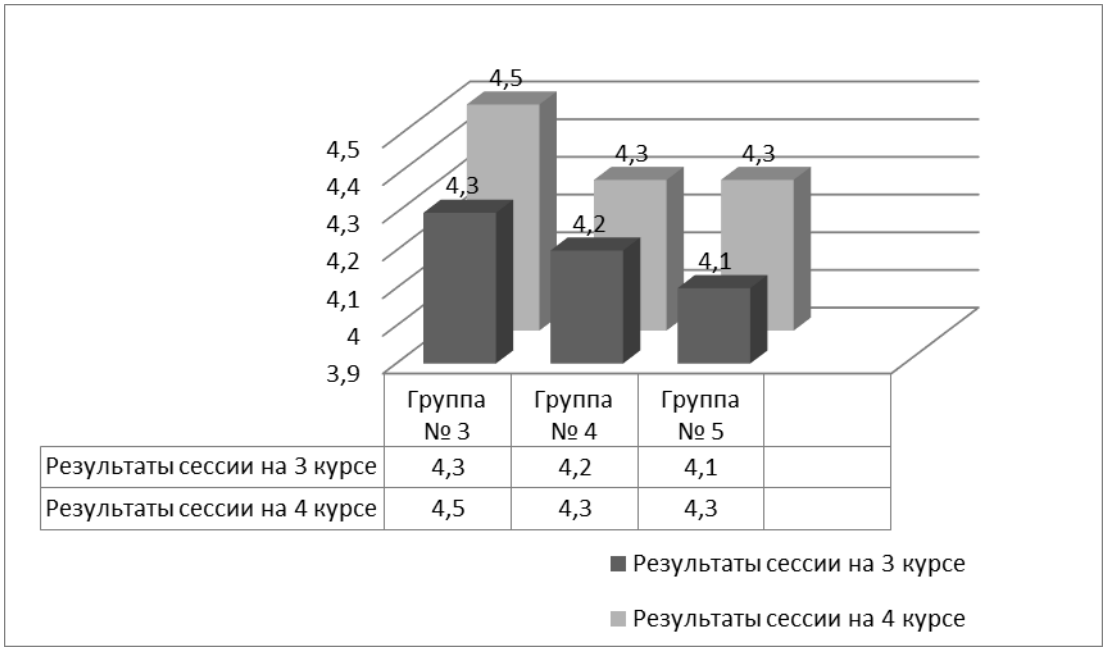

Рис. 1. Сравнение среднего балла экзаменационной сессии курсантов 3-й, 4-й, 5-й группы, обучающихся на 3-м и 4-м курсе

Таким образом, полученные результаты свидетельствуют о том, что на эффективность учебной деятельности курсантов образовательной организации системы МВД России большое влияние оказывает общее морально-психологическое состояние в коллективе.

Список литературы

1. *Андрианова О. В.* Влияние социально-психологического климата на формирование учебной деятельности студенческих коллективов. URL: http://dlib.rsl.ru/rsl01000000000/rsl01000217000/rsl01000217418/rsl01000217418.pdf (дата обращения: 10.11.2019).
2. *Бурцев А. О., Ефимкина Н. В.* Психологические аспекты организационно-штатных изменений в системе органов внутренних дел Российской Федерации // Прикладная юридическая психология. 2016. № 4. С. 109–112.
3. *Марьин М. И., Петров В. Е., Ульянина О. А.* Особенности психологического обеспечения в подготовке специалистов в образовательных организациях МВД России // Труды Академии управления МВД России. 2016. № 1 (37). С. 85–90.
4. URL: http://mirreferatov.com.ua/referat/ru/psihologiya/sotsialno-psihologicheskiy-klimat-v-trudovom-kollektive.html (дата обращения: 10.11.2019).

О. В. ВИШНЕВСКИЙ,
слушатель Академии управления МВД России

В. Ю. ПЕТРОВА,
доцент кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

О некоторых аспектах анализа ситуации обеспечения работоспособности программно-технических комплексов в территориальном органе МВД России

Анализ рисков в сфере оценки работоспособности программно-технических комплексов территориального органа МВД России необходимо начинать с идентификации всех объектов (активов), которые нуждаются в защите. Идентификацию некоторых объектов (например, коммуникационного оборудования) можно произвести очевидным образом, при этом другие объекты (например, люди, имеющие доступ к информационным системам) часто остаются без должного внимания. На наш взгляд, должно быть учтено все, чему может быть нанесен ущерб вследствие нарушения режима безопасности.

Достаточно корректной является следующая классификация объектов:

– программное обеспечение: исходные тексты, утилиты, объектные модули, операционные системы, диагностические программы, коммуникационные программы;

– аппаратное обеспечение: модули, процессоры, терминалы, клавиатуры, персональные компьютеры, рабочие станции, дисководы, принтеры, терминальные серверы, коммуникационные линии, маршрутизаторы, мосты;

– люди: обслуживающий персонал, пользователи;

– данные: непосредственно доступные, обрабатываемые, сохраненные в виде резервной копии, архивированные, базы данных, регистрационные журналы, данные, которые передаются по коммуникационным сетям.

В таблице приведено итоговое ранжирование информационных объектов в соответствии со степенью риска для территориального органа МВД России.

Наименование объекта	Ранг (ценность) объекта
Автоматизированная информационная система территориального органа МВД России	1
База данных ИС	1

БД ИМТС (интегрированная мультисервисная телекоммуникационная система МВД России)	1
Почтовый сервер	1
Распоряжения, приказы начальника территориального органа МВД России	1
Документы конфиденциального характера	2
Отчеты о деятельности отделов	2
Работа с персоналом	3
Здания, сооружения, оборудование, транспортные средства	4

Следовательно, можно выделить объекты, которые представляют наибольшую ценность с точки зрения информационной безопасности:

– сервер баз данных с информацией оперативного и конфиденциального характера;

– база данных ИС (поддержка деятельности подразделения полиции, отдела предварительного следствия и управления делопроизводства и режима);

– распоряжения, приказы начальника территориального органа МВД России;

– почтовый сервер.

Оценку угроз, уязвимостей и рисков информационной безопасности и работоспособности программно-технических комплексов целесообразно осуществлять именно для вышеперечисленных объектов.

Проведение оценки уязвимостей является допустимым не только по отношению к компьютерным сетям/системам, но и для многих других активов. Например, вполне допустима оценка здания на предмет наличия изъянов у его определенных частей. Если у взломщика существует возможность обхода охранника у турникета на входе или проникновения в здание через другие входы, то это, конечно, следует считать уязвимостью. При фактическом осуществлении подобного действия это называется эксплойтом. Вообще, физическая безопасность может быть отнесена к наиболее важным аспектам, которым должно быть уделено должное внимание. Действительно, в случае кражи сервера у злоумышленника уже будет отсутствовать необходимость в обходе системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), ему уже не требуется изыскивать способ получения информации с сервера, так как она уже у него вместе с сервером. В таком случае полезным может оказаться шифрование диска, однако использование подобного способа защиты на серверных дисках встречается крайне редко[10].

В качестве объектов защиты могут быть приняты следующие виды информационных ресурсов территориального органа МВД России:

[10] *Нестеров С. А.* Информационная безопасность: учебник и практикум. М., 2017.

– информация, которая хранится в базах данных, на файловых серверах и рабочих станциях, в почтовых ящиках пользователей внутренней сети и т. д.;

– информация (телефонные переговоры, факсы, данные), передача которых осуществляется по каналам связи;

– информация конфигурационного характера, а также протоколы работы сетевых устройств и программных комплексов и систем[11].

Моделирование риска можно провести на основе анализа угроз информационной безопасности и работоспособности программно-технических комплексов в сети территориального органа МВД России[12]. Технология расчета рисков R может быть реализована в случае оценки вероятности возникновения угрозы P_T, которая может привести к урону для территориального органа МВД России, и $P_V(z)$ – функции зависимости реализации заданной угрозы от вложений в информационную безопасность территориального органа. Однако вероятность хранения не только в базе ИС, но и в архивах конфиденциальной информации и коммерческой тайны не позволяет корректно определить функциональную зависимость реализации заданной угрозы от вложений в информационную безопасность территориального органа МВД России[13].

Тогда в качестве функциональной зависимости рассматривается дискретная функция и возможно применение стандартной матрицы рисков, разработанной согласно рекомендациям NIST.

Решение проблемы организации обеспечения работоспособности программно-технических комплексов для ОВД лежит в нескольких плоскостях, которые можно представить следующим образом:

– контроль за состоянием оборудования и выполнением своевременных текущих ремонтов, проведение профилактических работ;

– поддержка работоспособного состояния оборудования и программного обеспечения;

– оптимизация процесса выполнения поставленных задач сотрудниками ОВД с учетом имеющихся средств.

В связи с насущностью проблемы такого характера для всех видов современных организаций уже созданы специализированные инструменты, ориентированные на комплексное решение таких задач. Это системы

---

[11] *Шурховецкий Г. Н.* Безопасность информационного обеспечения экспертной и следственной деятельности МВД РФ // Актуальные вопросы инженерно-технических экспертиз: материалы всероссийской научно-практической конференции. 2018. С. 14–22.

[12] *Безмельников Ю. Ю.* Актуальные проблемы анализа и оценки рисков нарушения информационной безопасности информационных систем управления МВД России по Калининградской области (с учетом перехода в ЦОД) // Публичное и частное право. 2014. № 2 (22). С. 178–189.

[13] *Лукьянов Н. Е., Пилипушка С. В.* Деятельность органов внутренних дел по осуществлению информационной безопасности // Научное сообщество студентов XXI столетия. Общественные науки. 2018. № 1 (60).

поддержки IT-инфраструктуры, помогающие не просто проводить мониторинг работоспособности оборудования, но и перестроить работу всей IT-службы для оптимизации его деятельности.

Предлагаемые на рынке популярные ITSM-системы не являются актуальными в случае работы в территориальном органе МВД России, так как ни одна из них не имеет сертификат ФСТЭК соответствия по уровню защищенности от несанкционированного доступа к информации.

Подводя итог, можно констатировать, что перед территориальными ОВД еще достаточно много нерешенных вопросов в области обеспечения безопасности информационных ресурсов, которые невозможно осветить в рамках одной статьи.

Д. А. ГАВРИЛОВ,
руководитель лаборатории
цифровых систем специального назначения,
кандидат технических наук
(МФТИ)

Н. Н. ЩЕЛКУНОВ,
заместитель заведующего кафедрой радиоэлектроники
и прикладной информатики,
кандидат технических наук
(МФТИ)

Возможности применения автоматизированной оптико-электронной системы наземно-воздушного мониторинга в деятельности ОВД

Введение

Системы автоматизированной обработки и анализа изображений все более интенсивно применяются в различных областях деятельности человека. Несмотря на то, что существует достаточно большое количество разработанных и реализованных алгоритмов обнаружения, локализации и классификации графических объектов, проведение исследований в данной области не теряет актуальности [1]. В свою очередь, актуальность разработки автоматизированных оптико-электронных систем наземно-воздушного мониторинга обусловлена значительными перспективами внедрения искусственного интеллекта для предупреждения преступности, а также максимально быстрого реагирования на совершаемые преступления. Рутинные задачи, ранее выполняемые человеком-оператором, берет на себя искусственный интеллект. В настоящей работе рассматриваются подходы к решению задач сбора, обработки и хранения визуальной информации, использующейся в сфере безопасности, а также вопросы внедрения систем технического зрения и методов машинного обучения в практику деятельности ОВД.

Основные тенденции развития в области автоматизированной обработки визуальной информации

Одним из главных направлений, требующих развития автоматизированной обработки изображений, являются системы технического зрения. Перед разработчиками систем такого типа остро встают проблемы преобразования визуальной информации в аналитические данные, в том числе в режиме реального времени в условиях высоких скоростей движения мобильных объектов сложной формы в различных фоноцелевых обстановках. При этом каждая задача технического зрения, как правило, требует разработки оптимальных подходящих для данного типа задачи алгоритмов [2]. Универсальные способы и алгоритмы решения задач обнаружения, локализации и классификации пока не найдены.

Одним из основных требований к оптико-электронной системе является способность без участия оператора выделять во входном видеопотоке объекты интереса и осуществлять слежение за данными объектами. При этом обработка информации, получаемой оптико-электронной системой, должна осуществляться в автоматическом режиме. Таким образом, оптико-электронная система приобретает роль «органов зрения», ключевым моментом построения которых является необходимость реализации качественного алгоритма обнаружения объектов.

Одной из проблем в области автоматизированной обработки изображений является обеспечение высокой точности решения конкретных поставленных задач, устойчивых к различным оказывающим негативное влияние агрессивным факторам, с четко обозначенным и исследованным диапазоном применимости, а также повышение информационной добротности автоматизированных оптико-электронных систем переработки визуальной информации и анализа фоноцелевой обстановки [3, 4].

Общей тенденцией развития систем технического зрения является совершенствование методов и средств формирования и обработки зрительной информации. Современные цифровые средства формирования изображений охватывают практически весь электромагнитный спектр от гамма-излучения до радиоволн [5]. Полученные изображения позволяют проводить неограниченное число операций и процедур по их обработке, существенно отличающихся по сложности реализации. Тем не менее основной целью данных операций является получение информации описательного характера, позволяющей производить расширенный логический анализ имеющихся графических данных.

Процесс переработки визуальной информации охватывает широкий спектр методов, имеющих различное применение. Из множества методов выделяется определенный их набор с целью построения алгоритмов для решения конкретных поставленных задач.

Построение эффективной АОЭС представляется возможным на основе применения проблемно-ориентированного варианта комплексного ИКСД-подхода (информационно-кибернетически-синергетически-дидактического) [1], т. е. системного подхода с акцентированием внимания на его информационном, кибернетическом, синергетическом и дидактическом аспектах, состоящего в интеграции методологии информационного подхода (при котором объект рассматривается как целенаправленная информационная система), методологии кибернетического подхода (при котором объект рассматривается как система управления на уровне информационных процессов и алгоритмов функционирования информационной базы), методологии синергетического подхода (при котором объект рассматривается как динамическая самоорганизующаяся система, взаимодействующая со средой) и методологии дидактического подхода (при котором объект рассматривается как система, способная к самообучению) [6].

Основная функциональность автоматизированных оптико-электронных систем наземно-воздушного мониторинга

Основную функциональность АОЭС НВМ составляет решение задач детектирования, локализации и классификации объектов на фото- и видеоданных применительно к различным фоноцелевым обстановкам. Основные трудности при решении данных задач возникают вследствие: потери информации при проецировании трехмерной сцены на плоскость изображения; наличия шума на изображении; изменения экспозиции сцены; сложной формы объектов; изменения формы объекта; частичных или полных перекрытий и загораживаний объектов сцены; сложной траектории движения объекта; выхода объекта за пределы кадра и появления объекта в кадре; относительного движения камеры; требований обработки в реальном времени.

Все шаги по переработке визуальной информации, как правило, представляют собой последовательное удаление из изображения неинформативных компонент и выделение информативных для решения поставленной задачи. Иерархия методов включает процессы низкого, среднего и высокого уровня. Особенностью низкого уровня обработки является то, что и на входе, и на выходе процесса присутствуют изображения. В процессах среднего уровня изображение поступает только на вход, выходными данными являются результаты анализа, качественные особенности и отличительные свойства, извлекаемые из входных изображений объектов. Высокоуровневая обработка включает в себя методы анализа непосредственно найденных объектов и осуществление познавательных функций, связанных со зрением. Методы высокоуровневой обработки обеспечивают извлечение данных из изображений и дальнейший анализ полученной информации.

Выбор метода обработки изображения, полученного техническими средствами, определяется исходя из характера данного изображения и задач, которые необходимо решить.

Разведывательно-аналитический автоматизированный комплекс «Автопол»

На основе представленных теоретических положений осуществляется разработка разведывательно-аналитического автоматизированного комплекса «Автопол», представленного на XXIII Международной выставке средств обеспечения безопасности государств «Интерполитех – 2019». Внешний вид комплекса показан на рис. 1.

Рис. 1. Внешний вид разведывательно-аналитического автоматизированного комплекса «Автопол»

Комплекс «Автопол» включает совокупность алгоритмического, радиоэлектронного и вычислительного обеспечения, интегрированного с транспортными модулями наземного или воздушного базирования различного типа и позволяет осуществлять оперативное наблюдение за обстановкой с воздуха и с земли.

Комплекс включает следующие подсистемы:

- подсистема воздушного мониторинга представляет собой беспилотный летательный аппарат, оснащенный оптико-электронными и тепловизионными системами наблюдения;
- подсистема наземного мониторинга представляет собой автомобиль с системой автоматического управления, оснащенный оптико-электронными, тепловизионными и радиолокационными системами наблюдения;
- пункт командного управления обеспечивает интеграцию подсистем в единый комплекс и предназначен для сбора, анализа и визуализации воздушной и наземной обстановки.

Технические характеристики комплекса «Автопол» представлены в таблице.

Наименование	Подсистема воздушного мониторинга	Подсистема наземного мониторинга
Система спутниковой и инерционной навигации	✓	✓
Система круглосуточного наблюдения	✓	✓
Камера видимого диапазона	✓	✓
Тепловизионная камера	✓	✓
Система радиовидения с диапазоном 3 мм		✓
Радиоканал для передачи цифровых изображений	✓	✓
Функционал обнаружения, классификации и сопровождения объекта интереса	✓	✓

Автоматизированный комплекс «Автопол» разрабатывается в рамках ведомственной программы МВД «ЦИФРОПОЛ» и предназначен для обеспечения ситуационной осведомленности и оперативной передачи информации. В качестве основы для тестового автомобиля взят гибридный седан Toyota Prius последнего поколения. Оптико-электронные схемы обеспечивают 360-градусный видеообзор в двух спектрах, за счет чего можно создать модель пространства, в котором перемещается машина.

Выводы

Представлены основные подходы к решению задач сбора, обработки и хранения визуальной информации, использующейся в сфере безопасности, а также рассмотрены вопросы внедрения систем технического зрения и методов машинного обучения в практику деятельности ОВД.

Рассмотренные предложения представляют теоретико-прикладную значимость при решении задач разработки эффективных автоматизированных оптико-электронных систем наземно-воздушного назначения, обеспечивающих переработку многоаспектной визуальной информации, и позволяют значительно повысить эффективность

использования имеющихся методов и средств детектирования, локализации и классификации изображений и, как следствие, улучшить качество распознавания визуальной информации, обеспечить конфиденциальность переработки информации, а также повысить сохранность и достоверность оценки ситуаций в условиях интенсивного информационного соперничества и непрерывно меняющейся обстановки.

Список литературы

1. *Ловцов Д. А., Гаврилов Д. А.* Моделирование оптико-электронных систем дистанционно пилотируемых аппаратов: монография. М., 2019.

2. *Гаврилов Д. А., Местецкий Л. М., Семенов А. Б.* Метод разметки изображений самолетов на аэрокосмических снимках на основе непрерывных морфологических моделей // Программирование. 2019. № 6.

3. *Гаврилов Д. А., Павлов А. В., Щелкунов Д. Н.* Аппаратная реализация сжатия динамического диапазона цифровых изображений на ПЛИС Xilinx // Журнал радиоэлектроники. 2018. № 10.

4. *Гаврилов Д. А., Павлов А. В.* Поточная аппаратная реализация алгоритма SURF // Известия вузов. Электроника. 2018. № 5.

5. *Гаврилов Д. А., Мелерзанов А. В., Щелкунов Н. Н., Закиров Э. И.* Применение технологий глубокого обучения для диагностики кожных заболеваний на основе нейронных сетей // Медицинская техника. 2018. № 5.

6. *Ловцов Д. А., Гаврилов Д. А.* Формализация проблемы обеспечения эффективности автоматизированной оптико-электронной системы специального назначения // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем. Серпухов, 2019.

Ш. Х. ГОНОВ,
старший преподаватель кафедры информационных технологий,
кандидат технических наук
(Академия управления МВД России)

Применение технологии машинного обучения в информационно-аналитической деятельности органов внутренних дел

В современных условиях функционирования правоохранительных органов, в период бурного развития информационно-телекоммуникационных технологий, экспоненциального роста накопленных массивов данных и нестабильного состояния внешней среды наиболее востребованными являются технологии поддержки принятия решений. Очевидно, что потенциал современных систем управления базами данных и существующих интеллектуальных систем обработки данных близок к своему пределу. В ОВД за последние несколько лет накоплен значительный объем структурированной и неструктурированной информации о состоянии преступности, о результатах деятельности по выявлению и раскрытию преступлений и т. п. Решить возникающие проблемы можно за счет применения в аналитической деятельности современных методов анализа данных. Речь идет о технологиях больших данных и искусственного интеллекта.

Наиболее востребованными в аналитической работе становятся перспективные системы искусственного интеллекта. Актуальность этого направления в решении задач анализа данных получила новый вектор своего развития в октябре 2019 г., когда была утверждена Национальная стратегия развития искусственного интеллекта в России до 2030 года [1]. Примечательно то, что этот нормативный акт тесным образом связан со Стратегией развития информационного общества Российской Федерации на 2017-2030 годы и с национальной программой «Цифровая экономика Российской Федерации».

Вопросы применения методов машинного обучения рассматривались в работах многих отечественных специалистов. Вместе с тем применительно к оперативно-служебной деятельности ОВД технологии искусственного интеллекта рассматривались в недостаточной степени [2, 3, 4, 5, 6]. Заметим, что технологии больших данных наибольший эффект дают при обработке структурированной и неструктурированной информации. Вместе с тем практически все банки данных, формируемые в ОВД, имеют четко выраженную структурно-логическую схему, описанную в терминах реляционных баз данных. Объем же накопленных слабоструктурированных и неструктурированных данных занимает в общем массиве банков данных незначительное место и существенного влияния на энтропию не оказывает. Заметим также, что под большими данными в отечественной литературе

чаще всего понимают только сами данные, а не технологии, как это принято на Западе.

В настоящее время считается, что основным классом методов искусственного интеллекта является машинное обучение. Строго говоря, машинное обучение – это методы поиска зависимостей между объектами на основе применения готовых решений сходных задач. Между тем методы машинного обучения принято разделять на две большие группы – обучение с учителем и без учителя. Обучение с учителем – это построение прогнозных моделей, предполагает в первую очередь применение двух задач – классификации и регрессии.

В общем виде указанную выше модель регрессии можно представить следующим образом, в том числе факторы, оцениваемые по качественной шкале:

$$U^*(Y) = \beta_0 + \sum_{j=1}^{k} \beta_j x_j + \sum_{i=1}^{m} c_i z_i + \varepsilon, \qquad (1)$$

где x_j – факторы внешней среды, β_0, β_j, c_i – оцениваемые коэффициенты модели, ε – случайная компонента.

К сожалению, применение регрессионного анализа осложняется отсутствием качественных данных о состоянии внешней среды, особенно социально-экономических факторов. Рассмотрим постановку задачи принятия решения с применением моделей дискретного выбора.

Отличительной особенностью моделей дискретного выбора является возможность перехода от непрерывных значений $U^*(Y)$ в модели (1) к дискретным значениям. Так, по *logit*-модели, использующей бинарную переменную в качестве зависимой и имеющей вид стандартного логистического распределения $F(u) = \Lambda(u) = \frac{e^u}{1+e^u}$, строится функция правдоподобия *PP*.

Обозначим $P(Y_i=y_i|X_{1i}, X_{2i},\ldots, X_{ki})$ вероятность того, что предсказанная зависимая переменная y_i равна значению Y_i с учетом значений независимых переменных $X_{1i}, X_{2i},\ldots, X_{ki}$. В сокращенном виде $P(Y=y|X)$:

$$P(Y=y|X)=P(X)^Y \cdot [1-P(X)]^{(1-Y)}. \qquad (2)$$

Прологарифмировав обе части (2), получим:

$$ln[P(Y=y|X)]=y \cdot ln[P(X)] \cdot (1-y) \cdot ln[[1-P(X)]]. \qquad (3)$$

Тогда функция правдоподобия $PP=\sum ln[P(Y=y|X)]=$

$\sum Y_i \cdot P(X_i)+(1-Y_i)(1-P(X_i))$, где $P(x) = P(x) = \frac{e^L}{1+e^L}$.

Аналитическая работа в ОВД является неотъемлемой частью функционирования автоматизированных информационных систем. Очевидно, что в данной области они должны применяться на основе некоторых базовых принципов. Во-первых, аналитическая работа должна основываться на системе взаимосвязанных показателей, характеризующих эффективность управления. Во-вторых, аналитическая деятельность должна носить непрерывный характер, т. е. с момента ввода данных до выдачи агрегированных сведений. В-третьих, аналитическая работа должна проходить в диалоговом режиме при помощи автоматизированных систем поддержки принятия управленческих решений в режиме взаимодействия «человек-машина».

Исходя из изложенного, можно выделить два основных направления совершенствования информационно-аналитической работы в правоохранительной сфере. Первое заключается в улучшении самой технологии сбора и обработки статистических данных о состоянии преступности и результатов оперативно-служебной деятельности ОВД. Данное направление в первую очередь связано с поиском путей решения недостатков самой системы учета и регистрации преступлений, которая в свою очередь зависит от существующей системы права. Второе направление заключается в разработке специализированной системы поддержки принятия решений, ориентированной на применение разноообразных моделей анализа данных. Очевидно, что СППР должна разрабатываться в рамках основополагающих принципов информатизации ОВД: системности, открытости, консолидации данных и направленного развития. Следовательно, разрабатываемая СППР должна легко интегрироваться в качестве составного компонента в существующую единую систему информационно-аналитического обеспечения деятельности МВД России (далее – ИСОД) и эффективно взаимодействовать с интегрированными банками данных (далее – ИБД), предназначенными для формирования и ведения оперативно-справочных, криминалистических, разыскных учетов, а также со ссылочными массивами (далее – СМ) банков данных статистической информации. Ниже представлена концептуальная схема модели (рис. 1).

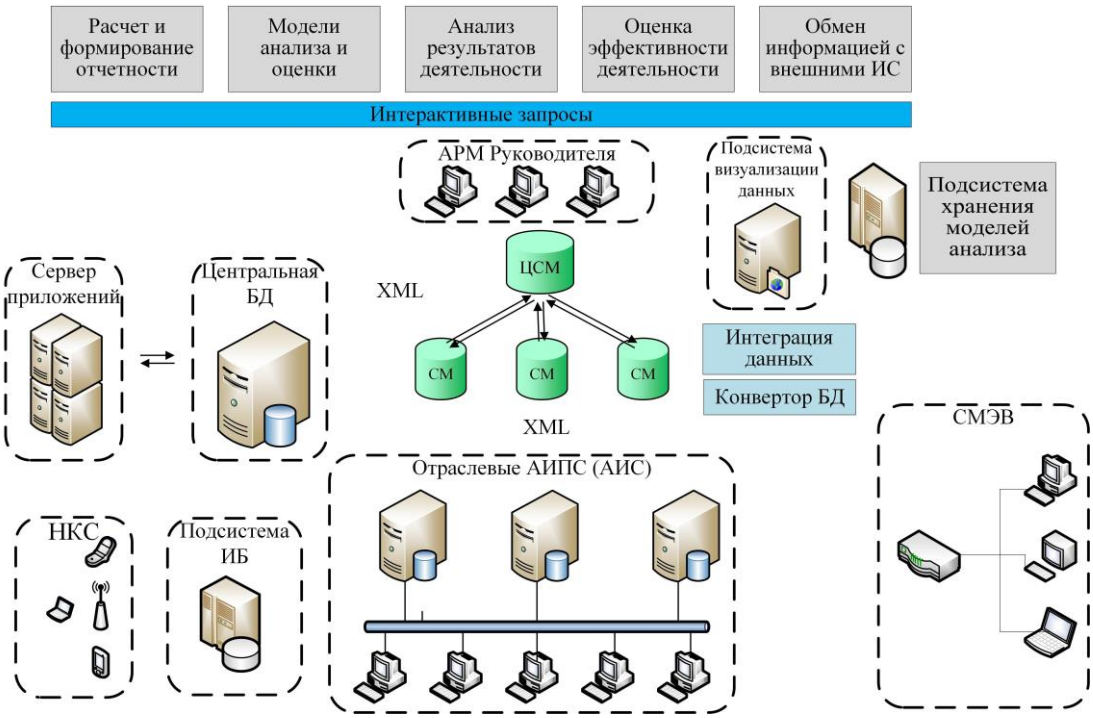

Рис. 1. Концептуальная схема автоматизации

В отличие от традиционного подхода к понятию информационно-аналитической работы как специфической деятельности, присущей в основном штабным подразделениям, мы считаем, что данный вид деятельности осуществляется на всех звеньях и уровнях управления ОВД. Настоящее исследование показало, что процесс информационно-аналитической деятельности должен состоять из трех последовательных и взаимообусловленных этапов: обработка первичной информации; моделирование и прогнозирование; оценка результатов. На первом этапе осуществляется сбор, обработка, обобщение и первичный анализ информации. На этом этапе важную роль играет качество и достоверность первичной информации, ее всесторонность и глубина. На этапе моделирования и прогнозирования осуществляется разработка и обоснование методов и моделей анализа результатов деятельности территориальных органов, объяснение причин роста (снижения) преступности и правонарушений, а также построение прогнозов. Заключительный этап характеризуется подготовкой выводов и оценки эффективности деятельности территориальных органов на основе проведенного анализа. Как было показано ранее, для этого этапа характерна оценка состояния внешней среды функционирования территориального органа (социально-экономическая и демографическая ситуация, ее насыщенность криминогенными факторами и т. п.). Схематичное отображение данного процесса с указанием основных компонентов представлено на рис. 2.

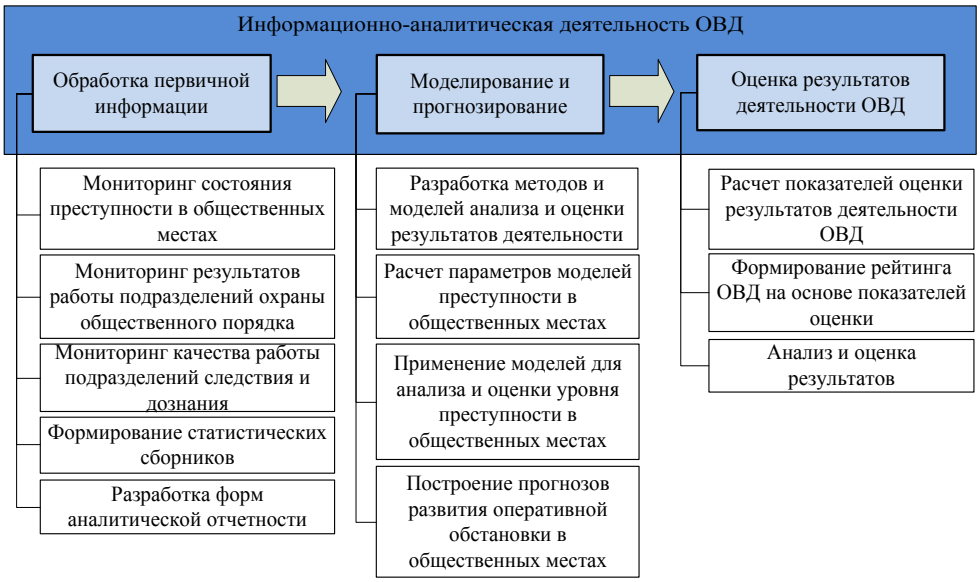

Рис. 2. Информационно-аналитическая деятельность ОВД

Совершенствование информационно-аналитической работы может достигаться только за счет повышения качества управления в ОВД. Данная задача достигается путем формирования сбалансированной и объективной системы критериев оценки результатов деятельности ОВД. Очевидно, что решить ее можно за счет разработки информационной системы поддержки принятия решений. На первом этапе разработки необходимо определение функционально-целевого назначения системы. Так, разрабатываемая СППР предназначена для:

– автоматизации процесса принятия управленческих решений;

– автоматизации процесса обработки данных о состоянии преступности, результатах оперативно-служебной деятельности.

Дальнейшие действия по разработке СППР связаны с уточнением функционального назначения основных компонентов системы. Общая структурная схема распределения подсистем и компонентов разрабатываемой СППР с указанием информационных связей между ними представлена на схеме (рис. 3). Центральным элементом данной схемы является подсистема хранения моделей анализа данных, которая связана с другими функционально-логическими подсистемами: обработки, хранения и анализа данных. Как уже отмечалось, добиться повышения эффективности информационно-аналитической деятельности ОВД возможно только при применении математического моделирования на постоянной основе. Следовательно, при разработке СППР должна быть предусмотрена возможность применения ранее разработанных моделей анализа данных.

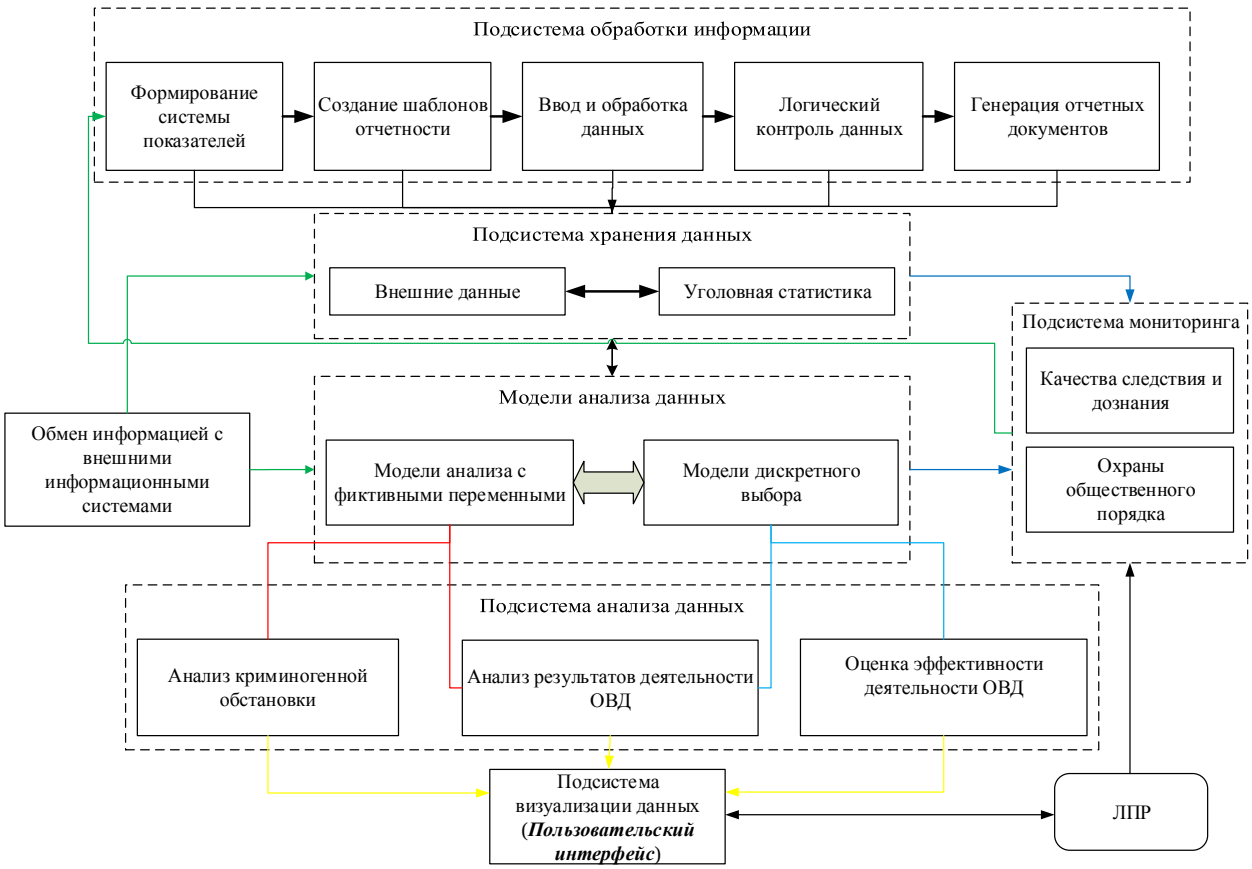

Рис. 3. Общая структурная схема компонентов СППР

Рассмотрим описанную выше структурную схему в терминах реляционной модели базы данных (далее – БД). Для реализации выполнения запросов к БД практически любая современная система управления базами данных (СУБД) оснащается структурированным языком запросов (*SQL – structured query language*). Следует отметить, что в настоящее время в *SQL* принято выделять в виде самостоятельной компоненты язык манипулирования данными (*DML – data manipulation language*), включающий операторы *SELECT*, *INSERT*, *UPDATE*, *DELETE*. Оператор выборки данных *SELECT* имеет следующий вид:

SELECT a_1, a_2, …,a_n
FROM r_1, r_2, …,r_m
WHERE <условие запроса>,

где a_1, a_2, …,a_n ($n \geq 1$) – выбираемые поля; r_1, r_2, …,r_m ($m \geq 1$) – таблицы БД; *<условие запроса>* – условия, накладываемые на записи таблиц r_1, r_2, …,r_m, формирующиеся на основе булевой логики и включающие в себя соответствующие отношения (*NOT*, *AND*, *OR*).

Данные о параметрах моделей хранятся в таблице (*Models*) и состоят из следующих основных полей: *Name* – наименование модели (**CHAR**); *Type* – тип модели (**INTERGER**) (1 – линейная; 2 – нелинейная; 3 – квадратичная; 4 – модель дискретного выбора); *Data Structure* – структура набора данных (**INTERGER**) (1 – пространственные; 2 – временные; 3 –

панельные); *Level* – уровень применения модели (**INTERGER**) (1 – федеральный; 2 – межрегиональный; 3 – региональный; 4 – территориальный).

Например, ЛПР необходимо проанализировать данные о криминогенной обстановке на территории Кабардино-Балкарской Республики. Для выборки из БД информации о моделях, удовлетворяющих сформулированным требованиям ЛПР, будет сформирован запрос следующего вида: SELECT *Name* FROM *Models* WHERE *Level*=3 AND (*Type*=1 OR *Type*=3).

Классическая реляционная модель данных, используемая для описания такой структурно-сложной системы данных, как уголовная статистика, не всегда удобна для обработки запросов, поскольку при их формировании требуется детальное знание структуры БД. Данное ограничение сложно решить стандартными средствами разработки АИС. Разработка модели, создаваемой в терминах прикладной области, может обеспечить повышение качества и сокращение сроков разработки нетиповых задач на основе технических заданий, формируемых ФКУ «ГИАЦ МВД России» (рис. 4).

Создание слоя метаданных в БД в период проектирования и разработки технических заданий упрощает процесс разработки выходных аналитических данных. Реализация набора интуитивно понятных инструментов формирования запросов, генерации отчетов и анализа обеспечивает ЛПР оперативный доступ к информации в БД. В то же время реализация единых и понятных правил логического контроля, выборок списков и расчета элементов уголовной статистики должна способствовать повышению качества и достоверности статистической информации.

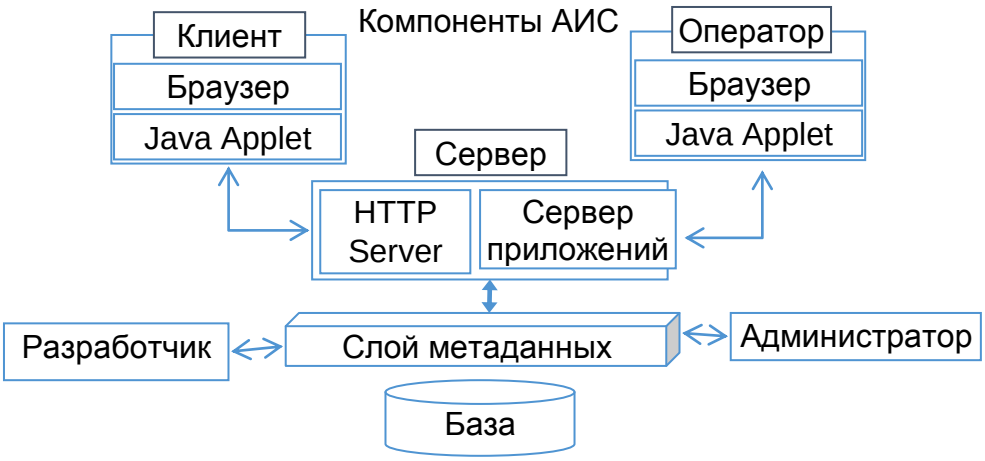

Рис. 4. Логическая модель данных

В результате при разработке и внедрении аналитических отчетов (табличных или списочных) представится возможность оперировать понятиями прикладной логики, исключив необходимость постоянного участия в разработке технических специалистов информационных центров.

Таким образом, разработка специализированного инструментального средства, обеспечивающего поддержку описания модели, позволит добиться упрощения и, соответственно, повышения доступности для всех категорий руководящего состава ОВД.

Рассмотрим основные требования, предъявляемые к разрабатываемой СППР. Очевидно, что важнейшим условием функционирования системы является полнота и достоверность обрабатываемой информации. Следовательно, СППР должна легко перестраиваться в соответствии с требованиями ЛПР и обеспечивать учет изменений, происходящих в нормативной правовой базе, действующей в сфере обеспечения правопорядка в общественных местах. Таким образом, в СППР должна быть предусмотрена возможность внесения изменений в подсистему обработки первичной информации. Как видно, именно данная компонента является наиболее подверженной изменениям.

Очевидно, что неполное или недостоверное отражение в ДПУ сведений об объекте учета может привести к неверной оценке и, как следствие, принятию неэффективных управленческих решений. Автором выделено три этапа функционирования подсистемы обработки информации:

1) подготовительный этап;

2) этап сбора и обработки данных;

3) этап формирования отчетов.

Ясно, что данная процедура должна повторяться с определенной периодичностью. Данные итерации необходимы для поддержания актуальности статистической информации о состоянии преступности. Возврат на первый этап может быть вызван изменением в системе учета и регистрации (введением новых типов объектов учета, изменением словарных значений реквизитов, изменением характеристик показателей). Таким образом, речь идет об адаптации подсистемы обработки информации к изменениям в нормативной правовой базе.

Рассматривая перспективы разработки и применения СППР, можно сделать вывод о том, что она должна включать в себя и подсистему доступа к общеправовой системе правового информирования, содержащей информацию справочного характера (данные Федеральной службы государственной статистики; пояснения специальных терминов; справочные данные о нормативах и коэффициентах, действовавших в определенный период; разъяснения сотрудников ФКУ «ГИАЦ МВД России», Договорно-правового департамента МВД России и Управления правовой статистики Генеральной прокуратуры РФ).

Список литературы

1. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 // СПС «Гарант».

2. *Болтачев Э. Ф., Россихина Л. В.* Методы машинного обучения для определения эффективности использования кадровых ресурсов органами внутренних дел // Вестник Воронежского института ФСИН России. 2019. № 2. С. 54–60.

3. *Сибилькова А. В.* Искусственный интеллект на службе у следователя // Российский следователь. 2019. № 3. С. 68–70.

4. *Донченко Д. С., Садовникова Н. П., Парыгин Д. С.* Прогнозирование степени тяжести последствий ДТП с использованием методов машинного обучения // Вестник Воронежского института высоких технологий. 2019. № 4 (31). С. 176–180.

5. *Баторов Б. О., Куприянов А. И., Емельянова Е. В.* Ранговый метод количественной оценки эффективности системы управления организацией // Вестник Воронежского института ФСИН России. 2018. № 3. С. 37–43.

6. *Макаров В. Ф., Торопов Б. А.* Вопросы внедрения систем электронного документооборота в деятельность органов внутренних дел. Область применения электронных документов // Труды Академии управления МВД России. 2012. № 2 (22). С. 63–66.

И. В. ГОРОШКО,
заведующий отделом Университета прокуратуры РФ,
профессор Академии управления МВД России,
доктор технических наук, профессор

Е. Н. РЯЗАНОВА,
заместитель начальника отдела УНК ГУ МВД России
по г. Санкт-Петербургу и Ленинградской области

К вопросу противодействия наркопреступности в современном обществе

Противодействие наркотизации является важной функцией государства. Для ее реализации уполномоченными государственными органами необходимо четко представлять масштабы распространения этого опасного явления, точно оценивать современную наркоситуацию в каждом конкретном регионе.

Современную наркоситуацию в Российской Федерации можно охарактеризовать как достаточно непростую, в которой обозначились новые негативные тенденции, несущие, на наш взгляд, серьезную угрозу безопасности личности, общества, государства, подрывающие экономические, социальные и нравственные основы человеческой жизнедеятельности.

Проблема незаконного распространения наркотиков затрагивает не только Российскую Федерацию, она носит международный характер. Политическая декларация ООН, принятая резолюцией S-20/2 от 10 июня 1998 г. на двадцатой специальной сессии Генеральной Ассамблеи ООН, посвященной совместной борьбе с мировой проблемой наркотиков, гласит, что «наркотики ломают жизнь людей, разрушают общины, подрывают устойчивое развитие человека и порождают преступность. Наркотики затрагивают все сектора общества во всех странах; в частности, злоупотребление наркотиками наносит ущерб свободе и развитию молодежи – наиболее ценного мирового достояния. Наркотики представляют серьезную опасность для здоровья и благополучия всего человечества, независимости государств, демократии, стабильности наций, структуры всех обществ, а также достоинства и надежд миллионов людей и их семей»[14]. Наркоугроза признана одной из основных угроз национальной безопасности государства, в связи с чем необходимо принимать действенные меры, направленные на совершенствование законодательства, а также деятельности органов, уполномоченных на предупреждение преступлений в обозначенной сфере.

[14] URL: https://www.un.org/ru/documents/decl_conv/declarations/political_declaration.shtml (дата обращения: 01.03.2020).

Транснациональные преступные группировки продолжают вовлекать в свою деятельность все больше лиц, происходит расширение круга потребителей наркотиков за счет вовлечения в их незаконный оборот граждан из социальных групп, ранее не входивших в так называемую группу риска, возросло количество служащих, руководителей, учащихся. Изобретаются новые формы синтетических наркотических средств и психотропных веществ, синтезируются наркотики, не встречавшиеся ранее в незаконном обороте.

По мнению ряда исследователей, в настоящее время, несмотря на публичное неприятие, в Российской Федерации происходит либерализация отношения общества к наркотикам – допустимость употребления тех или иных веществ, но только при определенных условиях. Неприятие «тяжелых» наркотиков сменилось более лояльным отношением к другим, так называемым «новым» или «дизайнерским» наркотическим и психотропным веществам. Распространение стали получать так называемые «мягкие» модели потребления («статусное», «контролируемое»), не ведущие к быстрому выпадению из социума, но имеющие серьезные социальные последствия, создавая иллюзию безопасности потребления, увеличивая тем самым процент скрытой наркотизации[15].

В соответствии с Указом Президента РФ от 5 апреля 2016 г. № 156 «О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров в сфере миграции» функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров были возложены на МВД России.

26 февраля 2020 г. на расширенном заседании коллегии МВД России Президент В. В. Путин выделил противодействие незаконному обороту наркотиков как одно из важнейших направлений работы подразделений МВД России. Он обратил внимание на необходимость взаимодействия МВД России с Роскомнадзором по перекрытию доступа к сайтам и страницам в социальных сетях, пропагандирующим наркотики. Кроме того, Президент отметил, что требуется законодательная инициатива по установлению уголовной ответственности за пропаганду наркотиков в сети Интернет.

Распространение наркотиков через Интернет касается все большего количества населения Российской Федерации и может привести к масштабной национальной катастрофе.

Стоит отметить, что распространение наркотиков через «темный» Интернет – это общемировая тенденция. Так, 3 и 4 декабря 2018 г. в Вене в рамках совещания межправительственной группы экспертов

[15] *Позднякова М. Е., Брюно В. В.* Новые тенденции наркотизации как риски социального характера // Вестник Института социологии. 2018. № 24. С. 115–139.

по международной проблеме, вызванной употреблением синтетических опиоидов в немедицинских целях, признана необходимость использования новаторских специальных методов расследования, в том числе для отслеживания и пресечения незаконного изготовления и онлайн-маркетинга, торговли, распределения и связанных с ними финансовых потоков через Интернет, а также необходимость разработки оперативной информации и многостороннего обмена ею.

На МВД России было возложено принятие незамедлительных мер по изменению организационно-штатного, кадрового и материально-технического обеспечения деятельности по пресечению преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров с использованием информационно-телекоммуникационной сети Интернет[16] как места массового тиражирования информации о наркотиках, распространение которой в Российской Федерации запрещено.

Такие действия являются наиболее общественно опасными, поскольку охватывают многомиллионную аудиторию, существенной частью которой являются несовершеннолетние, способствуют созданию устойчивого спроса на наркотики, приводят к расширению рынка сбыта запрещенных веществ, делая доступной и популярной пронаркотическую субкультуру.

[16] URL: http://kremlin.ru/acts/assignments/orders/61916 (дата обращения: 01.03.2020).

И. В. ГРИГОРЬЕВА,
преподаватель кафедры ОТМ ОВД
(ВИПК МВД России)

Сведения о противодействии хищениям бюджетных средств

В настоящее время наблюдается повышенное внимание государства к вопросам противодействия преступным посягательствам на бюджетные средства, в том числе их хищениям. Ведь бюджетные средства имеют важное экономическое, политическое и социальное значение. Только благодаря их сохранению и надлежащему использованию государство имеет возможность обеспечивать провозглашенные Конституцией РФ признание, соблюдение и защиту прав и свобод граждан, создавать условия для их достойной жизни и свободного развития.

Поэтому противодействие хищениям бюджетных средств официально оформлено как необходимость обеспечения государственной и общественной безопасности. Так, в Стратегии национальной безопасности Российской Федерации 2015 г. [2] одним из приоритетных направлений признано развитие системы выявления, предупреждения и пресечения преступных посягательств на государственную собственность, в число объектов которой входят и бюджетные средства.

В Стратегии экономической безопасности Российской Федерации 2017 г. [3] одной из основных задач обеспечения такой безопасности России провозглашена борьба с нецелевым использованием и хищением государственных бюджетных средств.

Однако государству ежегодно причиняется ущерб от хищений бюджетных средств. Так, согласно статистическим данным по оконченным в 2013–2018 гг. уголовным делам, связанным с хищениями бюджетных средств, государству и муниципальным образованиям причинен средний ущерб на сумму около 7 млрд рублей в год, что составляет 60 % от общего объема материального ущерба, причиненного хищениями государственного и муниципального имущества. Кроме того, именно хищения среди всех преступных посягательств на бюджетные средства составили основную часть (82 %) [7].

В настоящее время возможно составить некоторую картину преступности в рассматриваемой сфере, но не в полном объеме, так как предоставление всех основных сведений о таких преступлениях в соответствующих формах отчетности не предусмотрено.

Во-первых, в Сводном отчете по России о преступности в сфере экономики [4] представлены общие сведения относительно преступных посягательств, таких как кража, мошенничество, мошенничество при получении выплат, присвоение или растрата: о количестве выявленных преступлений; о количестве преступлений, уголовные дела по которым

находились в производстве в отчетном периоде (окончены расследованием, разрешены, направлены в суд), которые совершены группой, преступным сообществом (организацией); о размере причиненного материального ущерба, добровольно погашенного материального ущерба, изъятого имущества, о стоимости имущества, на которое наложен арест, по оконченным уголовным делам и материалам об отказе в возбуждении уголовного дела, о размере причиненного материального ущерба по преступлениям, уголовные дела по которым приостановлены. Данные сведения позволяют определить общую картину хищений чужого имущества. Эти сведения представлены в том числе в отношении государственной и муниципальной собственности. Однако сведения не дифференцированы по предмету хищений, не позволяют установить показатели, касающиеся преступных посягательств на бюджетные средства. В то же время в данном отчете предоставляются сведения по хищениям предметов, имеющих особую ценность, незаконным получениям кредита, злоупотреблениям полномочиями, благодаря которым возможно провести сравнительное исследование результатов противодействия данным преступлениям.

Во-вторых, в Сводном отчете по России о результатах работы по выявлению и раскрытию преступлений экономической направленности представлены сведения о преступлениях, связанных с освоением бюджетных средств [7], дифференцированные по 85 субъектам РФ и транспорту России: о количестве выявленных преступлений, в том числе связанных с реализацией приоритетных национальных проектов, о количестве предварительно расследованных преступлений, в том числе направленных в суд; о размере причиненного материального ущерба, наложенном аресте на имущество по оконченным уголовным делам (из числа находящихся в производстве); о количестве выявленных лиц, совершивших преступление. Однако этих сведений недостаточно:

– они предоставлены по преступлениям против собственности (глава 21 УК РФ) в общем, т. е. показатели касаются и преступлений, не являющихся хищениями;

– сведения предоставлены по чч. 2–4 ст. 159, 159.2, 159.4, 160 УК РФ, однако анализ приговоров по хищениям бюджетных средств показал, что такие деяния также квалифицируются и по ч. 1 ст. 159 УК РФ.

В качестве положительной стороны можно отметить наличие в данном отчете сведений, позволяющих провести сравнительный анализ преступных посягательств на бюджетные средства и подтверждающих наличие или отсутствие в отчетном периоде совершенных преступлений, связанных с бюджетными средствами, предусмотренных разными главами УК РФ:

– в сфере экономической деятельности (глава 22), в том числе незаконные получения кредита (ч. 2 ст. 176), уклонение от уплаты налогов и (или) сборов с организации (ст. 199);

– против интересов службы в коммерческих и иных организациях (глава 23), в том числе коммерческий подкуп (ст. 204);

– против государственной власти, интересов государственной службы и службы в органах местного самоуправления (глава 30), в том числе злоупотребление должностными полномочиями (ст. 285), нецелевое расходование бюджетных средств (ст. 285.1), превышение должностных полномочий (ст. 286), получение взятки (ст. 290), дача взятки (ст. 291), посредничество во взяточничестве (ст. 291.1), служебный подлог (ст. 292), халатность (ст. 293).

В-третьих, в подобном предыдущему Сводном отчете по России [7] о результатах работы по выявлению и раскрытию преступлений экономической направленности представлены сведения о преступлениях, связанных с освоением бюджетных средств, с дифференциацией их по статьям УК РФ (против собственности (глава 21) в общем, чч. 2–4 ст. 159, 159.2, 159.4, 160 УК РФ): о количестве выявленных преступлений; количестве предварительно расследованных преступлений, в том числе направленных в суд; о размере причиненного материального ущерба по оконченным уголовным делам (из числа находящихся в производстве), о наложенном аресте на имущество; о количестве выявленных лиц, совершивших преступление, в том числе дела по которым направлены в суд. Однако в данном отчете, как и в предыдущем, сведений недостаточно, так как они предоставлены по преступлениям против собственности в общем, в том числе и не являющимся хищениями, а также нет сведений по ч. 1 ст. 159 УК РФ.

В качестве положительной стороны можно отметить наличие в данном отчете сведений, позволяющих провести сравнительный анализ преступных посягательств на бюджетные средства и подтверждающих наличие или отсутствие в отчетном периоде совершенных преступлений, связанных с бюджетными средствами, предусмотренных разными главами УК РФ, как и в предыдущем отчете.

В-четвертых, в Сборнике по Российской Федерации [6] представлены сведения о мероприятиях по защите средств федерального бюджета, направленных на реализацию приоритетных национальных проектов «Здоровье», «Образование», «АПК», «Жилье». Данные сведения содержат показатели по 85 субъектам РФ о количестве вынесенных постановлений об отказе в возбуждении уголовного дела по пп. 1, 2 ч. 1 ст. 24 УПК РФ в результате таких мероприятий. Однако этих сведений недостаточно для полноты картины, необходимы сведения о количестве вынесенных постановлений об отказе в возбуждении уголовного дела по всем преступным посягательствам на средства федерального бюджета, бюджетов субъектов РФ, местных бюджетов, в том числе и по хищениям таких средств, и не только относительно указанных проектов, но и разных направлений освоения бюджетных средств.

В-пятых, в Сводном отчете по России о работе ОВД по раскрытию преступлений [5] представлены сведения о хищениях, связанных с финансовой деятельностью, страхованием и деятельностью общественных объединений; сведения о хищениях культурных ценностей, лицах, их совершивших, а также

об установленном и возмещенном материальном ущербе; сведения о преступлениях, связанных с пожарами. Однако очевидно, что как особый вид преступлений хищения бюджетных средств также можно отнести к хищениям, связанным с финансовой деятельностью, но такие сведения в данном отчете отсутствуют.

Однако вышеперечисленные сведения позволяют отобразить только отдельные фрагменты картины преступности по хищениям бюджетных средств. И в настоящее время не осуществляется сбор сведений именно по хищениям бюджетных средств как по особому виду преступлений, что значительно облегчило бы проведение анализа состояния преступности данного вида.

Считаем, что для сбора таких сведений необходимо включить дополнительные реквизиты в соответствующие формы отчетности, установленные приказом Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29 декабря 2005 г. «О едином учете преступлений» [1].

Так, в соответствии с п. 17 раздела III данного приказа в статистической карточке на выявленное преступление заполнением реквизита «27» отображаются сведения (по Справочнику № 15 «Дополнительная характеристика преступления») о том, что преступление связано:

– с деятельностью по реализации приоритетных национальных проектов (код 094, 109, 110, 111, 112), т. е. совершенное преступление связано с освоением денежных средств, выделяемых из бюджета РФ и бюджетов субъектов РФ на реализацию приоритетных национальных проектов;

– с жилищно-коммунальным хозяйством (код 131), т. е. преступление, предусмотренное ст. 159, 159.4, 160, 165, 171, 172, 174, 174.1, 195, 196, 197, 201, 204, 215.1, 215.2, 216, 238, 285, 285.1, 285.2, 286, 289, 290, 291, 291.1, 292, 293, 330 УК РФ, связано с нарушениями законодательства при распределении и расходовании денежных средств, предоставляемых из бюджетов различных уровней и государственных внебюджетных фондов на нужды ЖКК (на строительство, ремонт и модернизацию систем коммунальной инфраструктуры; на переселение граждан из ветхого и аварийного жилья; на проведение ремонтных работ или иного обслуживания жилых помещений и объектов, предназначенных для постоянного проживания граждан);

– с освоением бюджетных средств (код 130);

– с хищением бюджетных средств (код 151).

Считаем, что необходимо привести в соответствие Справочник № 3 «Предмет преступного посягательства», по которому вносятся сведения в реквизит «23», и включить в перечень данного Справочника как предмет преступного посягательства средства федерального бюджета, бюджета субъекта РФ, местного бюджета.

В Статистической карточке об установленной сумме материального ущерба, результатах его возмещения и изъятия предметов преступной деятельности заполнением реквизита «11» отображаются сведения о сумме

материального ущерба, погашенного в бюджеты: федеральный (код 1), субъекта РФ (код 2), местный (код 3).

Для отображения сведений о потерпевшем от хищения бюджетных средств – государстве, субъекте РФ или муниципальном образовании – в Статистической карточке о потерпевшем необходимо их включить в реквизит «11» («Материальный ущерб причинен»).

В результате проведенного исследования выявлено, что из всех изученных приговоров о хищениях бюджетных средств значительную часть составляли дела, по которым потерпевшие и виновные знакомы, так как являются работниками одного учреждения или ведомства. И по таким делам подача гражданского иска о возмещении имущественного ущерба реже, чем по иным приговорам. Поэтому считаем, что в реквизит «10» («Характеристика потерпевшего») необходимо включать сведения о том, что представитель потерпевшего и виновный – работники одного учреждения или ведомства.

Таким образом, для сбора сведений в наиболее полном объеме о состоянии преступности по хищениям бюджетных средств с целью комплексного противодействия таким преступлениям необходимо включить внесение дополнительных сведений о признаках составов хищений бюджетных средств в статистическую отчетность и сводные ведомственные отчеты: о предмете преступного посягательства, о потерпевшем, о количестве приостановленных и прекращенных уголовных дел по таким преступлениям, о количестве вынесенных постановлений об отказе в возбуждении уголовного дела по всем преступным посягательствам на средства федерального бюджета, бюджетов субъектов РФ, местных бюджетов.

Список литературы

1. О едином учете преступлений: приказ Генпрокуратуры РФ, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития и торговли России и ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 // Рос. газ. 2006. № 0 (3979).
2. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 декабря 2015 г. № 683 // Собр. законодательства Рос. Федерации. 2016. № 1 (ч. 2). Ст. 212.
3. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: Указ Президента РФ от 13 мая 2017 г. № 208 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2902.
4. Форма 010: «Сводный отчет по России о преступности в сфере экономики» за 2018 г. // ЦСИ ФКУ «ГИАЦ МВД России».
5. Форма 041: «Сводный отчет по России о работе органов внутренних дел по раскрытию преступлений» за 2017 г. // ЦСИ ФКУ «ГИАЦ МВД России».
6. Форма 465: «Сборник по Российской Федерации о мероприятиях по защите средств федерального бюджета, направленных на реализацию приоритетных

национальных проектов «Здоровье», «Образование», «АПК», «Жилье» за 2015 г. // ЦСИ ФКУ «ГИАЦ МВД России».
7. Форма 050: «Сводный отчет по России о результатах работы по выявлению и раскрытию преступлений экономической направленности» за 2013–2018 гг. // ЦСИ ФКУ «ГИАЦ МВД России».

Д. Г. ДОБРЕНЬКИЙ,
слушатель факультета подготовки руководителей территориальных органов МВД России (Академия управления МВД России)

Проблемные вопросы внедрения сервиса обеспечения деятельности дежурных частей (СОДЧ) ИСОД МВД России

Дежурная часть является одним из подразделений ОВД, которое непосредственно связано с процессом управления. Важнейшая особенность процесса управления заключается в его информационной природе. Можно сказать, что управление начинается и заканчивается работой с информацией. Сотрудники различных сфер управления до 70 % рабочего времени затрачивают на поиск, сбор, обработку, передачу сведений [1]. Применение информационных технологий позволяет автоматизировать процесс обработки информации.

В настоящее время, в связи с развитием науки и техники, в управленческой деятельности активно применяются различные автоматизированные информационные системы. В МВД России создана единая система информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России. На базе ИСОД МВД России разработан и введен в эксплуатацию сервис обеспечения деятельности дежурных частей (далее – СОДЧ).

СОДЧ ИСОД МВД России предназначен для автоматизации процессов приема и регистрации информации, поступающей в дежурные части территориальных органов МВД России, обеспечения надлежащего качества ее сбора, обработки и хранения [2]. Применение данного сервиса особо актуально в условиях оптимизации штатной численности личного состава ОВД, в том числе сотрудников дежурных частей МВД России.

Основными подсистемами (модулями), автоматизирующими деятельность дежурных частей территориальных органов (отделов, отделений, пунктов полиции) МВД России, являются: «управление силами и средствами», «оперативный дежурный», «оперативные ориентировки», «диспетчеризация «02», «доставления», «сводка». Для контроля за работой подчиненных подразделений и повышения эффективности управленческой деятельности по всем модулям предусмотрено формирование различных отчетов. Обеспечивается взаимодействие компонентов между собой и с другими сервисами ИСОД МВД России.

Каждая подсистема выполняет определенные функции.

Подсистема «диспетчеризация «02» предназначена для приема и обработки информации, принимаемой по телефону службой «02», формирования карточек происшествий и направления их для организации реагирования в территориальные подразделения. Кроме того, по адресу

происшествия автоматически определяется территориальный орган МВД России, в который следует отправить информацию, при необходимости имеется возможность скорректировать список оповещаемых подразделений. Подсистема также позволяет отслеживать информацию о дате и времени выполнения каждой стадии отработки сообщения о происшествии в территориальном органе МВД России, просмотреть информацию о звонках абонента, если он уже обращался в службу «02» в течение последних 24 часов.

Разработчиками сервиса СОДЧ также предусмотрена возможность организации сетевой связанности между Системой-112 и СОДЧ в соответствии с протоколом обеспечения информационной безопасности. Это позволяет организовать взаимодействие между системами с целью передачи карточки происшествия из Системы-112 в СОДЧ и возврата статуса карточки происшествия из СОДЧ в Систему-112. В ряде случаев данная система показала свою эффективность, однако имеют место факты необоснованного направления некриминальной информации в ОВД, которая не относится к их компетенции. Например, доля таких сообщений, поступающих в дежурные части территориальных органов МВД России по Республике Татарстан из «Службы-112», составляет около 8 % (*мужчина упал – потерял сознание, днем шумят соседи – делают ремонт, идет дым из мусорного бака, бегает стая собак, протекает крыша, гололед на дороге, не работает светофор, отсутствует разметка дорог, подозрительные люди, застряли в лифте и т. п.*) [3]. Вместе с тем для обработки такого рода информации также задействуются силы и средства. Причиной этого является отсутствие единого нормативно-правового акта, который бы регулировал порядок действий всех министерств и ведомств при получении сообщений о происшествиях и реагирования на них.

Кроме того, подсистема «диспетчеризация «02» имела бы гораздо большую эффективность, если бы имелась возможность автоматизации процесса приема информации о происшествии. Например, по номеру телефона звонящего автоматически определялся бы адрес абонента, при поступлении звонка с мобильного телефона определялось бы местоположение абонента. Данный процесс дает нам возможность сократить время для заполнения карточки происшествия, а также дает возможность системе определить ближайшие наряды для оперативного реагирования на происшествие. Подсистема также должна иметь доступ к электронным картам местности и справочным информационным системам.

Подсистема «оперативный дежурный» предназначена для приема и регистрации сообщений о преступлениях, административных правонарушениях и происшествиях (электронный КУСП), а также внесения необходимой информации по рассмотрению материала и решения по нему. С положительной стороны необходимо отметить возможность составления различных отчетов, которые формирует оперативный дежурный в оперативно-служебной деятельности. Доступны для формирования

следующие отчеты: «просрочен срок принятия решения по записи КУСП (от 3 суток до 10 суток)»; «просрочен срок принятия решения по записи КУСП (от 10 суток до 30 суток)»; «просрочен срок принятия решения по записи КУСП (свыше 30 суток)»; «выгрузка записей КУСП за период (выгрузка для предоставления данных в прокуратуру)»; рапорт оперативного дежурного о результатах дежурства; форма № 2-Е «Сведения о рассмотрении сообщений о преступлении»; форма № 4-Е «Отчет о результатах работы ОВД по обеспечению учетно-регистрационной дисциплины»; сверка уголовной статистики; акт сверки достоверности регистрации КУСП.

Работа по ведению подсистемы «оперативный дежурный» самая рутинная и трудоемкая по сравнению с другими модулями, так как связана с процессом обработки большого массива информации. Конечно, применение процессов автоматизации при введении в электронную базу сведений о происшествиях существенно облегчит работу сотрудникам дежурных частей. Большую часть времени оперативный дежурный тратит на введение установочных данных заявителей, потерпевших, свидетелей (фамилия, имя, отчество, адреса проживания и т. д.). Причем все эти данные имеются в информационных базах МВД России. Возможность автоматического переноса этих данных в электронный КУСП намного сократит время обработки данных, а также исключит возможность внесения ошибочных или вымышленных данных. Кроме того, несмотря на большой объем работы по внесению сведений в электронный КУСП, процесс усложняется еще и дублированием всей информации в Книгу учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП).

Подсистема «управление силами и средствами» предназначена для формирования основной дислокации сил и средств территориального органа МВД России, управления нарядами при отработке сообщений о происшествии, визуализации оперативной обстановки на территории обслуживания.

Подсистема «доставления» предназначена для автоматизации работы оперативного дежурного с лицами, доставленными в дежурные части территориальных органов МВД России. Протоколы, формируемые в автоматическом режиме, – о доставлении, об административном задержании, об административном правонарушении.

Подсистема «сводка» предназначена для формирования оперативной сводки на всех уровнях структурной организации территориальных органов МВД России, передачи информации, необходимой для создания оперативной сводки, на вышестоящий уровень. Реализована возможность по автоматизированному формированию в СОДЧ оперативной сводки в соответствии с методическими рекомендациями о порядке формирования оперативной сводки территориального органа. Кроме того, модуль «сводка» позволяет авторизованным пользователям просматривать сформированную оперативную сводку территориального органа МВД России за любую дату

без возможности редактирования данных, что отменяет необходимость тиражирования информации на бумажных носителях. В вышестоящем территориальном органе МВД России существует возможность просматривать загруженные сводки подчиненных подразделений.

Подсистема «аналитика» предназначена для формирования статистических отчетов по различным критериям. Кроме того, в целях осуществления действенного контроля за эксплуатацией СОДЧ в дежурных частях территориальных органов МВД России на различных уровнях структурной организации реализована возможность формирования статистических отчетов по внесению данных в сервис (количество внесенной информации по модулям «оперативный дежурный», «сводка», «доставления», «оперативные ориентировки»).

Подсистема «оперативные ориентировки» предназначена для доведения оперативных ориентировок до дежурных частей и мобильных нарядов. Обеспечивает автоматизацию деятельности сотрудников мобильных сил (пеших нарядов, патрулей и экипажей, следственно-оперативных групп и т. д.) и оперативных дежурных в части проведения оперативных мероприятий по рассылаемым ориентировкам при организации сотрудниками дежурных частей неотложных разыскных действий. Здесь необходимо учитывать, что данная подсистема будет действовать только в том случае, если наряды будут оснащены соответствующими мобильными автоматизированными рабочими местами.

До введения в эксплуатацию сервиса СОДЧ ИСОД МВД России в деятельности дежурных частей территориальных органов МВД России использовались различные автоматизированные информационные системы. Данные системы продолжают эксплуатироваться, потому что полностью отказаться от них территориальные органы не готовы. Остается нерешенным вопрос взаимодействия этих систем с сервисом СОДЧ ИСОД МВД России. Это приводит к дублированию ввода и обработки информации. То есть поступающая информация (о происшествиях, о преступлениях, об оперативной обстановке) вносится как в сервис СОДЧ, так и в существующие системы. Это приводит к задействованию дополнительных трудовых ресурсов и временных затрат. Существенно увеличивается нагрузка на сотрудников дежурных частей по обработке информации. Пути решения данной проблемы видятся в расширении функциональных возможностей сервиса СОДЧ ИСОД МВД России в части информационного и технологического взаимодействия с уже существующими автоматизированными информационными системами дежурных частей МВД России.

Список литературы

1. *Кононов А. М., Захватов И. Ю.* Организация управления органами внутренних дел: учебник. М., 2017.

2. *Сухов С. Н., Смирнов С. А., Макаров А. В.* Сервисы единой системы информационно-аналитического обеспечения деятельности МВД России: учеб.-практ. пособие. Н. Новгород, 2017.
3. *Худяков В. В.* Использование информационных систем в дежурных частях Республики Татарстан: проблемы и пути их решения // Материалы всероссийского круглого стола (27 мая 2016 г.). Казань, 2016.

Р. Е. ЖИХОРЕВА,
старший преподаватель кафедры административного права и административной деятельности полиции, кандидат юридических наук
(Московский областной филиал Московского университета МВД России имени В. Я. Кикотя)

Особенности внедрения технологий искусственного интеллекта в сферу обеспечения безопасности дорожного движения

Период с 2011 по 2020 гг. Генеральной Ассамблеей ООН объявлен как Десятилетие действий по обеспечению безопасности дорожного движения. Это историческое решение стало основой для изменения катастрофической тенденции постоянного увеличения уровня аварийности на мировых дорогах, а также количества прерванных человеческих жизней в результате ДТП.

В сентябре 2019 г. в рамках официального визита состоялась встреча Министра внутренних дел РФ генерала полиции В. А. Колокольцева и Министра по делам инфраструктуры Королевства Швеция Тумаса Энерута.

В. Колокольцев подчеркнул, что достижения технического прогресса открывают широкие возможности как для решения отдельных транспортных задач, так и для комплексного формирования целостной системы безопасности общества и государства. В настоящее время в России эффективно применяется аппаратно-программный комплекс «Безопасный город», который является одним из важных элементов обеспечения общественного порядка и антитеррористической защищенности мест массового скопления людей.

Министр также подчеркнул, что Третья конференция под названием «Достижение глобальных целей к 2030 году», которая запланирована на 2020 г. в Стокгольме, станет не только платформой для подведения итогов Десятилетия действий по безопасности дорожного движения, но и стимулом для дальнейшего совершенствования деятельности в данном направлении.

Примечательно, что Международной ассоциацией руководителей полиции были сформулированы тенденции в области движения автомототранспортных средств в XXI в.:

– увеличение количества заторов и, как следствие, загруженности автомобильных магистралей;

– повсеместное появление «интеллектуальных» ТС и автомобильных дорог;

– снижение скорости движения (оборудование транспортных средств и стационарных постов такими электронными устройствами, которые

способны контролировать системы зажигания, в связи с чем водитель будет вынужден соблюдать установленную скорость движения);

– повышение уровня агрессивности на дороге;

– увеличение количества ДТП по вине водителей пожилого возраста, массовая доля которых в структуре населения с каждым годом имеет тенденцию к росту;

– повсеместное применение устройств автоматического выявления и фиксации нарушений ПДД;

– внедрение и использование новейших инновационных технических средств при работе на месте происшествия;

– значительное сокращение времени проверки водителя и ТС;

– сохранение приоритетной роли дорожной полиции в борьбе с преступностью [5].

Обозначенные тенденции должны найти свое отражение в соответствующих нормативных источниках национального законодательства, в том числе регламентирующих правила дорожного движения, а также ответственность за их нарушение.

На расширенном заседании коллегии МВД России 28 февраля 2019 г. Министр Колокольцев подчеркнул, что одним из приоритетных направлений деятельности ОВД остается повышение безопасности дорожного движения. Несмотря на некоторые улучшения показателей, ситуация в целом на дорогах по-прежнему остается сложной. Ежедневно в ДТП погибают около 50 и получают ранения свыше 600 человек. Это очень серьезные данные [4].

В этой связи Министром были обозначены основные направления совершенствования безопасности дорожного движения, а именно: последовательное развитие технических средств контроля за соблюдением правил дорожного движения, расширение возможностей систем автоматической фото- и видеофиксации правонарушений, а также предъявление повышенных требований к сдаче правил дорожного движения и выдаче водительских прав.

Также в Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года одной из перечисленных целей государственной политики в сфере развития транспорта является создание необходимых условий для повышения уровня конкурентоспособности экономики и качества жизни населения, включая повышение комплексной безопасности и устойчивости транспортной системы.

Федеральная целевая программа «Повышение безопасности дорожного движения в 2013–2020 годах» предусматривает следующую цель создания данного документа – сокращение смертности в результате дорожно-транспортных происшествий к 2020 г. на 8 тыс. человек (примерно 28 %) по сравнению с 2012 г.

Программа предусматривает ряд мероприятий, направленных на улучшение ситуации в сфере безопасности дорожного движения, а именно:

– развитие системы, направленной на предупреждение и профилактику опасного поведения участников дорожного движения;

– обеспечение безопасного участия детей в дорожном движении;

– повышение уровня состояния технической эксплуатации транспортных средств;

– повышение уровня безопасности дорожных условий;

– развитие системы оказания своевременной помощи пострадавшим в ДТП;

– совершенствование правового регулирования в сфере безопасности дорожного движения [2].

Что касается Стратегии безопасности дорожного движения в Российской Федерации на 2018–2024 годы [3], то она ставит задачу определить базу для эффективной организации работы всей системы органов власти по повышению безопасности дорожного движения. При ее разработке учитывались основные положения стратегических документов в области национальной, экономической, государственной политики, транспортной безопасности, внешней и миграционной политики, а также социально-экономического развития.

С 2021 по 2024 гг. в рамках реализации указанной Стратегии планируется реализация комплекса мероприятий, которые непосредственно будут влиять на индикаторы дорожного движения. К 2030 г. Стратегия закрепляет «стремление к нулевой смертности».

Одной из основных причин ДТП является именно человеческий фактор, из чего можно сделать вывод, что актуальным и перспективным направлением является поиск идей и технологий, способных снизить риск ошибок и халатности непосредственно участников дорожного движения. Таким направлением в настоящее время должно быть применение в транспортной инфраструктуре элементов интеллектуальных транспортных систем, в частности внедрение технологий искусственного интеллекта.

Развитие данного направления связано с современной государственной политикой в этой сфере, а именно с подписанием Указа Президента РФ № 490 от 10 октября 2019 г. «О развитии искусственного интеллекта в Российской Федерации», утверждающего Национальную стратегию развития искусственного интеллекта на период до 2030 г.

Технологии искусственного интеллекта (далее – ИИ) уже сегодня довольно широко применяются в различных видах транспорта, включая беспилотные летательные аппараты, а также многочисленные системы помощи пилоту или системы навигации, которыми оборудованы современные морские суда. Тем не менее в автомобильном транспорте подобные системы пока не находят массового применения, в первую очередь потому, что стоимость такого ТС и масштабы используемой

для перемещения территории не позволяют применять довольно дорогостоящие средства автоматизации. Однако приятно видеть, что лидирующие позиции в мире в этом направлении занимают отечественные разработчики.

Примером может служить российская компания Cognitive Technologies, которая в 2018 г. представила на ведущих мировых форумах решения для управления автономными транспортными средствами, способными работать в любых погодных условиях и на любых дорогах (даже при отсутствии разметки и при наличии повреждений дорожного полотна), гарантируя безопасность участников движения. Примечательно, что обозначенные технологии возглавили множество технологических рейтингов отечественных и зарубежных СМИ.

Компанией был представлен антропоморфный подход в качестве базового элемента в системе компьютерного зрения: разработчиками были построены определенные системы ИИ по тем же принципам, как это устроено у человека. Благодаря этому ИИ беспилотника, например, заметив пешехода, движущегося в сторону проезжей части и скрывшегося перед выходом на дорогу за деревом или другим препятствием, «вспомнит» о возможной опасности и даст команду либо притормозить, либо перестроиться в соседний ряд.

Российская разработка оказалась довольно востребованной. Эксперты в этой области уверены, что более чем на 70 % территории планеты Земля имеется реальная необходимость в подобных системах управления автопилотом, которые были бы предназначены именно не для идеальных дорог. В итоге отечественная компания подписала более 30 соглашений с ведущими мировыми автопроизводителями таких государств, как США, Китай, Япония, а также ряда стран Европы.

Хотелось бы отметить снижение травматизма и аварийности на дорогах Австралии вследствие использования камер с ИИ, которые способны фиксировать нарушения водителей, пользующихся во время вождения смартфонами. Думается, использование таких камер в России способно повлиять на правосознание водителей и намного снизить количество ДТП.

ИИ обладает высоким потенциалом снижения уровня риска ДТП, он призван сократить нагрузку на водителя, помочь ему следить за дорогой, планировать маршрут, соблюдать скоростные режимы и знаки, а также в целом создать более комфортные и безопасные условия вождения. Находят свое применение и так называемые «умные светофоры», способные самостоятельно переключаться в зависимости от плотности дорожного движения. Передача части управления транспортным средством системам, основанным на ИИ, позволит снизить влияние человеческого фактора, предупредив возможные ошибки. ИИ базируется на программах, для реализации которых требуются особые электронные устройства и технологии, внедренные в систему транспортного средства, которые, как и любая техника, могут выйти из строя или претерпеть сбой. Безусловно,

нельзя говорить о том, что технологии ИИ способны полностью решать проблемы транспортной безопасности. Именно совместная работа интеллекта искусственного и интеллекта живого человека способна максимально снизить вероятность ДТП, а значит, спасти множество человеческих жизней.

Таким образом, в настоящее время необходима реализация новейших возможностей для повышения безопасности дорожного движения, в том числе с помощью международного сотрудничества.

Хотя в обозримом будущем невозможно ликвидировать все несчастные случаи, имеются убедительные доказательства того, что в результате комплексного подхода к решению данной проблемы число и доля смертельных случаев и серьезных травм могут быть значительно сокращены за короткий период за счет сосредоточения внимания на ключевых факторах риска и применения принципов и мер безопасности, которые подтвердили свою точность и эффективность как в Российской Федерации, так и в других странах.

Список литературы

1. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 // СПС «Гарант».
2. О федеральной целевой программе «Повышение безопасности дорожного движения в 2013–2020 годах»: постановление Правительства РФ от 3 октября 2013 г. № 864 // СПС «Гарант».
3. Об утверждении Стратегии безопасности дорожного движения в Российской Федерации на 2018–2024 годы»: распоряжение Правительства РФ от 8 января 2018 г. № 1-р // СПС «Гарант».
4. Выступление Министра внутренних дел РФ В. А. Колокольцева на расширенном заседании коллегии МВД России 28 февраля 2019 г. URL: https://xn--b1aew.xn--p1ai/Fotoarhiv/Meroprijatija_s_uchastiem_rukovodstva (дата обращения: 14.11.2019).
5. *Молчанов П. В.* Особенности государственного регулирования обеспечения безопасности дорожного движения за рубежом: ключевые направления, критерии и ответственность // Вестник Университета имени О. Е. Кутафина. 2018. № 1. С. 121–124.
6. Рос. газ. 2019. № 7959.
7. *Кравцов Д. А.* Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. № 3. С. 108–110.
8. *Суходолов А. П., Бычкова А. М.* Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. Т. 12. С. 753–766.

9. *Бахтеев Д. В.* Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 43–49.
10. *Солнцева О. Г.* Аспекты применения технологий искусственного интеллекта // Технологии искусственного интеллекта в менеджменте. 2018. № 1. Т. 1. С. 43–51.

А. Ю. ЗВОНАРЕВА,
начальник кафедры
организации деятельности органов внутренних дел
центра командно-штабных учений,
кандидат социологических наук
(Академия управления МВД России)

К вопросу использования электронного документооборота в деятельности ОВД России

Применение современных информационных технологий в деятельности ОВД России имеет важное значение не только для удобства в работе за счет технической автоматизации отдельных процессов, но и для формирования положительного имиджа.

Так, в марте 2012 г. Министерством внутренних дел РФ была утверждена концепция создания единой системы информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России 2012–2014 гг. Хотя согласно некоторым источникам проведение комплекса мероприятий, предусматривающих внедрение унифицированных прикладных решений по основным направлениям оперативно-служебной деятельности, организацию по каждому из направлений соответствующих централизованных баз данных, создание единой инфраструктуры дата-центров для размещения этих баз данных и прикладных приложений по принципам «ведомственного облака», реализацию единой технологии регламентированного доступа к ним, начато уже с декабря 2011 г. [5, 1].

Создание ИСОД МВД России стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, который велся с 2005 г. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и госорганами различных уровней.

В настоящее время ИСОД МВД России является единым источником информации для всего личного состава системы МВД России, обеспечивает электронное взаимодействие, а также способствует повышению эффективности принимаемых управленческих решений за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных данных, оперативном и своевременном анализе ключевых показателей деятельности МВД России.

Следует отметить, что организация работы с документами существенно влияет на оперативность и качество управления.

Очевидно, что в век информационных технологий только использование электронного документооборота позволит справиться с существующими объемами документопотоков.

В настоящее время при осуществлении делопроизводства информационные технологии применяются в ОВД по четырем направлениям:

– для создания документов;

– для передачи информации (документов в электронном виде) адресатам в рамках электронного документооборота;

– для регистрации (учета) и контроля за сроками исполнения документов;

– для создания архивного электронного фонда, сохранения информации и быстрого ее поиска.

Сервис электронного документооборота (далее – СЭД) ИСОД МВД России предназначен для повседневного использования личным составом ОВД России.

Следует отметить, что указанный сервис используется не только для организации документооборота, т. е. охватывает не только процесс движения документа с момента поступления в организацию или создания и до отправки или исполнения и помещения документа в дело, но и для осуществления иных делопроизводственных операций, включая регистрацию документов, контроль за исполнением, информационно-справочную работу, оперативное и архивное хранение информации. Поэтому, на наш взгляд, корректнее было бы употребление применительно к сервису названия «Сервис электронного делопроизводства» ИСОД МВД России.

Система электронного документооборота разработана и установлена в региональных центрах обработки данных, расположенных в защищенном контуре МВД России.

Внедрение осуществлялось поэтапно в 2016 г. в соответствии с распоряжением МВД России № 1/9112 от 9 ноября 2015 г. «О мерах по переходу на электронный документооборот» [4].

На первом этапе подразделения системы МВД России, подключенные к СЭД, перешли на регистрацию входящих, подготовленных (исходящих) документов, нормативных правовых, ведомственных актов и их пересылку в другие подразделения системы МВД России с использованием СЭД. Данный этап предусматривал изменение алгоритма деятельности подразделений делопроизводства и режима системы МВД России при организации документооборота.

На втором этапе должностные лица, осуществляющие руководящие функции, обеспечивали рассмотрение несекретных входящих документов, нормативных правовых и ведомственных актов с использованием средств СЭД.

На третьем этапе весь личный состав МВД России являлся задействованным при внедрении сервиса, так как разработку, согласование, подписание (утверждение) и рассылку несекретных подготовленных (исходящих) документов требовалось осуществлять в электронном виде с использованием электронных подписей.

В исключительных случаях для направления документа в подразделения МВД России, не подключенные к СЭД, а также в иные ведомства и организации (при отсутствии межведомственного электронного документооборота) требовалось распечатывать бумажный экземпляр с отметкой о том, что документ подписан электронной подписью соответствующего руководителя.

Следует отметить, что обработка информации с использованием сервиса имеет ограничения. Так, запрещается внесение в учетные формы СЭД сведений, составляющих государственную тайну, а также сканирование документов, имеющих грифы секретности или пометку «для служебного пользования».

Перечень документов, образующихся в деятельности ОВД, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов, утвержден приказом МВД России от 31 мая 2011 г. № 600 [1].

Общий порядок работы с электронными документами регламентирован Инструкцией по делопроизводству в ОВД, которая утверждена приказом МВД России от 20 июня 2012 г. № 615 [2].

Для отдельных видов документов, подготовленных в электронном виде, требования определены соответствующими приказами. Так, в Правилах подготовки правовых актов в территориальных органах, утвержденных приказом МВД России от 26 декабря 2018 г. № 880, указывается, что на бумажных носителях создаются следующие проекты правовых актов [3]:

– содержащие сведения, составляющие государственную тайну;

– содержащие служебную информацию ограниченного распространения;

– издаваемые совместно или по согласованию с другими государственными органами и организациями (при отсутствии технических возможностей для обмена электронными документами через систему межведомственного электронного документооборота);

– не включенные в Перечень документов, образующихся в деятельности ОВД, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов.

Таким образом, в настоящее время порядок использования электронного документооборота, а точнее электронного делопроизводства, в деятельности ОВД России регламентирован в достаточной степени. С 2011 г. наблюдается единый подход к его организации и целенаправленное внедрение в деятельность ОВД, что позволяет говорить о перспективах его использования и развития.

Отметим, что использование СЭД способствует оптимизации документооборота при подготовке, принятии и реализации управленческих решений в системе МВД России. Вместе с тем системный анализ проблем внедрения СЭД не позволяет значительно сократить документопотоки. Например, в деятельности ОВД значительный объем несекретного

документооборота образуется при организации специального делопроизводства, которое не адаптировано к электронному документообороту и не учитывается при анализе его динамики.

Кроме того, до настоящего времени не определен порядок перехода на межведомственный электронный документооборот.

Хотя функционал сервиса постоянно дорабатывается (например, в период с 2016 г. по ноябрь 2019 г. подготовлено уже 70 релизов по нововведениям и исправлениям ошибок по работе сервиса), до сих пор не решена проблема автоматизированного формирования отчетных сведений по заданному пользователем шаблону, автоматизированного поиска и анализа контента, прогнозирования и моделирования оптимальных документопотоков, распознавания сведений в отношении конкретного лица, внесенных в различные прикладные сервисы ИСОД МВД России, и их связи между собой.

Кроме того, на наш взгляд, важным направлением совершенствования СЭД могла бы стать автоматизированная разработка моделей типовых информационно-справочных документов посредством извлечения данных из различных источников, находящихся в электронном архиве.

Список литературы

1. Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов: приказ МВД России от 31 мая 2011 г. № 600 // СПС «КонсультантПлюс».

2. Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации: приказ МВД России от 20 июня 2012 г. № 615 // СПС «КонсультантПлюс».

3. Об утверждении Правил подготовки правовых актов в территориальных органах Министерства внутренних дел Российской Федерации: приказ МВД России от 26 декабря 2018 г. № 880 // СПС «КонсультантПлюс».

4. О мерах по переходу на электронный документооборот: распоряжение МВД России от 9 ноября 2015 г. № 1/9112 // СПС «КонсультантПлюс».

5. *Тюркин М. Л.* Об информатизации органов внутренних дел // Информатизация и информационная безопасность правоохранительных органов. М., 2012. С. 1–3.

П. И. ИВАНОВ,
главный научный сотрудник
научно-исследовательского центра,
доктор юридических наук, профессор, заслуженный юрист РФ
(Академия управления МВД России)

А. С. ШИТОВ,
адъюнкт 3-го факультета
(подготовки научных и научно-педагогических кадров)
(Академия управления МВД России)

К вопросу о важности приспособления механизма противодействия налоговой преступности к цифровой реальности

Новая современная реальность, как показало изучение исследуемой проблемы, такова: широкое распространение получили методы и технологии (информационно-телекоммуникационная сеть), информационно-поисковые системы, автоматизированные банки данных, электронный документооборот и другие новшества, которые криминально активные лица всячески пытаются использовать в преступных целях. Нередко приходится проводить оперативно-разыскные мероприятия в виртуальном пространстве.

Как нам представляется, происходящие перемены требуют научного их осмысления. Уже сегодня следует искать пути и способы адаптации существующего механизма оперативно-разыскного противодействия, например, налоговой преступности к цифровой реальности.

Под цифровизацией нами понимается процесс перехода с аналоговой формы передачи информации на цифровую. Иначе говоря, это средство получения желаемого результата. При этом ключевым является цифровая трансформация традиционных сил, средств, методов, форм ОРД и оперативно-разыскных мероприятий. Указанные сведения в конечном итоге будут представлены в цифровой форме.

Что же касается цифровых технологий, то их мы рассматриваем как дискретную систему, которая базируется на способах кодирования и трансляции информационных данных, позволяющих решать разнообразные оперативно-тактические задачи за относительно короткие отрезки времени.

Авторы настоящей статьи на основе изучения и анализа правоприменительной практики подразделений экономической безопасности и противодействия коррупции (далее – ЭБиПК), научной литературы, нормативных правовых актов разработали модель, состоящую из трех относительно самостоятельных блоков, а именно: 1) идентификационные признаки, указывающие на вероятность подготовки и совершения преступлений налоговой направленности; 2) совокупность способов (схем); 3) примерный алгоритм принятия оперативно-разыскных и иных мер, в том

числе мероприятий, накладываемых на уже установленный способ противоправного действия проверяемых лиц. Все это, вместе взятое, мы назвали системой документирования. Для справедливости отметим, практика знает об этом. Однако с учетом нынешних реалий указанная система в научном плане не подвергалась осмыслению. Мы со своей стороны полагаем, что автоматизация процессов, связанных с документированием (ключевым моментом оперативно-разыскного противодействия налоговой преступности), – давно назревшая задача.

Рассмотрим более подробно каждый блок по отдельности.

Первый блок: идентификационные признаки, указывающие на вероятность подготовки и совершения преступлений налоговой направленности.

Эти признаки, на наш взгляд, следует делить на основные и факультативные. К числу основных мы относим: расхождение общих расчетно-плановых экономических показателей поступления налогов с их реальным поступлением; предоставление налогоплательщиками «нулевой» налоговой отчетности; расхождение в структуре поступления налогов различных видов по сравнению с расчетно-плановой структурой налоговых платежей (это свидетельствует о том, что какой-то вид налогов недоплачивается и, возможно, укрывается); несоответствие расходов налогоплательщиков тем доходам, по которым они отчитываются перед налоговыми органами. При изучении и анализе разного рода несоответствий следует особо обращать внимание на *документальные* – между первичными документами и документами реальной хозяйственной деятельности, а также между разными первичными документами; *учетные* – между данными учета и отчетности, учетом и первичными документами либо внутри учета (например, между его аналитической и синтетической частями); наличие материальных подлогов в документах, связанных с расчетами величины дохода (прибыли) и сумм налога.

Что же касается факультативных признаков, то ими, в частности, являются: несоблюдение установленных правил ведения учета и отчетности; нарушения правил производства кассовых операций; необоснованные списания товарно-материальных ценностей; неправильное ведение документооборота; нарушения технологической дисциплины.

Важно знать, что отдельно взятый признак может не указать на сам факт возможного совершения преступления налоговой направленности. Их, как правило, анализируют в комплексе, чтобы убедиться в правильности отрабатываемой оперативно-разыскной версии.

Второй блок: совокупность способов (схем), известных правоприменительной практике подразделений ЭБиПК, обслуживающих объекты налогообложения.

Знание сотрудниками подразделений ЭБиПК способов совершения налоговых преступлений позволяет им выбрать оперативно-тактическую ситуацию, в рамках которой в последующем можно определить круг

необходимых оперативно-разыскных и иных мероприятий по фиксации и закреплению того или иного способа противоправных действий проверяемых лиц.

Типичными способами совершения анализируемых видов преступлений выступают: совершение фиктивных сделок с использованием фирм-«однодневок», выступающих как схема оптимизации налогов; «искусственное дробление бизнеса» с целью применения специального налогового режима; применение льготных налоговых ставок; подмена договоров.

Приведем краткую характеристику всех вышеназванных способов.

Классической схемой уклонения от уплаты налогов является применение *фиктивных сделок* с целью увеличения стоимости приобретенного товара или услуг – завышение расходной части либо занижение доходной части (продажа товара по заниженной стоимости).

На «*искусственное дробление бизнеса»* указывают следующие действия: разделенные организации осуществляют один вид деятельности, находятся по одному юридическому адресу, используют одни и те же помещения, один и тот же персонал, имеют единую материально-техническую базу, одних заказчиков, представляют собой единый комплекс, вовлеченный в единый производственный процесс; ведение налоговой и бухгалтерской отчетности одними лицами, оказание услуг одним заказчикам; сотрудники организаций выполняют одну и ту же работу в соответствии с должностными обязанностями, у сотрудников может быть одежда с единым логотипом; организации совместно хранят бухгалтерские документы и документы по ведению финансово-хозяйственной деятельности, используют единый IP-адрес; расчетные счета компаний открыты одними и теми же лицами в одних и тех же банках; товарно-материальным обеспечением занимается один менеджер по снабжению; в случае приближения получаемых доходов в одной из организаций группы взаимозависимых лиц к лимиту по упрощенной системе налогообложения договоры с заказчиками либо расторгаются, либо заключаются дополнительные договоры с другой взаимозависимой организацией на тех же условиях.

Как видим, в современных условиях «искусственное дробление бизнеса» – несколько нетрадиционный способ ухода от налогообложения.

Применение льготных налоговых ставок. Чтобы скрыть доходы от налоговой инспекции, здания и техника переводятся компании-резиденту особой экономической зоны (далее – ОЭЗ), который платит налог на прибыль по ставке 0 %. При этом те же самые активы налогоплательщик берет в аренду у резидента ОЭЗ. В итоге у компании образуется расход, уменьшающий налог на прибыль, а у резидента-льготника – доход, с которого он налог не платит.

Подмена договоров. На практике чаще всего встречается подмена договора купли-продажи, который, в зависимости от обстоятельств,

преподносится как договор комиссии, как договор лизинга либо как договор реализации долей в уставном капитале. С целью ухода от НДС с аванса компании заключают договор займа, а после отгрузки товара засчитывают заемные средства в счет его оплаты; или заключают с контрагентом договоры комиссии, хотя реально осуществляют сделки по купле-продаже товаров.

Третий блок: примерный алгоритм принятия оперативно-разыскных и иных мер, в том числе мероприятий, накладываемых на уже установленный способ противоправного действия проверяемых лиц.

В свою очередь, в рамках этого блока мы выделяем три группы мер (комплексов), направленных на установление всех лиц, причастных к совершению налогового преступления, обстоятельств, связанных с данным противоправным деянием, а также обеспечение возмещения причиненного материального ущерба от налогового преступления. Вся работа в рамках указанных комплексов осуществляется в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ.

Предложенная нами модель теснейшим образом связана с современной информационной технологией. Такая технология, например, применительно к документированию противоправных действий лиц, совершающих налоговые преступления, на наш взгляд, должна включать в себя:

– цели и основные задачи развития и использования информационных технологий в процессе документирования противоправных действий лиц, совершающих налоговые преступления;

– основу (предпосылки) для разработки (корректировки) ведомственных нормативных правовых актов, относящихся к сфере противодействия налоговой преступности;

– использование имеющегося опыта адаптирования информационных технологий в рассматриваемой области;

– искусственный интеллект (комплекс технологических решений);

– заранее заданный алгоритм при решении конкретных оперативно-тактических задач в ходе документирования (речь, прежде всего, идет об автоматизации рутинных (повторяющихся) «производственных» операций);

– программное обеспечение (основа – методы машинного обучения);

– массив собранных подразделениями ЭБиПК оперативно значимых данных;

– информационно-телекоммуникационную сеть, включая сеть Интернет;

– поиск средствами вычислительной техники приемлемого решения на различных этапах процесса документирования;

– общий («сквозной») характер применения прикладных технологических решений при организации документирования противоправных действий лиц, совершающих налоговые преступления;

– совокупность факторов, влияющих на развитие информационных технологий;

– основные принципы их развития и использования;

– предупреждение и минимизацию рисков (исключение умышленного причинения вреда) при внедрении информационных технологий;

– обеспечение доступности и качества выходных данных (после их обработки), необходимых для процесса документирования.

Из-за ограниченности объема настоящей статьи нам не представляется возможным более подробно рассмотреть все элементы названной системы. Укажем лишь некоторые базы данных ФНС России как федерального органа исполнительной власти, осуществляющего функции по контролю и надзору за соблюдением законодательства о налогах и сборах, Росфинмониторинга и ФТС России.

Автоматизированная информационная система ФНС России (АИС «Налог-3») представляет собой единую информационную систему, обеспечивающую автоматизацию деятельности ФНС России по всем выполняемым функциям, определяемым Положением о Федеральной налоговой службе.

Федеральная информационная адресная система (ФИАС) – федеральная государственная информационная система, обеспечивающая формирование, ведение и использование содержащихся в государственном адресном реестре сведений об адресах.

Электронный сервис «Прозрачный бизнес» позволяет получить комплексную информацию о налогоплательщике – организации.

Открытый реестр сведений о налогоплательщиках – ЕГРЮЛ (ЕГРИП).

Единая информационная система в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма *Росфинмониторинга*.

Единая автоматизированная информационная система таможенных органов *ФТС России*.

Содержащаяся в указанных системах информация в установленном порядке используется сотрудниками подразделений ЭБиПК при рассмотрении ими жалоб, заявлений, обращений граждан и должностных лиц, а также при проверке данных, полученных оперативным путем. Тем самым им удается во многом обеспечить полноту и всесторонность их рассмотрения. Сочетание данных, полученных из гласных и негласных источников, позволяет целенаправленно вести оперативно-разыскную работу.

Большое обилие дискретной и неструктурированной информации, которая после ее обработки может быть полезна в интересах решения оперативно-тактических задач при выявлении и документировании налоговых преступлений, подразумевает налаживание тесного взаимодействия ОВД и их подразделений ЭБиПК с налоговыми и другими государственными органами.

Несмотря на наличие в ФКУ «ГИАЦ МВД России» централизованных автоматизированных систем оперативно-разыскного назначения, потребность использования баз данных других министерств и ведомств пока что реально существует. Отрадно, что большинство централизованных учетов оперативно-разыскного назначения, находящихся в ФКУ «ГИАЦ МВД России», в настоящее время автоматизированы. Как известно, информация концентрируется в автоматизированных информационно-поисковых системах (АИПС), автоматизированных информационных системах (АИС), автоматизированных банках данных (АБД). В этих системах концентрируется информация, представляющая интерес и для сотрудников подразделений ЭБиПК.

В заключение статьи представляется возможным сформулировать следующие выводы.

Во-первых, на цифровую информационную платформу оперативно-разыскная работа наряду с другими видами правоохранительной деятельности неизбежно перейдет.

Во-вторых, традиционные средства и приемы документирования преступных действий лиц, совершающих преступления налоговой направленности, будут последовательно заменяться новыми, основанными на цифровых технологиях алгоритмами: глобальным использованием больших данных, применением компьютерных программ для анализа этих данных и выработки на их основе проектов оперативно-служебных документов.

В-третьих, внедрение цифровых технологий предполагает кодирование и трансляцию информационных данных, позволяющих решать разнообразные задачи за относительно короткие отрезки времени. Внедрение указанных технологий призвано ускорить ведение дел оперативного учета, а также документирование преступных действий лиц, совершающих преступления налоговой направленности.

О. О. ИЛЛАРИОНОВА,
слушатель 2-го факультета заочной формы обучения
(Академия управления МВД России)

Совершенствование правовых основ деятельности начальника территориального органа МВД России на районном уровне в век информационных технологий

Информационные технологии постепенно охватывают все области человеческой деятельности – социальную, культурную, производственную. Они традиционно используются для автоматизации большого числа монотонных и рутинных операций: документооборот, задачи учета, контроля и распределения различных ресурсов, задачи, связанные с большим объемом вычислений.

В современном мире информационные технологии находят все более широкое применение при решении задач, требующих нестандартного, творческого подхода, начиная с задач управления (прогнозирование и принятие оптимальных решений) и заканчивая методом математического моделирования.

ОВД представляют собой сложную систему социально-правового управления, характеризующуюся материальными, пространственными, временными, энергетическими и информационными связями. Параметры этих связей поддаются количественной оценке, а система в целом допускает формализацию. Благодаря этому появляется возможность использования математических методов и основанных на них информационных технологий для оптимизации процессов управления в системе ОВД.

Успешное применение передовых информационных технологий в правоохранительной сфере зависит не только от степени владения личным составом необходимыми теоретическими знаниями и практическими навыками в указанной сфере, но и от регламентации порядка, сроков, механизма их внедрения.

В соответствии со ст. 11 Федерального закона «О полиции» использование достижений науки и техники, современных технологий и информационных систем является одним из принципов деятельности полиции [2]. Так, полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Кроме того, полиция в порядке, установленном законодательством РФ, применяет электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями; использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств

совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности.

При осуществлении управленческой деятельности руководитель территориального органа МВД России выполняет ряд функций, которые можно дифференцировать на аналитическую, информационную, планирование, учет, контроль, ресурсное обеспечение и др.

Каждая из функций подразумевает выполнение конкретных действий. Так, выполнение информационной функции подразумевает сбор и аналитическую обработку информации, поступающей из различных источников, а также передачу части информации вышестоящим органам, органам государственной власти, местного самоуправления, средствам массовой информации и гражданам в соответствии с действующим законодательством. Данная функция может реализовываться через целый ряд действий: изучение нормативных правовых актов; изучение ненормативной документации системы МВД России; организацию проведения различных мероприятий; оказание методической помощи подчиненным и доведение до них оперативной информации; сбор отчетности с подчиненных и ее аналитическую обработку; составление отчетов о деятельности районного ОВД для предоставления вышестоящим органам; предоставление информации средствам массовой информации о текущей деятельности ТО МВД России на районном уровне и т. д. В свою очередь, анализировать организационную деятельность начальника ТО МВД России на районном уровне можно, разделив ее на два компонента: внутреннюю деятельность, направленную на обеспечение эффективного функционирования подразделения, и внешнюю деятельность, направленную на охрану прав и свобод личности путем создания условий для их безопасной реализации. Внутриорганизационная деятельность обусловлена теми мероприятиями, которые выполняются для обеспечения внешней деятельности, напрямую от них зависит. Внутренняя среда производна. В век информационных технологий начальник должен таким образом выстраивать внутреннюю деятельность, чтобы его подчиненные могли наиболее эффективно решать внешние задачи, используя достижения науки и техники.

Совершенствование деятельности начальника ТО МВД России на районном уровне может происходить как путем внесения изменений в действующую нормативную базу, регулирующую его деятельность, так и путем совершенствования организационных и научно-методических условий его деятельности в рамках действующих нормативных актов.

В настоящее время руководители ТО МВД России на районном уровне проявляют творческий подход в поиске и внедрении программного обеспечения, технологий учета, контроля и т. д., которые могли бы быть им полезны в повседневной деятельности. Существуют положительные примеры внедрения современных информационных технологий, в том числе

запатентованных, которые доказали свою эффективность в ряде ТО МВД России на региональном уровне (например, в МВД по Республике Татарстан, МВД по Чувашской Республике и др.).

Однако обмен положительным опытом между ТО МВД России по различным субъектам в части, касающейся внедрения информационных технологий, отсутствует. Не предусмотрен порядок обмена успешно зарекомендовавшими себя информационными технологиями между территориальными органами и в рамках нормативных правовых актов.

Если обратиться к нормативному регулированию деятельности руководителей ТО МВД России на районном уровне, то можно заметить, что практика формирования нормативной базы деятельности территориальных органов МВД складывается таким образом, что вносимые в нормативные акты изменения запаздывают за изменениями в жизни общества. Такая ситуация характерна для всех органов исполнительной власти, которые все время вынуждены «догонять» изменения в реальной жизни, подстраиваясь под них таким образом, чтобы наиболее эффективно выполнять стоящие перед ними задачи, и вовсе не является следствием несвоевременной реакции на происходящие изменения.

В пределах своей компетенции начальник ТО МВД России на районном уровне может сам издавать локальные нормативные акты. Данные акты являются обязательными для исполнения всеми сотрудниками, находящимися в его подчинении. Однако, когда речь идет о внедрении и использовании новых информационных технологий путем регламентации механизма в локальном нормативном акте, новый алгоритм может быть интересен и для других ТО МВД России на районном уровне.

Поскольку от деятельности начальника ТО МВД России на районном уровне во многом зависит эффективность функционирования возглавляемого им органа и реализация стоящих перед данным органом задач, деятельность руководителя должна быть четко и полно нормативно урегулирована. Однако, как справедливо замечает О. Ю. Коневская, «используемая методологическая база и имеющееся структурирование функций должностных лиц в статусных документах (положениях), безусловно задав вектор развития системе государственной власти, не являются совершенными» [5].

Следует отметить, что общественные отношения в сфере деятельности ОВД регулируются большим количеством нормативных правовых актов различного уровня. Основываясь на Конституции РФ, данные отношения регулирует целый ряд федеральных законов, основными из которых можно назвать «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации», «О социальных гарантиях сотрудникам органов внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» [1], «О полиции» [2], «Об оперативно-розыскной деятельности» [3] и др. В соответствии с ними принят целый ряд подзаконных актов, которые регулируют данную сферу отношений.

Основным нормативным актом, непосредственно устанавливающим полномочия начальника ТО МВД России на районном уровне, является приказ МВД России от 5 июня 2017 г. № 355 [4].

В соответствии с приказом территориальный орган в целях реализации своих полномочий имеет право использовать достижения в области науки и техники, современные технологии и информационные системы (п. 11). Вместе с тем регламентированный порядок их внедрения, в частности при реализации полномочий начальника ТО МВД России на районном уровне, отсутствует. На наш взгляд, целесообразно было бы рассматривать внедрение информационных технологий при реализации полномочий в трех аспектах: при осуществлении управленческой деятельности, исполнительской и правоприменительной.

Деятельность начальника ТО МВД России на районном уровне должна проходить на научной основе, с использованием новейших достижений науки и техники. Как отмечает по данному поводу А. Д. Ульянов, «научная организация труда – это постоянный, проходящий при строжайшем соблюдении требований законодательства процесс совершенствования оперативно-служебной деятельности, основанный на новейших достижениях науки и практики, имеющий своей целью повышение результативности (продуктивности) труда и призванный содействовать его экономии» [6].

Действительно, научный прогресс и научная организация труда позволяют более качественно и быстро выполнять стоящие перед территориальным органом задачи, наилучшим образом распределять людские и временные ресурсы, рационализировать деятельность ТО МВД России на районном уровне, улучшить условия труда, что благоприятно сказывается на коллективе. Обеспечение коллектива современными техническими средствами, использование передовых технологий и соответствующего программного обеспечения позволяет осуществлять сбор информации, своевременную ее передачу заинтересованным лицам и быстрое ее получение от других лиц в случае необходимости, совершенствует и упрощает оперативно-служебную деятельность, повышает ее результативность.

Однако отсутствие регламентированного механизма гарантированного получения передовых информационных технологий и соответствующего программного обеспечения способствует затягиванию процесса совершенствования оперативно-служебной деятельности. В условиях стремительно развивающихся технологий деятельность руководителя должна совершенствоваться такими же темпами.

Подводя итог вышесказанному, можно сделать вывод, что научная организация труда, а также четкая регламентация порядка использования современных информационных технологий в оперативно-служебной деятельности, в частности их гарантированного получения и обмена положительным опытом по внедрению, позволят начальнику ТО МВД

России на районном уровне как самому овладевать новыми приемами и знаниями, так и значительно улучшить деятельность подчиненных.

Список литературы

1. О социальных гарантиях сотрудникам органов внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 19 июля 2011 г. № 247-ФЗ (ред. от 23 апреля 2018 г.) // Собр. законодательства Рос. Федерации. 2011. № 30 (ч. 1). Ст. 4595.
2. О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 18 июля 2019 г.) // Собр. законодательства Рос. Федерации. 2011. № 7. Ст. 900.
3. Об оперативно-розыскной деятельности: федер. закон от 12 августа 1995 г. № 144-ФЗ (ред. от 6 июля 2016 г.) // Собр. законодательства Рос. Федерации. 1995. № 33. Ст. 3349.
4. Об утверждении Типового положения о территориальном органе Министерства внутренних дел Российской Федерации на районном уровне: приказ МВД России от 5 июня 2017 г. № 355 // Рос. газ. 2017. № 7320.
5. *Коневская О. Ю.* Функции управления МВД России в контексте требований административной реформы // Труды Академии управления МВД России. 2009. № 2 (10). С. 48.
6. *Ульянов А. Д., Никитин М. Н.* Организация деятельности руководителя территориального органа МВД России: учеб. пособие. М., 2016. С. 41.

Р. М. ИСАЕВА,
начальник кафедры уголовного процесса,
кандидат юридических наук, доцент
(Уфимский юридический институт
МВД России)

Э. Д. ФАЙРУШИНА,
заместитель начальника кафедры
уголовного процесса,
кандидат юридических наук
(Уфимский юридический институт
МВД России)

Отдельные проблемы обеспечения государственного статистического учета преступлений

В настоящее время вопросы статистической отчетности преступлений являются актуальными для нашей страны. Уровень достоверности статистической информации обусловлен функционированием правоохранительных органов и организацией работы по оформлению, сбору, переработке предоставляемых сведений для государственной системы учета преступлений. Вопросам координации деятельности по улучшению ситуации с регистрацией преступлений главой государства В. В. Путиным было уделено особое внимание на расширенном заседании коллегии Генеральной прокуратуры РФ, проходившем 15 февраля 2018 г. Там же Ю. Чайка подчеркнул, что первоочередной задачей являются выработанные мероприятия по развитию государственной автоматизированной системы правовой статистики [3].

Важность рассматриваемой деятельности раскрыта в проекте Указа Президента РФ «О государственной автоматизированной системе правовой статистики» [2], а также во внесенных 27 июня 2019 г. Правительством на рассмотрение Госдумы проектах федеральных законов «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственного единого статистического учета данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» и «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации». Цель законопроектов – обеспечить государственные органы и граждан достоверной и полной статистической информацией о результатах рассмотрения сообщений о преступлениях, состоянии преступности, результатах следственной работы, дознания и прокурорского надзора, создать эффективные механизмы общественного контроля с целью обеспечения независимого экспертного мнения в области изучения

социальных причин преступности, оценки эффективности работы государственных органов, своевременного выявления проблемных районов и регионов, а также создать эмпирическую базу для развития отечественной криминологической науки [4].

Сегодня единообразие и полнота отражения в формах государственного статистического учета определяется Положением о едином порядке регистрации уголовных дел и учета преступлений, утвержденным приказом Генеральной прокуратуры РФ, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений» [1] (*далее – Приказ*). Единый учет преступлений заключается в первичном учете и регистрации преступлений и иных объектов учета. От надлежащей постановки первичного учета зависит полнота и достоверность показателей, характеризующих состояние преступности, указанная деятельность регулируется Инструкцией о порядке заполнения и представления учетных документов (приложение № 3 к Приказу) *(далее – Инструкция)*. Обратимся к аспектам, касающимся заполнения лицами, проводящими расследование и судебное производство, документов первичного учета преступлений (статистических карточек).

В некоторых статистических карточках прослеживаются ***дублирующие реквизиты.*** К примеру, в статистической карточке формы № 1 «На выявленное преступление» имеются реквизиты 26 «Способ совершения преступления» и 28 «Преступление совершено с использованием…». Так, реквизит 26 по справочнику 12 «О способе совершения преступления» (например, преступление совершено с использованием сети Интернет, предметов в качестве оружия и т. д.) совпадает с реквизитом 28, что способствует двойному отражению сведений в статистической карте и приводит к нарушению принципа процессуальной экономии времени органов предварительного расследования.

Остается нерешенным отдельный вопрос ***при заполнении статистических карточек форм № 1.1 (реквизит 13), № 2 (реквизит 36) – «Преступление совершено лицом в состоянии … наркотического, токсического опьянения».*** К примеру, согласно материалам уголовного дела, возбужденного по признакам преступления, предусмотренного ст. 264.1 УК РФ, подозреваемое лицо отказалось от прохождения медицинского освидетельствования на употребление наркотических, токсических средств. Возникает вопрос, может ли в данном случае сотрудник, проводящий предварительное расследование, отразить сведения в статистической карточке о совершении преступления лицом, находящимся в наркотическом, токсическом опьянении, без медицинского освидетельствования. Указанный аспект также не отражен и в Инструкции.

Также имеется некоторая ***неопределенность и при заполнении статистической карточки формы № 3 «О движении уголовного дела» по многоэпизодным уголовным делам***. Например, при соединении одного

уголовного дела с другим в отношении одного и того же лица, согласно ч. 4 ст. 153 УПК РФ, «срок производства по ним определяется по уголовному делу, имеющему наиболее длительный срок предварительного расследования. При этом срок производства по остальным уголовным делам поглощается наиболее длительным сроком и дополнительно не учитывается». Однако в базах данных ИЦ субъектов РФ преступления, соединенные в одно производство, согласно п. 22 Инструкции, с учета не снимаются, вследствие чего возникает вопрос, должно ли должностное лицо, проводящее предварительное расследование, составлять статистическую карточку формы № 3 (например, при продлении срока расследования (реквизиты 9, 10), при направлении уголовного дела прокурору: с обвинительным заключением, актом, постановлением (реквизит 12.2) и т. д.) по присоединенным уголовным делам. Если указанные статистические карточки не выставляются, то как решить вопрос, что в базе данных ИЦ данные уголовные дела продолжают учитываться.

По многоэпизодным уголовным делам необходимо выделить и заполнение реквизита 10 «Установленная сумма материального ущерба» статистической карточки формы № 4 «О результатах возмещения материального ущерба и изъятия предметов преступной деятельности». В п. 28 Инструкции указано, что «установленная сумма материального ущерба включает в себя сумму ущерба по всем преступлениям, расследование по которым проводится в рамках одного уголовного дела», однако если производство основного дела ведется по преступлению неимущественного характера, то форма № 4 составляется на соединенное уголовное дело имущественного характера. Указанное требование в Инструкции не раскрывается.

Возникает ***сложность и в заполнении реквизита 32 «Предъявлен гражданский иск» статистической карточки формы № 4 «Об установленной сумме материального ущерба, результатах его возмещения и изъятия предметов преступной деятельности»,*** где отражен только заявленный материальный ущерб, а моральный вред не учитывается, что противоречит нормам УПК РФ, Конституции РФ и Положению, где в п. 11 в разделе II «Общие правила заполнения и предоставления статистических карточек» указано, что содержание заполненных реквизитов документов первичного учета должно полностью соответствовать имеющимся в уголовном деле материалам.

Конечно, необходимо отметить, что сам Приказ устарел, требует переработки в соответствии с действующим законодательством и, как следствие, внесения изменений в сопутствующие документы (статистические карточки, справочники и т. д.). Важно выделить, что облегчение заполнения сведений статистического учета преступлений органами, проводящими предварительное расследование, судебное производство, должно быть первоочередным, в связи с чем предлагается создать условия и провести соответствующие мероприятия, организовать

обучение сотрудников, рассматривать указанные вопросы на курсах повышения квалификации, в образовательных организациях предусмотреть выделение отдельных часов для обучающихся по составлению документов первичного учета.

Список литературы

1. Положение о едином порядке регистрации уголовных дел и учета преступлений: утв. приказом Генеральной прокуратуры РФ, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений» // Рос. газ. 2006. № 13.

2. URL: http://www.garant.ru/products/ipo/prime/doc/56587365/#ixzz5T myx4moa (дата обращения: 12.06.2020).

3. URL: http://www. kremlin.ru (дата обращения: 12.06.2020).

4. URL: https://minjust.ru/ru/novosti/zakonoproekty-sovershenstvuyushchie-sistemu-gosudarstvennogo-statisticheskogo-ucheta-dannyh (дата обращения: 12.06.2020).

А. Н. КОНЕВ,
начальник Академии управления МВД России,
доктор технических наук, кандидат юридических наук, доцент,
академик Российской академии юридических наук

Идеологема «состязательность» как предмет научного исследования

Идеологема «состязательность» является выражением феномена состязательной идеологии, которая в последнее время может быть презентована как самый яркий пример проектной идеологии. Вместе с тем сам этот проектный замысел не выпячивается, чтобы придать самому идеологическому замыслу характер проявления естественных законов. Формула «состязательная идеология» используется в юридической литературе как нечто само собой разумеющееся. Авторам, ее продвигающим, кажется, что она говорит сама за себя. Похожее отношение к этой формуле было и у нас, пока объективный научный интерес не потребовал обращения к подлинной сути явления, скрывающегося за этими уже ставшими привычными словами.

Однако постижение сущности состязательной идеологии по имеющимся сегодня источникам оказалось делом далеко не простым. И сложность состояла не только в том, что в описании состязательности идеологическая аргументация обычно подавляет беспристрастное научное обоснование. Основные трудности обусловлены тем, что в рамках сложившейся научной традиции исследователи не особо удосуживаются строгим разграничением идеологических и технологических аспектов в интерпретации состязательности, не разделяют онтологическую и методологическую аргументацию. Во всяком случае, нам так и не удалось отыскать источник, в котором бы четко и внятно формулировались постулаты состязательной идеологии, позитивно излагались ее основные концепты.

Как правило, вслед за заявлениями о приметах этой идеологии идет перечисление преимуществ технологических правил процедурного соревнования, вытекающих из разделения процессуальных функций, самостоятельности суда, широты права на защиту и т. д. Все это, несомненно, имеет отношение к состязательности как таковой, но не раскрывает ее идеологических основ, не предъявляет тех ключевых идей, на которых и строится состязательная идеология.

В каком-то смысле можно говорить о том, что идеологическое предчувствие не сплетается в один узор с глубоким теоретическим пониманием. По мнению Н. А. Колоколова, «принцип состязательности, свойственные ему правоотношения многими российскими авторами не понимаются, а если и воспринимаются, то формально, в институциональном плане, в рамках, закрепленных законодательством, в результате чего такое сложное явление, как состязательность, получает

чисто нормативное, порой и схоластическое толкование. Состязательный процесс для них – данность, а не проблема, требующая решения» [17]. «С сожалением приходится констатировать, что российская правовая наука в настоящий период времени только приближается к пониманию феномена состязательного судопроизводства во всей его глубине, сложности и многообразии»[18].

Образ глубины профессором Н. А. Колоколовым задействован совсем не случайно. В свете нашего идеологического взгляда на процессуальные явления этот образ означает не что иное, как заинтересованность указанного ученого в приближении к концептуальной сущности состязательности. «Глубина» есть первое кодовое слово, призывающее на помощь уголовно-процессуальную концептологию. Мы согласны с Н. А. Колоколовым в том, что концептологического разбора феномена состязательности в отечественной науке пока не случилось, а потому не приходится говорить и о том, есть ли в науке осознание сущности состязательной идеологии.

Причем следует согласиться с профессором Н. А. Колоколовым и в другом важном наблюдении. Упрек в отсутствии должной глубины может быть адресован не только современникам, но и предшественникам. «Несмотря на обилие работ, опубликованных в конце XIX – начале XX в. по избранной нами тематике, говорить о серьезных «прорывах» в сфере состязательного судопроизводства не приходится»[19].

Следует заметить, что для этих упреков есть и свои идеологические причины. Безо всякого преувеличения можно говорить о том, что целое поколение российских ученых, яркими представителями которого являются А. Ф. Кони, В. К. Случевский, В. Д. Спасович, И. Я. Фойницкий и др., попали под гипнотическое очарование идеи состязательности. И даже не самой идеи в чистом виде, а ее юридического воплощения в англосаксонском уголовном процессе.

Этот тип уголовного процесса, равно как и других технологий государственного управления, вызывал неподдельный интерес у юристов той поры. Судить об этом мы можем хотя бы по следующей цитате: «Когда речь заходит о возможно лучшей организации государственных учреждений, каждый исследователь обращается к классической в этом отношении стране – к Англии, учреждения которой, по справедливому замечанию Спасовича, "подобно всем великим созданиям человеческого творчества, с одной стороны, весьма национальны, с другой стороны – способны к бесконечному космополитическому распространению". Заметим, кстати, что потребляемый довод о невозможности перенесения учреждений одной страны в другую заключает в себе слишком очевидные преувеличения и много недоразумения: нет ничего более противоречащего духовной

[17] Теория уголовного процесса: состязательность: монография / под ред. д-ра юрид. наук Н. А. Колоколова. Ч. 1. М., 2013. С. 20–21.
[18] *Там же.* С. 19.
[19] *Там же.* С. 19.

природе человека и общества, понятию об идеалах, как руководящей силе общественной жизни, наконец, и историческому опыту всех народов, чем утверждение, что, например, государственные учреждения Англии пригодны только для Англии»[20].

Таким образом, истинный смысл состязательности все еще скрыт от науки.

Вероятно, по этой причине схемы, «утаивающей» смысл идеи состязательности, на наш взгляд, придерживается и законодатель. Законодательная формулировка уводит этот вопрос в зону размежевания уголовно-процессуальных функций, а первая строчка (ч. 1 ст. 15 УПК РФ «Состязательность сторон») ни о чем особом не говорит. Это простая констатация – «уголовное судопроизводство осуществляется на основе состязательности сторон». Едва ли данное нормативное положение можно трактовать как идеологическое основание состязательности.

Для объяснения этого факта (сокрытия ключевых идей, концептов состязательности) вполне уместна была бы гипотеза, согласно которой термин «состязательная идеология» используется скорее для красоты и пафоса, нежели для сути, которая в конечном итоге упирается всего лишь в процедурные особенности, вытекающие из принципа конкуренции, присущего всем сферам человеческого бытия. Тот факт, что идея состязательности родилась не в юридическом процессе, а всего лишь им приспособлена, юридической наукой не отрицается. «Состязательность в праве, – пишет Р. А. Якупова, – является следствием и одной из форм социальной состязательности (конкуренции и конкурентности) и обусловлена различием между потребностями, интересами и целями взаимодействующих субъектов правовых отношений, что выражается в регулирующих эти отношения правовых нормах и механизмах, которые создают возможность для ее проявления и реализации»[21].

Однако гипотеза о том, что термин «состязательная идеология» используется исключительно для эстетических потребностей, не подтверждается по той простой причине, что в тех текстах, которые, по нашим оценкам, не содержали внятного повествования о сути состязательной идеологии (а порой и самого этого термина), все приметы идеологии присутствовали. Об этом, в частности, говорят как минимум две основные приметы, вытекающие из общего понятия идеологии.

Первая примета может быть названа нами *приметой позитивного идеологизирования.* Это создание своеобразного ореола божественности, выражающегося в констатации универсальности и исключительности принципа состязательности, в ее явных преимуществах не только перед

---

[20] *Михайловский И. В.* К вопросу об уголовном суде. По поводу предстоящей судебной реформы. Нежин, 1899. С. 28.

[21] *Якупова Р. А.* Состязательность в праве: теоретико-правовое исследование: автореф. дис. … канд. юрид. наук. М., 2010. С. 8–9.

конкурирующей идеологией инквизиционности, но и перед прочими идеологиями, так или иначе проявляющими себя в уголовном судопроизводстве. Причем указанный ореол может формироваться как в агрессивно-пропагандистской манере, так и в мягкой наукообразной форме с разными оговорками и допущениями. Пример подобной аргументации мы встречаем у той же Р. А. Якуповой. Она пишет: «В целом положительные качества состязательности в праве и ее юридически значимые последствия обеспечивают общественные выгоды, значительно перевешивающие присущие ей недостатки и неопределенности». И далее – состязательность «создает условия для максимально возможной сегодня объективности рассмотрения и справедливости решения в уголовном, гражданском и арбитражном процессе, защищает общество и государство от злоупотреблений правами и властными полномочиями»[22].

Как видим, автор ненавязчиво заявляет о том, что лучше состязательности для отечественного уголовного процесса нет ничего. Надо отдать должное, что в своей работе, идеализирующей состязательность, Р. А. Якупова обходится без критических выпадов в адрес конкурирующей инквизиционной идеологии. Но это скорее исключение, чем правило. Традиционно приверженцы состязательности считают своим долгом непременно умалить розыск и соответствующую ему идеологию.

«С 90-х годов, – пишет А. В. Смирнов, – состязательно-розыскная проблематика начинает обсуждаться в литературе. Лейтмотивом дискуссий за редким исключением являлось убеждение о необходимости преодоления розыскных начал в российском уголовном процессе и утверждения здесь состязательности. Однако отсутствие достаточно четкой и полной разработки этих понятий порой приводило к предложениям, не вполне адекватным благим намерениям самих авторов»[23].

Е. Г. Васильева замечает, что подобный подход сложился гораздо раньше. При этом ее вовсе нельзя заподозрить в симпатии к розыску. И тем не менее она считает своим долгом подчеркнуть, что «нет никакой возможности поспорить с тем, что поисковая технология в ее практической реализации, как показала история, гораздо больше подвержена злоупотреблениям, чем исковая. Но нельзя упускать из вида и другой очевидный факт: при любом сравнении исковой и поисковой технологии уголовного процесса первую обычно берут в ее лучшем виде, тогда как вторую – в худшем»[24].

Таким образом, мы выходим на вторую примету присутствия в текстах о состязательности идеологического компонента – это *примета негативного идеологизирования,* заключающаяся в неизменном обращении авторов к формированию образа врага (причем не только уголовного процесса, но

---

[22] *Там же*. С. 11–12.

[23] *Смирнов А. В.* Модели уголовного процесса. СПб., 2000. С. 5.

[24] *Васильева Е. Г.* Уголовный процесс: догматико-аксиологическое исследование: монография. М., 2013. С. 366–367.

и всего человечества), которого призвана победить или как минимум ослабить состязательность. И розыск в этом качестве вовсе не показательный пример. Есть у состязательности «враги» и посерьезнее.

Можно с полной ответственностью говорить о том, что идеологами состязательности планомерно создается учение об этом серьезном вражеском образе. Активное формирование этого образа – уже сложившаяся историческая традиция. Первая эпопея выявления врагов состязательности была предпринята еще во времена судебной реформы второй половины XIX в. И. Я. Фойницкий, С. В. Познышев, Н. Н. Розин и другие русские процессуалисты со всем свойственным им научным изяществом формулировали основные черты недружественных состязательности явлений.

Вторая мощная волна изгнания неугодных состязательности концептов пришлась на конец прошлого века. Не закончилась она и сегодня. Где бы ни начинались разговоры о состязательности как процессуальной панацее, всюду призывают этот образ врага. И тот факт, что он тщательно и пристрастно разработан, говорит о том, что состязательность действительно является идеологией. Ведь идеология – это априорное знание (учение) о благе, базовым блоком которого непременно выступает опять же преимущественно спекулятивное знание о том, что препятствует и вредит достижению этого блага. Несмотря на то, что о состязательности как о благе толкуют преимущественно в технологическом ключе, идеологические вкрапления здесь тоже встречаются. В то же время образ врага состязательности формируется исключительно на идеологических доводах (на лозунгах, антипатиях, спекулятивных обобщениях).

И вместе с тем активность в поиске врагов и убеждении в их существовании других не приносит весомых практических результатов. Практика такова, что современное уголовное судопроизводство не видит своего будущего в этой идеологии. Идеологи состязательности все чаще констатируют провалы своей идеологии. И очень жаль, что видят они в этом лишь происки врагов и козни недоброжелателей, а не слабость и научную несостоятельность основных концептов состязательной идеологии.

О. С. КУБАНОВ,
адъюнкт 3-го факультета (подготовки научных и научно-педагогических кадров)
(Академия управления МВД России)

Цифровые технологии обработки статистических данных при противодействии экономическим преступлениям в сфере сельского хозяйства

Современные цифровые технологии стремительно развиваются. Вместе с тем изменения и события, происходящие в нашей стране и мире, так или иначе связаны с цифровыми технологиями, что лишний раз подчеркивает актуальность их внедрения в деятельность ОВД. В настоящее время в российской науке наблюдается тенденция развития искусственного интеллекта путем проведения научных исследований, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области. Данные положения закреплены в Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [1].

Под цифровыми технологиями принято понимать технологии, использующие электронно-вычислительную аппаратуру для записи кодовых импульсов в определенной последовательности и с определенной частотой [7], в то время как в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» под информационными технологиями понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [2].

При совершении преступлений злоумышленниками нередко используются последние достижения науки и техники, в связи с чем перед ОВД стоит задача по совершенствованию своей научно-технической базы, инструментов сбора и обработки информации, по внедрению новых информационных технологий, что свидетельствует о тесной взаимосвязи между цифровыми и информационными технологиями.

Одним из обязательных условий реализации Национальной стратегии развития искусственного интеллекта является то, что положения стратегии должны учитываться:

– при реализации государственных программ, программно-целевых документов, эффективность реализации которых может быть повышена за счет использования технологий искусственного интеллекта;

– при реализации проектов, обеспечивающих достижение целей и показателей деятельности федеральных органов исполнительной власти (ведомственных проектов) [1] и т. д.

Как известно, начиная с 2008 г. приоритетный национальный проект «Развитие АПК» трансформировался в Государственную программу «Развитие сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия на 2013–2020 годы» (далее – Государственная программа). Мероприятия Государственной программы адаптированы к условиям членства России во Всемирной торговой организации. Для достижения целей Государственной программы выделены значительные бюджетные средства в виде субсидий, дотаций и грантов. На сегодняшний день объем бюджетных ассигнований составляет около 1 820 513 255 тыс. руб., в том числе в 2020 г. планируется оказать поддержку аграриям на сумму 294 062 010 тыс. руб. [8].

В этой связи возникает особая актуальность в организации деятельности ОВД, направленной на обеспечение целевого использования выделенных бюджетных средств, противодействия преступлениям в сфере агропромышленного комплекса, в том числе совершаемым в составе организованных преступных групп и сообществ, с использованием должностного положения, так называемым *коррупционным преступлениям*.

В соответствии с Положением о ГУЭБ и ПК МВД России [3] в числе главных задач подразделения – организация и участие в выявлении, предупреждении, пресечении и раскрытии тяжких и особо тяжких преступлений экономической и коррупционной направленности, в том числе в сфере сельского хозяйства. Вместе с тем ГУЭБ и ПК МВД России является подразделением центрального аппарата МВД России и выполняет, скорее, функцию стратегического управления по реализации государственной политики в сфере сельского хозяйства. Основная работа по данному направлению оперативно-служебной деятельности, на наш взгляд, все же проводится территориальными органами МВД России на региональном и районном уровнях.

В соответствии с приказом МВД России «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации» [4] оценка деятельности территориального органа МВД России складывается из вневедомственной (общественное мнение, освещение деятельности ОВД в СМИ, сведения о жалобах, количество мигрантов, уровень безработицы и т. д.) и ведомственной оценки – экспертная оценка и оценка деятельности территориального органа МВД России по статистическим показателям. Ведомственная оценка деятельности территориального органа МВД России по линии противодействия преступлениям в сфере сельского хозяйства формируется на основе экспертной оценки ГУЭБ и ПК МВД России. Полученные сведения об экспертных оценках по направлениям деятельности после обработки в ОАД МВД России обобщаются и направляются в ФКУ «ГИАЦ МВД России», где

производится их оценка, которая базируется на следующих подходах: а) расчет статистической оценки производится по показателям, отражающим конечный результат деятельности территориального органа МВД России по значимым направлениям; б) расчет статистической оценки с целью мониторинга оперативно-служебной деятельности территориального органа МВД России; в) показатели статистической оценки рассчитываются на основе официальной статистической информации.

Таким образом, по итогам отчетного периода в ФКУ «ГИАЦ МВД России» формируется массив сведений по линиям оперативно-служебной деятельности территориальных органов МВД России. Информация о деятельности подразделений ЭБиПК с результатами работы по противодействию экономическим преступлениям в сфере сельского хозяйства отражается в статистической форме «5-БЭП» (495). Данная форма охватывает достаточно широкий диапазон статистической информации, которая может иметь практическую пользу для руководителя при организации деятельности территориального органа МВД России по противодействию преступлениям в сфере сельского хозяйства при условии ее качественной обработки, анализа и выработки на ее основе управленческих решений. На наш взгляд, качественная обработка статистической информации позволит руководителю территориального органа МВД России: а) установить закономерности и тенденции развития оперативной обстановки в сфере сельского хозяйства на территории обслуживания; б) выявлять недостатки в организации оперативно-служебной деятельности подразделений ЭБиПК по противодействию преступлениям в сфере агропромышленного комплекса; в) составлять прогноз дальнейшего развития криминогенной обстановки в сфере сельского хозяйства на территории оперативного обслуживания; г) принимать управленческие решения по активизации работы на том или ином участке оперативно-служебной деятельности путем сосредоточения сил и средств с постановкой конкретных задач.

Тем не менее существует проблематика качественного анализа и обработки информации, что во многом обусловлено человеческим фактором. Зачастую недостаток квалифицированных кадров, сложность обработки большого массива данных и произведения математических расчетов приводят к тому, что объемы полезной статистической информации «пылятся на полке». Именно в таких случаях в деятельности руководителя и управленческого аппарата могут быть использованы современные цифровые и информационные технологии, позволяющие быстро, качественно и достоверно обрабатывать большие данные.

Внедрение цифровых и информационных технологий в деятельность ОВД является объектом научного интереса многих ученых и практиков, которые видят перспективу развития искусственного интеллекта, понимают неотвратимость его активного использования в будущем и уделяют значительное внимание исследованиям актуальных вопросов использования

информационных технологий в управленческой деятельности ОВД. Основной целью внедрения информационных технологий в сферу управления, как справедливо подчеркивает И. В. Горошко, является не только повышение его оперативности, но и эффективности за счет улучшения качества информационного обеспечения [5].

В рамках настоящей статьи на основе статистических сведений о результатах работы подразделений ЭБиПК по линии противодействия преступлениям в сфере сельского хозяйства за 2017–2019 гг. [6] автором предпринята попытка с помощью программы Microsoft Excel вывести некоторые закономерности, которые могут быть использованы в управленческой деятельности отдельно взятого территориального органа МВД России.

ГОДА	Ф.495 КН.101 - сельское хозяйство																								
	Количество преступлений, зарегистрированных в отчетном периоде		ИЗ НИХ:													Преступления, уголовные дела и материалы о которых				По оконченным и приостановленным уголовным делам (из числа находившихся в производстве)		Выявлено лиц, совершивших преступления	из них
			против собственности	в том числе		в сфере экономической деятельности	из них	налоговые	из них	против государственной власти, интересов государственной службы и службы в органах местного самоуправления	из них			против интересов службы в коммерческих и иных организациях	коррупционной направленности	предварительно расслед. в отчетном периоде(из числа наход. в производстве)	из них						уголовные дела о которых направлены в суд
				мошенничество	из них связано с незаконным возмещением НДС		незаконное предпринимательство		уклонение от уплаты налогов и сборов с организации		получение взятки	дача взятки	посредничество во взяточничестве				совершенных группой лиц либо группой лиц по предварительному сговору	совершенных ОПС или ПО	направлены в суд	размер причиненного материального ущерба / средний ущерб от одного преступления	наложен арест на имущество; добровольно погашено; изъято имущества, денег, ценностей на сумму		
2017	1486	показатели	994	544	29	260	8	179	53	85	8	7	0	49	313	1050	102	64	802	5588567	3617640	867	660
		доли от общ.	66,8	36,6	1,9	17,5	0,5	12,0	3,6	5,7	0,5	0,5	0,0	3,3	21,1	70,66	9,7	6,10	76,38	3760,8	64,73	1,21	76,1
2018	1252	показатели	861	647	19	214	15	132	39	76	25	11	0	43	274	844	84	7	654	8025473	5174253	749	551
		доли от общ.	68,7	51,7	1,5	17,1	1,2	10,5	3,1	6,1	2,0	0,9	0,0	3,4	21,9	67,41	10,0	0,83	77,49	6410,1	64,47	1,13	73,6
2019	1192	показатели	868	641	15	179	8	105	18	66	21	7	2	31	245	743	79	14	592	4449578	4810286	649	498
		доли от общ.	72,8	53,8	1,3	15,0	0,7	8,8	1,5	5,5	1,8	0,6	0,2	2,6	20,6	62,33	10,6	1,88	79,68	3732,9	108,11	1,14	76,7

Таблица выявленных преступлений в сфере сельского хозяйства за 2017–2019 гг.

Основными показателями деятельности подразделений ЭБиПК являлись: количество преступлений, зарегистрированных в отчетном периоде, в том числе: против собственности, в сфере экономической деятельности, налоговые, против государственной власти, интересов государственной службы и службы в органах местного самоуправления, против интересов службы в коммерческих и иных организациях и коррупционной направленности; выявленные преступления, уголовные дела и материалы; причиненный ущерб; количество выявленных лиц, совершивших преступления.

На основе вышеуказанных статистических данных, используя методы анализа и обработки информации, можно вычислить средний размер причиненного ущерба в течение 2017–2019 гг. В данном случае в 2017 г. в сельском хозяйстве было совершено 1 486 преступлений, а средний ущерб от одного преступления составил 3 760,8 тыс. руб., в 2018 г. – 1 252 преступления и 6 410,1 тыс. руб., в 2019 г. – 1 192 преступления и 3 732,9 тыс. руб.

За рассматриваемый период в сфере сельского хозяйства в 2013–2019 гг. наблюдалось резкое снижение, а затем длительный рост количества совершенных преступлений. С 2017 по 2019 гг. наблюдалось улучшение криминогенной обстановки либо спад выявляемости преступлений рассматриваемой категории.

С точки зрения организации деятельности руководителя территориального органа МВД России по противодействию преступлениям в сфере сельского хозяйства полезным будет отметить следующее.

1. У рассматриваемого вида преступлений нет четкой линии тренда, что в совокупности со спецификой этих преступлений свидетельствует о том, что их количество, в отличие от преступлений общеуголовной направленности, напрямую зависит от активности и эффективности работы ОВД в выявлении и документировании данной преступной деятельности. Таким образом, прослеживается взаимосвязь между инициативой ОВД по данному направлению оперативно-служебной деятельности и достижением поставленной цели.

2. Четко выражена тенденция того, что в общем объеме экономических преступлений в сфере сельского хозяйства снижается доля коррупционных преступлений. Это свидетельствует о том, что определенные положительные достижения по данному направлению деятельности имеются и коррупция идет на убыль либо становится более латентной, в связи с чем руководителю территориального органа МВД России важно: а) систематически, целенаправленно осуществлять деятельность по указанному направлению; б) организовать работу по подбору более качественных источников оперативной информации в отношении должностных лиц, причастных к коррупционным преступлениям.

3. Прослеживается тенденция роста преступлений имущественного характера, совершенных путем мошенничества, как в абсолютных числах, так и в долях. В совокупности, со снижением коррупционных преступлений наблюдается изменение структуры преступности – не только чиновники, но и обычные граждане вовлечены в процесс хищения бюджетных средств,

выделенных в рамках развития агропромышленного комплекса. В свою очередь, это свидетельствует о том, что действующие защитные механизмы не актуальны, их легко обойти – и обмануть государство можно и без коррупционной составляющей. В сложившейся оперативной обстановке актуальны вопросы межведомственного взаимодействия и совершенствования существующих организационных форм в сфере сельского хозяйства.

4. Анализ статистических данных свидетельствует о том, что на спад идет количество выявленных и расследованных преступлений в сфере сельского хозяйства. Несмотря на то, что в отчетном периоде могут расследоваться уголовные дела за совершение преступлений прошлых лет, в среднем этот показатель должен быть равным. В данном случае наблюдается снижение этого показателя с 70,7 % до 62,3 % – это прямое свидетельство волокиты и сложностей организационного характера при осуществлении деятельности по расследованию преступлений рассматриваемой категории.

5. Эффективность возмещения причиненного ущерба в среднем составляет 79,1 %, что является достаточно неплохим показателем, и тем не менее со стороны руководителя должны быть приняты дополнительные меры по активизации работы по установлению имущества подозреваемых, в том числе добытого преступным путем, с целью наложения ареста и дальнейшего возмещения причиненного вреда.

Кроме того, для эффективной организации деятельности по противодействию преступлениям в сфере агропромышленного комплекса, используя информационные технологии, можно создавать пространственные модели обработки статистических данных, характеризующих, к примеру, динамику регистрируемой преступности и производства сельскохозяйственной продукции (метод регрессии). На основе полученных данных можно проводить мероприятия профилактического характера в секторе производства сельскохозяйственных товаров, что, в свою очередь, может положительно отразиться на количестве регистрируемых преступлений рассматриваемой категории в будущем.

Таким образом, использование современных информационных технологий в деятельности ОВД позволяет в короткие сроки обрабатывать большие массивы данных, определять причины, условия и закономерности развития криминогенной ситуации на территории оперативного обслуживания и составлять прогнозы ее дальнейшего развития. В современных условиях использование информационных технологий в организации деятельности ОВД является одним из критериев успешного противодействия преступлениям в сфере сельского хозяйства.

Список литературы

1. О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года): Указ Президента РФ от 10 октября 2019 г. № 490 // СПС «КонсультантПлюс».
2. Об информации, информационных технологиях и защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».
3. Об утверждении Положения о Главном управлении экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации: приказ МВД России от 16 марта 2015 г. № 340 // СПС «КонсультантПлюс».
4. Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации: приказ МВД России от 31 декабря 2013 г. № 1040 // СПС «КонсультантПлюс».
5. Информационные технологии в управлении органами внутренних дел: учебник / под ред. д-ра тех. наук, проф. И. В. Горошко. М., 2015.
6. Статистическая информация ФКУ «ГИАЦ МВД России» за 2017–2019 гг. (дата обращения: 20.11.2019).
7. URL: https://rus-official-terms.slovaronline.com/29427-Цифровые%20технологии (дата обращения: 20.11.2019).
8. URL: https://agro-ferma.ru/dayatelnost/rekonstruktsiya-sooruzheniy/stati/gosprogramma-razvitiya-apk-2013-2020-gody/ (дата обращения: 20.11.2019).

И. А. КУБАСОВ,
профессор кафедры информационных технологий,
доктор технических наук, доцент
(Академия управления МВД России)

А. Н. ДЕРЮГИН,
слушатель 2-го курса 2-го факультета
(Академия управления МВД России)

Оценка качества решений, принимаемых искусственным интеллектом

В середине XX в., когда компьютеров было мало, они были очень большими и дорогими, появился знаменитый тест Алана Тьюринга. На тот момент абсолютно всем было понятно, что выполнять арифметические действия ламповые компьютеры уже могут намного быстрее, чем человек. Однако переводить текст с одного языка на другой, играть в шахматы, доказывать теоремы и т. д. ламповые компьютеры еще не могли. В связи с этим Тьюринг предложил тестировать качество будущего искусственного интеллекта в диалоге обычного человека с вычислительной машиной. Человек задавал искусственному интеллекту обычные для людей вопросы. Компьютер должен был имитировать присутствие у него сознания известными на тот момент вычислительными процедурами. Например, на вопрос «Как дела?» компьютер мог случайно выбрать один из нескольких заранее записанных ответов: «Все отлично»; «Все нормально»; «Средненько» и т. п.

Естественно, что в широком контексте множества произвольных тем разговора человек-тестор всегда мог почувствовать, что он имеет дело с компьютером, а не с другим таким же человеком за стенкой, набирающим ответы на другой клавиатуре. Фиксируя длину диалога (после какого по счету вопроса человек-тестор принимал решение о подмене собеседника компьютером), можно было в первом приближении оценить качество искусственного интеллекта.

При проведении подобных численных экспериментов выяснилось, что сужение тематики диалога дает компьютеру неожиданное преимущество. Как только диалог попадал в очень узкую тематику (типа «мой автомобиль утром не завелся, почему?»), компьютер получал возможность долго отвечать разумно и задавать разумные вопросы. Этот режим оказался востребован практикой, проявилось множество прикладных экспертных систем [2], содержащих знания узких специалистов и оказывающих ощутимую помощь обычному человеку.

К началу 80-х годов стало понятно, что компьютеры лишились ламп и многократно уменьшились в размерах, перейдя на микросхемы

и микропроцессоры. Искусственный интеллект начал играть со своими хозяевами в шахматы, сочинять музыку и переводить тексты с одного языка на другой. Естественно, что первые успехи искусственного интеллекта могли произвести значительное впечатление только на дилетантов, плохо играющих в шахматы, не умеющих писать музыку и способных переводить текст на другой язык только со словарем. Профессионал любого уровня чувствовал низкое качество работы первых приложений искусственного интеллекта и мог указать множество допускаемых им ошибок. Тем не менее даже самые первые приложения начали продаваться и покупаться. Дилетанты покупали приложения на всякий случай, профессионалы низкого уровня покупали потому, что могли легко поправить ошибки автомата и сэкономить свои личные затраты, утаивая от заказчиков причину снижения расценок на свою работу.

Как следствие, в обществе пришло понимание того, что искусственный интеллект следует делить на «слабый» и «сильный». «Слабый» интеллект – это то, что мы купим по приемлемой цене сегодня или завтра, прекрасно зная все его недостатки. «Сильный» интеллект – это то, что сегодня не продается и завтра, скорее всего, продаваться всем подряд не будет и не получит массового применения.

За примером далеко ходить не приходится. В 1997 г. команда IBM из 100 программистов смогла написать шахматный движок, с помощью которого суперкомпьютер Deep Blue выиграл 6 партий в шахматы у чемпиона мира Гарри Каспарова. То есть был создан прецедент, когда по одному из множества узкоспециализированных приложений искусственный интеллект машины смог временно превзойти одного из лучших профессионалов-людей и стал очень «сильным». Если перевести это в плоскость детективной литературы, то появилась техническая возможность для любого выпускника института МВД России, допущенного к суперЭВМ, обыграть в шахматы профессора Мариарти (литературного гения преступного мира). Вполне возможно, что такая мысль будет помогать молодому лейтенанту полиции на первых порах в его оперативно-служебной деятельности.

Также стало очевидным, что космонавт во время длительного межпланетного перелета сможет удалить сам себе или своему коллеге воспалившийся аппендикс, если на борту межпланетного корабля будет присутствовать робот-хирург «Да Винчи» и его искусственный мозг.

Фактически искусственный интеллект за 70 лет своего развития стал играть не только техническую, но и политическую роль. Все прекрасно осведомлены о том, в какой стране была написана шахматная программа, обыгравшая чемпиона мира, где написаны операционная система Windows и программное обеспечение робота-хирурга. Однако ничто не вечно под луной. Так, весь мир в 2011–2012 гг. следил за тем, как в США была проведена политико-пропагандистская акция по созданию на их территории очередного самого мощного в мире суперкомпьютера «Титан». СуперЭВМ

«Титан» ввели в действие в 2012 г. на одной из закрытых территорий Министерства энергетики США. Однако «Титан» продлил лидерство США всего на 9 месяцев. В 2013 г. самая большая в мире вычислительная машина появилась на территории Китая – «Танхе-2». Китайцы добавили мощности к уже существовавшей у них вычислительной машине «Танхе-1» и легко обогнали гордость США – «Титан».

США претензии на их мировое лидерство по искусственному интеллекту никогда не скрывали, а однополярный мир охотно это поддерживал. Более того, после событий 11 сентября 2001 г. даже большинство граждан США согласилось отдать значительную часть своих конституционных прав государству. Все иные страны однополярного мира согласились добровольно уступить мировому лидеру свой национальный суверенитет по контролю биометрических данных своих граждан. Началось создание системы международных биометрических паспортов. В декабре 2002 г. был создан международный комитет по стандартизации ISO/IEC JTC1 sc37 («Биометрия»), который фактически осуществляет перевод национальных стандартов США в ранг международных стандартов. С 2003 г. Национальный институт стандартизации США (NIST) прекратил разработку национальных стандартов, полностью переключив свои усилия на разработку порядка 153 международных стандартов, ориентированных на закрепление за США статуса лидера биометрических приложений искусственного интеллекта. Действительно, большинство стран значительно отстают от США по искусственному интеллекту приложений биометрии, и им выгодно рассматривать сложившуюся ситуацию положительно как экономию своих собственных ресурсов.

Единственной страной, которая не полностью отказалась от своего суверенитета над биометрией своих граждан, является Россия. Только Россия продолжает создавать свои национальные стандарты по технологической ветви развития нейросетевой биометрии.

Причина, по которой Россия заняла такую позицию, состоит в фактическом саботировании США или, если угодно, мировым сообществом разработки надежных механизмов защиты персональных биометрических данных пользователей. Начиная с конца прошлого века (с введения в действие стандарта США NIST БиоАПИ-1998) активно продвигаются так называемые «нечеткие экстракторы» как механизм защиты биометрических данных. К сожалению, это техническое решение плохо справляется со своей основной задачей. «Нечеткие экстракторы» не учатся, они используют коды, способные обнаруживать и исправлять ошибки с 20-кратной избыточностью. Например, могут быть использованы БЧХ-коды. В этом случае выходной скорректированный код «нечеткого экстрактора» уменьшается в 20 раз и для рисунка отпечатка пальца составляет менее 16 бит (эквивалентный пароль доступа должен иметь длину от 1 до 2 символов).

Ситуация кардинально меняется, если отказаться от применения зарубежных «нечетких экстракторов» в пользу отечественных нейросетевых преобразователей биометрии. Если эти нейросетевые преобразователи выполнены в соответствии с требованиями отечественных стандартов, длина пароля доступа увеличивается до 32 символов случайного пароля.

Стойкость к атакам подбора пароля из 1 или 2 символов незначительна, однако рост длины пароля до 32 случайных символов кардинально меняет ситуацию. Так как выходной код пароля доступа для нейросетевых преобразователей всегда длиннее, чем у «нечетких экстракторов», отечественную технологию иногда называют высоконадежной. Принципиальным является также то, что пароли доступа из 1 или 2 случайных символов легко запоминаемы человеком, а вот пароль доступа из 32 случайных символов обычный человек запомнить уже не может. То есть нейросетевые преобразователи снимают с человека проблему запоминания длинных паролей из большого числа случайных знаков. Если при этом данные таблиц связей нейронов и весовые коэффициенты нейронов будут зашифрованы, объединив пакет международных стандартов с 7 российскими стандартами, мы фактически лишаем США преимуществ от свободного наблюдения биометрии граждан России и любой иной страны, воспользовавшейся российскими стандартами.

Понять, насколько это все эффективно и насколько меняется ситуация с безопасностью, проще всего, глядя на экранные формы обычных приложений парольного доступа и парольного доступа, поддерживаемого нейросетевой биометрией (см. рис. 1).

Из рис. 1 видно, что экранные формы обычного парольного доступа скрывают длину короткого пароля, усложняя тем самым задачу его подбора хакерам. Совершенно иная идеология закладывается в экранные формы биометрико-нейросетевой аутентификации. Нейросеть способна преобразовать биометрический образ в пароли любой длины, однако увеличивать длину кодов больше 32 случайных знаков (256 бит) нет смысла, так как ОС Windows и ОС Android не способны работать с кодами доступа большей длины. В связи с этим приложение биометрико-парольного доступа заранее объявляет всем, что придется набирать пароль максимально возможной длины или предъявить биометрический образ. При открытии экранной формы появляются 32 пустых (незаполненных) знакоместа пароля максимально возможной длины.

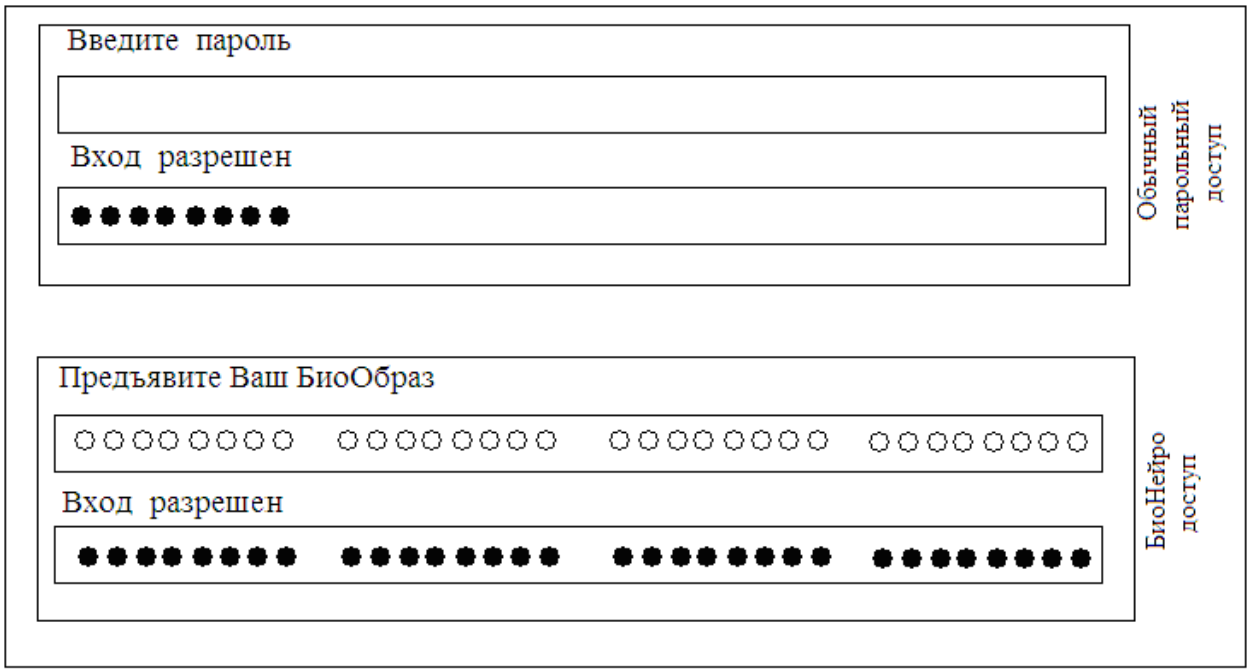

Рис. 1. Типовые экранные формы входа в компьютер обычного парольного доступа и биометрико-нейросетевого парольного доступа

Экранная форма предупреждает хакеров о высокой сложности стоящей перед ними задачи подбора длинного пароля из 32 случайных клавиш. Примерно то же самое предупреждение получают злоумышленники, пытающиеся выудить пароль доступа или ПИН-код по телефону. Обманутый пользователь, защищенный его же собственной биометрией, назовет по телефону все реквизиты своей банковской карты, а вот сообщить злоумышленнику свой длинный ПИН-код доступа он не сможет. Пользователь его не знает, он его ни разу не видел.

Таким образом, очевидно значительное отставание англоязычной (мировой) научно-технической мысли от уже стандартизованного в России положительного опыта быстрого тестирования нейросетевого искусственного интеллекта процедурами ГОСТ Р 52633.3-2011. Можно с уверенностью прогнозировать сохранение лидерства России в развитии практических приложений искусственного интеллекта усилиями нового технического комитета по стандартизации (ТК 164 «Искусственный интеллект»).

И. А. КУБАСОВ,
профессор кафедры информационных технологий,
доктор технических наук, доцент
(Академия управления МВД России)

В. Ф. ТЯГУНОВ,
заместитель начальника центра эксплуатации интегрированной мультисервисной телекоммуникационной системы ФКУ «Главный центр связи и защиты информации» – начальник отдела поддержки пользователей интегрированной мультисервисной телекоммуникационной системы,
слушатель 2-го курса 2-го факультета Академии управления МВД России

Соотношение уровня защищенности отечественного и международного искусственного интеллекта

Переход к использованию больших искусственных нейронных сетей. Рекомендации ФСТЭК России (ТК 362) и ФСБ России (ТК 26)

Идеология перехода к новым технологиям нейросетевого искусственного интеллекта проста. Так как классические коды с обнаружением и исправлением ошибок плохо справляются со своей задачей, необходимо корректировать ошибки кода «Свой» большими, заранее обученными искусственными нейронными сетями. Большие сети искусственных нейронов должны быть заранее специально обучены корректировать ошибки кода «Свой». Во время обучения они получают ЗНАНИЯ о стабильности всех контролируемых биометрических параметров. Уже за счет ЗНАНИЯ реальных статистик контролируемых биометрических параметров получается ВЫИГРЫШ. Классические коды (коды БЧХ) построены в рамках гипотезы равновероятных ошибок в любом разряде и отсутствия группирования ошибок. Эти гипотезы никогда не выполняются в кодах биометрии. Реальные биометрические данные образа «Свой» и образов «все Чужие», применительно к нашему случаю, достаточно хорошо описываются нормальным законом. Особенности корреляционной связанности и распределения состояний реальных биометрических данных не могут быть учтены иначе, чем через обучение нейронов.

С 2006 г. по настоящее время было разработано 9 национальных стандартов, 7 из которых введены в действие на территории РФ, а 2 проекта находятся на этапе публичного обсуждения (см. таблицу 1).

Следует отметить, что искусственный нейрон – это достаточно простая конструкция. Самый простой нейрон (персептрон) состоит из сумматора и квантователя (порогового элемента) на выходе сумматора. Набрать множество таких нейронов и организовать из них сеть очень больших размеров не сложно. Проблема состоит в том, как эту сеть из множества нейронов обучить. Существует несколько сотен алгоритмов обучения, однако все они, как правило,

итерационные, неавтоматические и занимают длительное время. Кроме того, итерационные алгоритмы обучения неустойчивы, а также требуют использования огромных баз биометрических образов. Для биометрии это не подходит, биометрические приложения должны обучаться на маленьких выборках, быть полностью автоматическими и иметь гарантии быстрого окончания процесса обучения. Под столь противоречивые требования в России разработан специальный стандарт ГОСТ Р 52633.5-2011 (строка 6 таблицы 1).

Принципиальным отличием нейросетевых преобразователей биометрии в длинный стабильный код является то, что каждый искусственный нейрон такого преобразователя отвечает за один разряд выходного кода. То есть разрядность выходного кода может быть любой: 128 бит, 256 бит, 512 бит.

Таблица 1

№	Номер и полное название национального стандарта
1	**ГОСТ Р 52633.0-2006** «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»
2	**ГОСТ Р 52633.1-2009** «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
3	**ГОСТ Р 52633.2-2010** «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
4	**ГОСТ Р 52633.3-2011** «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора»
5	**ГОСТ Р 52633.4-2011** «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа»
6	**ГОСТ Р 52633.5-2011** «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия - код доступа»
7	**ГОСТ Р 52633.6-2012** «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу "Свой"»
Обсуждение	Техническая спецификация (проект, публичное обсуждение начато с 01.02.2017 членами ТК 26 «Криптографическая защита информации») «ЗАЩИТА НЕЙРОСЕТЕВЫХ БИОМЕТРИЧЕСКИХ КОНТЕЙНЕРОВ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ»
Обсуждение	ГОСТ Р 52633.5+х-2019+х «Защита информации. Техника защиты информации. Автоматическое обучение сетей квадратичных нейронов с многоуровневым квантованием биометрических данных». Головной исполнитель проекта – Пензенский государственный университет

Все зависит от числа нейронов, объединяемых в одном нейросетевом преобразователе. Число входов у каждого нейрона – 16, в соответствии с ГОСТ Р 52633.5-2011 они подключены случайно без повторений к 512 входам всей нейросети. В качестве 512 биометрических параметров, анализируемых нейронной сетью, используются коэффициенты двухмерного Фурье-преобразования рисунков взаимного расположения особых точек папиллярных линий. Фактически это некоторый вариант JPEG-архиватора-конвертора, параметры которого специально подобраны под решаемую задачу. Сами по себе JPEG-архиваторы стандартизованы, однако под решаемую задачу известные варианты JPEG-архиваторов не подходят. В 2019 г. в России при Госстандарте был создан специальный технический комитет № 164 «Искусственный интеллект». Вполне вероятно, что в рамках этого технического комитета удастся разработать национальный стандарт по преобразованию изображений взаимного расположения особых точек отпечатков пальцев в данные, пригодные для автоматического обучения больших искусственных нейронных сетей алгоритмом ГОСТ Р 52633.5-2011 (строка 6 таблицы 1).

Высокий уровень доверия к нейросетевым решениям искусственного интеллекта, обученным алгоритмом ГОСТ Р 52633.5

Длина криптографического ключа (пароля доступа) в 16 бит (2 случайных символа) и длина в 256 бит (32 случайных символа) не сопоставимы по вычислительной сложности их подбора. Гражданин США или Евросоюза, попытавшийся защитить свои цифровые права в интернет-облаке «нечетким экстрактором» (паролем из двух случайных символов клавиатуры), вряд ли сможет быть уверенным в конфиденциальности своей информации. Совершенно иная ситуация возникает для граждан России. Новая технология позволяет им не запоминать длинные пароли доступа из случайных символов. Вполне достаточно предъявить свой биометрический образ (и в том числе рисунок отпечатка пальца) для того, чтобы из нейросети появился пароль доступа с максимально возможным числом случайных символов для операционных систем Windows или Android. Подобрать пароли из максимально возможного числа в 32 случайных символа практически невозможно.

Таким образом, отечественная нейросетевая защита от хакеров, подбирающих пароли, выходит на новый, гораздо более высокий уровень доверия. Естественно, что этот высокий уровень доверия должен быть проверен (подтвержден) испытательной лабораторией во время сертификации продукта защиты информации. Эта задача решается стандартом ГОСТ Р 52633.3-2011 (строка 4 таблицы 1).

Основная математическая идея стандарта состоит в упрощении вычислений. Упрощение вычислений достигается за счет перехода

от традиционного прямого анализа длинных кодовых состояний к коротким сверткам Хэмминга. При этом из разряда вычислительно сложных задач мы переходим в разряд решения задач с линейной вычислительной сложностью. Свертку Хэмминга, или расстояние Хэмминга, стандарт предлагает вычислять следующим образом:

$$h = 256 - \sum_{i=1}^{256} \begin{Bmatrix} c_i \\ \oplus \\ x_i \end{Bmatrix} \quad (1),$$

где c_i – состояние i-го разряда кода «Свой», x_i – состояние i-го разряда кода «Чужой», $\oplus$ – операция сложения по модулю два.

По сути дела, сравниваются между собой одинаковые разряды двух кодов и подсчитывается число не совпадающих между собой разрядов. Принципиально важным является то, что число состояний свертки Хэмминга по модулю два составляет всего 257, что много меньше числа исходных состояний свертываемых между собой кодов. Вторым важным моментом является то, что свертка Хэмминга вычисляется через суммирование 256 случайных состояний, т. е. по основной теореме статистики происходит нормализация данных. Таким образом, для выполнения статистических оценок не нужно привлекать тестовые базы, состоящие из миллиардов образов «Чужой». Нормальный закон определяется двумя статистическими моментами: математическим ожиданием E(h) и стандартным отклонением σ(h). Для вычисления этих двух статистических моментов вполне достаточно предъявления 64 случайно выбранных образов «Чужой»:

$$\begin{cases} E(h) \approx \frac{1}{64} \cdot \sum_{i=1}^{64} h_i \\ \sigma(h) \approx \sqrt{\frac{1}{63} \cdot \sum_{i=1}^{64} (h_i - E(h))^2} \end{cases} \quad (2).$$

В рамках гипотезы о нормальном распределении случайной величины оценка вероятности появления ошибок второго рода (вероятности случайного совпадения кодов «Свой» и «Чужой») сводится к вычислению следующего интеграла:

$$P_2 \approx \frac{1}{\sigma(h) \cdot \sqrt{2 \cdot \pi}} \int_0^1 \exp\left\{ \frac{-(v - E(h))^2}{2 \cdot \{\sigma(h)\}^2} \right\} \cdot dv \quad (3).$$

Тройки записанных выше уравнений достаточно для того, чтобы оценить риски принятия неверного решения отечественного нейросетевого искусственного интеллекта. Возникла уникальная для России ситуация: выполненный по национальным стандартам (см. таблицу 1) искусственный интеллект оказывается намного надежнее своих зарубежных аналогов, причем любой желающий может убедиться в этом, выполнив преобразования (1–3).

Новый уровень доверия к промышленно применимым сверточным (многослойным) нейросетевым приложениям

Одной из проблем промышленного применения искусственного интеллекта в целом и нейросетевого искусственного интеллекта в частности является неоднозначность оценок ошибок первого и второго рода у той или иной обученной нейронной сети произвольного вида. Осознание этой проблемы у мирового научно-технического сообщества появилось с появлением применения в промышленных приложениях глубоких (многослойных) сетей искусственных нейронов. Если опираться на научные традиции, то глубокие нейронные сети следует называть сетями Галушкина-Хинтона. Именно наш соотечественник А. И. Галушкин первым в 1974 г. предложил многослойные нейронные сети и метод обучения для них. Несмотря на то, что новая идеология была уже создана, на тот момент отсутствовали доступные вычислительные ресурсы, и про многослойные нейронные сети, а также про метод их обучения через обратное распространение ошибок забыли примерно на 10 лет как в России, так и в Европе.

Ситуация изменилась в период 1985–1986 гг., появилась перспектива реализации новых технологических идей, возник бум увлечения обучения многослойных нейронных сетей методом обратного распространения ошибок.

Достаточные вычислительные ресурсы появились только через 30 лет после пионерской работы Галушкина, наиболее значимыми по осмыслению новых технических возможностей являются работы Дж. Хинтона. Именно благодаря его усилиям технология стала промышленно востребованной. Так, исторически сложилось, что технологический прорыв был достигнут при решении биометрической задачи поиска и распознавания лиц людей. Как следствие, сегодня любая цифровая фотокамера способна находить в кадре лица людей.

Сегодня несколько сотен компаний разных стран владеют технологией обучения глубоких (от 30 до 1000 слоев) сетей искусственных нейронов, анализирующих порядка 1000 входных параметров образа. При этом, если производитель объявляет вероятности ошибок второго рода (вероятности случайного перепутывания разных образов) на уровне 0.001 (доверительная вероятность – 0.999), то для достоверной оценки этой величины требуется тестовая выборка примерно в миллион тестовых образов. Кто-то должен отвечать за формирование большой базы тестовых образов и за само проведение тестирования. Сегодня для глубоких нейронных сетей эта проблема решается через привлечение платного публичного сервиса по тестированию.

Такое решение проблемы вполне приемлемо для публичных приложений применения глубоких нейронных сетей (например, «умного коттеджа» с интернет-управлением автоматизированной отопительной

системой), однако этот подход неприемлем, когда речь идет о нейросетевых приложениях силовых ведомств.

Тестирование должно быть быстрым, эффективным и непубличным. Достоверные знания об уровне уязвимостей искусственного интеллекта силовых структур государства – это совершенно не публичная информация. Передача глубоких (сверточных) нейронных сетей для коммерческого тестирования какой-либо организации, находящейся вне юрисдикции России, недопустима.

Решить эту проблему удается добавлением к глубокой нейронной сети «широкой» нейронной сети, обученной по ГОСТ Р 52633.5.

Как только появляется длинный выходной код, начинают работать рекомендации ГОСТ Р 52633.3 и сложная задача формирования и применения очень больших тестовых баз биометрических образов упрощается многократно.

Соотношение мощности отечественного и международного искусственного интеллекта

Мощность искусственного и естественного интеллекта в первом приближении определяется тем, сколько образов интеллект может различать и применять на практике (интерпретировать). Мощность искусственного интеллекта, прежде всего, связана с размерностью решаемых им задач, а также с эффективностью его обучения.

Для формальной оценки мощности проще всего воспользоваться опытом криптографии. Публичное обсуждение документа ТК 26 (строка 8 таблицы 1) показало, что 256 выходных бит нейросетевого преобразователя отпечатка пальца (рисунок 2) не может рассматриваться как полноценный криптографический ключ. Полноценный ключ появится только тогда, когда предъявление на вход преобразователя случайных образов «Чужой» будет давать выходные коды с независимыми (некоррелированными) разрядами. Для реальных нейросетевых преобразователей «биометрия – код» этого не происходит. То есть вероятность угадывания выходного кода (см. формулу 3) всегда много выше, чем вероятность угадывания криптографического ключа длиной в 256 бит. Необходимо пересчитать длину видимого криптографического ключа с K=256 зависимыми разрядами в длину меньшего криптографического ключа – k с независимыми разрядами. Операция пересчета выполняется следующим образом:

$$k \approx -\log_2(P_2) \qquad (4).$$

Всегда длина короткого ключа k для нейросетевой биометрии оказывается от 2 до 3 раз выше, чем длина информационной части кодов с обнаружением и исправлением ошибок зарубежных «нечетких экстракторов». Именно по этой причине появился пакет национальных биометрических стандартов (см. таблицу 1), как дополнение к значительно

более слабым международным стандартам простых биометрических шаблонов.

Весьма важным является также то, что работы по созданию национальных биометрических стандартов России не остановились. В начале 2019 г. создан еще один перспективный стандарт (строка 9 таблицы 1). Он описывает автоматическое обучение нейронов с многоуровневыми выходными квантователями. Переход к новому типу более сложных нейронов повышает уровень криптографической защищенности искусственного интеллекта и одновременно уровень его мощности. При этом все рекомендации предшествующих стандартов, ранее введенных в действие на территории России, оказываются верны и для нового стандарта. Исключением является только стандарт по тестированию (строка 4 таблицы 1). Этот стандарт придется расширить, в него нужно ввести новую формулу для вычисления сверток Хэмминга по другим модулям. Например, свертка Хэмминга для сети из 256 нейронов с 4-уровневыми квантователями должна вычисляться по формуле:

$$h = 2044 - \sum_{i=1}^{511} \begin{Bmatrix} c_i, & c_{i+1} \\ \oplus & \oplus \\ x_i, & x_{i+1} \end{Bmatrix} \quad (5).$$

Как видно из формулы (5), складываются (по модулю 2) два одинаковых разряда свертываемых кодов, далее суммируются значения полученных пар 511 бинарных кодов.

Необходимость в дальнейшем совершенствовании сетей искусственных нейронов формально обуславливается тем, что длина эквивалентного короткого выходного ключа k должна как минимум удвоиться в сравнении с уже действующим стандартом по автоматическому обучению ГОСТ Р 52633.5-2011. Примерно то же самое утверждение может быть сформулировано не только по отношению к уровню защищенности, но и к уровню мощности следующего поколения отечественного нейросетевого искусственного интеллекта.

Таким образом, можно констатировать утрату безусловного лидерства США в контексте создания искусственного интеллекта в защищенном исполнении начиная с 2006 г., когда в России был введен первый национальный стандарт ГОСТ Р 52633.0-2006, регламентирующий требования к защищенному нейросетевому искусственному интеллекту.

Р. Ф. КУРМАЕВ,
адъюнкт кафедры
организации деятельности ОВД ЦКШУ
(Академия управления МВД России)

Использование данных об участии правозащитных организаций в обеспечении прав и свобод граждан в правоохранительной деятельности органов правопорядка

В соответствии со ст. 2 Конституции РФ человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства.

Это требует от органов государственной власти РФ, включая ОВД, в пределах их компетенции принимать все необходимые меры по защите прав и свобод человека и гражданина. В связи с этим актуален вопрос проработки теоретических, правовых и организационных основ этой деятельности, на что постоянно обращает внимание руководство страны.

Так, на расширенном заседании коллегии МВД России, состоявшемся 28 февраля 2019 г., Президент РФ В. В. Путин обозначил необходимость создания действенного механизма защиты прав, свобод и интересов граждан и одновременно повышения эффективности и «прозрачности» работы правоохранительных органов [1].

В Дорожной карте дальнейшего реформирования органов внутренних дел Российской Федерации отмечено, что для дальнейшего укрепления взаимодействия МВД России с гражданским обществом необходимо создать условия конструктивной работы для правозащитных организаций, заинтересованных в совершенствовании работы ОВД России [2].

Наряду с этим только в 2018 г. в адрес Уполномоченного по правам человека в Российской Федерации поступило 38 698 обращений, из которых 1 728 – коллективные, по вопросам защиты прав и свобод граждан. В общей сложности Уполномоченному по правам человека в Российской Федерации удалось оказать помощь в защите нарушенных прав 184 797 гражданам (включая неопределенный круг лиц) по 929 жалобам из 9 686 принятых к рассмотрению [3].

Кроме того, в настоящее время на разных этапах рассмотрения в Европейском суде по правам человека находится 11 745 дел по жалобам граждан РФ. В 2018 г. Судом всего рассмотрено 248 дел по обращениям российских граждан. В 238 делах из числа указанных признано нарушение прав и свобод граждан. Чаще всего российские власти допускали жестокое и бесчеловечное отношение с гражданами – 99 раз. Столько же раз было нарушено право на свободу и безопасность. Нарушение права на справедливое судебное разбирательство признали 46 раз, 67 – нарушение права на эффективное расследование, 26 – нарушение права

на неприкосновенность частной жизни. При этом, например, в том же периоде по жалобам граждан Германии рассмотрено всего 19 дел, нарушение прав граждан признано лишь в 2 делах [4].

Как правило, граждане взаимодействуют с ОВД России намного чаще, чем с иными органами правопорядка. В большей степени это обусловлено значительной численностью личного состава ОВД России, а также широким кругом вопросов, входящих в их компетенцию. Поэтому защита прав и свобод граждан зачастую связана с предотвращением либо пресечением неправомерных действий или бездействий сотрудников ОВД России.

Длительный период государство выступало единственной формой организации общественной жизни, организуя и направляя всякую социально значимую деятельность людей [5].

Однако в настоящее время результативность деятельности государственных органов РФ, в том числе ОВД, в значительной мере обусловлена взаимодействием с гражданами и общественными организациями.

Особое место в этом процессе занимают правозащитные организации. Перед ОВД стоят задачи по защите прав и свобод человека, решение которых невозможно без создания эффективных форм взаимодействия с общественностью и правозащитными организациями как одним из институтов гражданского общества.

Деятельность ОВД России и правозащитных организаций осуществляется в общем правовом пространстве. Разные по природе, выполняя различные функции, они решают единую задачу – защита прав и свобод человека и гражданина. При этом между ними возникает множество нерешенных вопросов, проблем, что и обуславливает необходимость их сотрудничества.

Надлежащим образом организованное взаимодействие с правозащитными организациями обеспечит результативность работы по защите прав и свобод граждан, взаимный обмен значимой информацией, правовое просвещение населения, повышение правовой культуры самих сотрудников, а также формирование позитивного общественного мнения и повышение авторитета ОВД России.

Однако в настоящее время не разработаны формы и методы взаимодействия ОВД России с правозащитными организациями, отсутствует нормативная правовая база, регламентирующая эту деятельность, не созданы соответствующие организационные структуры. Отдельные меры, предпринимаемые в данном направлении, разрозненны, стихийны и не носят системного характера.

При этом первостепенные проблемы, усложняющие взаимодействие правозащитных организаций с ОВД России, в значительной степени связаны с отсутствием у последних информации, образующейся в результате деятельности правозащитников, либо с недооценкой и зачастую полным игнорированием информации об этой деятельности.

Представляется, что для решения указанных проблем необходимо более широко использовать информационные технологии, а также достижения науки и техники.

Анализ и использование данных об участии правозащитных организаций в обеспечении прав и свобод граждан будет способствовать совершенствованию правозащитной деятельности как самих институтов гражданского общества, так и ОВД России.

Список литературы

1. Сайт Президента РФ. URL: http://kremlin.ru/events/president/news/59913 (дата обращения: 15.12.2019).
2. Дорожная карта дальнейшего реформирования органов внутренних дел Российской Федерации. URL: https://мвд.рф/document/829054 (дата обращения: 17.12.2019).
3. Сайт Уполномоченного по правам человека в Российской Федерации. URL: http://ombudsmanrf.org/content/doclad2018 (дата обращения: 17.12.2019).
4. URL: https://pravo.ru/news/208489 (дата обращения: 17.12.2019).
5. *Кин Д.* Демократия и гражданское общество. М., 2001. С. 56, 57.

В. Н. ЛЕБЕДЕВ,
заместитель начальника кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

Ю. С. КАРПА,
слушатель факультета подготовки
руководителей территориальных органов МВД России
(Академия управления МВД России)

Проблемы правового регулирования применения геоинформационных систем в деятельности ОВД

В настоящее время информационные технологии играют важную роль в жизни современного общества. Они не просто оказывают воздействие на протекающие в обществе экономические и социальные процессы, но и являются катализатором мирового роста экономики, проникая в производственные сферы деятельности и совершенствуя системы управления. Это в конечном итоге способствует увеличению объемов производства товаров и оказания услуг, а также сокращению сроков и повышению качества выполняемых работ. Все это способствует широкому применению разнообразных информационных технологий в различных профессиональных сферах деятельности общества. В последнее десятилетие активно происходит разработка и внедрение информационных технологий в деятельность государственных органов, в том числе и в деятельность ОВД.

Одним из основных классов информационных технологий, используемых сотрудниками ОВД, являются географические информационные (геоинформационные) технологии. Сотрудники правоохранительных органов используют в своей деятельности геоинформационные системы в целях противодействия преступности, обеспечения общественной безопасности, охраны общественного порядка, а также предупреждения и пресечения преступлений.

Несмотря на повсеместное внедрение геоинформационных систем в деятельность ОВД, в настоящее время нормативная регламентация использования данных систем остается на недостаточном уровне.

В соответствии с ГОСТ Р 52438-2005 под геоинформационными системами понимается информационная система, оперирующая пространственными данными. В этом же ГОСТ дается определение информационной системы, под которой следует понимать систему, предназначенную для хранения, обработки, поиска, распространения, передачи и представления информации [1]. Из чего можно сделать вывод, что геоинформационные системы являются разновидностью информационных систем, порядок создания и эксплуатации которых законодательно закреплен в Федеральном законе «Об информации, информационных технологиях

и о защите информации» от 27 июля 2006 г. № 149-ФЗ [2]. Однако геоинформационные системы обладают рядом особенностей, к которым можно отнести: специализированное программное обеспечение, дополнительные технические и аппаратные средства и многое другое. Все это сказывается на процессах внедрения и эксплуатации данных систем. Это, в свою очередь, требует дополнительной нормативной регламентации вопросов разработки и эксплуатации геоинформационных систем как на федеральном уровне, так и на уровне федеральных органов исполнительной власти, в том числе в сфере внутренних дел.

Важное прикладное значение в использовании геоинформационных систем в ОВД имеет их сопряжение со спутниковыми навигационными системами, например, с такой, как ГЛОНАСС. Их сопряжение предоставляет правоохранительным органам дополнительные возможности по эффективному управлению имеющимися в их распоряжении силами и средствами.

На основе сопряжения геоинформационных систем, спутниковых навигационных систем и средств связи формируются навигационные мониторинговые системы. Данные системы функционируют путем установки на транспортное средство бортового комплекта, который осуществляет прием навигационных данных с космических спутников и иной информации от внутренних датчиков (например, видео- и аудиоинформации) и посредством радиоканалов, в основном сотовых сетей связи, осуществляет взаимодействие с центрами мониторинга.

Использование навигационных мониторинговых систем получило широкое распространение в деятельности ОВД, и в настоящее время данные системы используются для решения задач по оперативному реагированию на происшествия, охране общественного порядка, обеспечению безопасности дорожного движения, раскрытию преступлений, осуществлению специализированными подразделениями негласных мероприятий, сопровождению перевозок лиц, подлежащих охране, пассажиров, специальных и опасных грузов, а также перевозок спецконтингента.

Деятельность ОВД по использованию навигационных мониторинговых систем регламентируется приказом МВД России от 31 декабря 2008 г. № 1197 «Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России». В данном приказе изложены основные понятия, касающиеся навигационных мониторинговых систем, а также предъявляемые к данным системам тактико-технические требования [3]. Помимо данного приказа деятельность по использованию глобальной навигационной спутниковой системы, а также навигационная деятельность в целом регламентируется рядом нормативно-правовых актов, в том числе на законодательном уровне. Так, Федеральный закон от 14 февраля 2009 г. № 22-ФЗ «О навигационной деятельности» определяет основные понятия,

касающиеся навигационной деятельности, и регламентирует общественные отношения в сфере навигации [4].

Также деятельность по использованию глобальной навигационной спутниковой системы нормативно закреплена в Указе Президента РФ от 17 мая 2007 г. № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации». В нем указано, что для обеспечения безопасности Российской Федерации аппаратура спутниковой навигации, приобретаемая для нужд федеральных органов исполнительной власти и подведомственных им организаций, должна функционировать с использованием сигналов системы ГЛОНАСС [5].

Во исполнение данного Указа Правительством РФ было принято постановление от 30 апреля 2008 г. № 323 «Об утверждении Положения о полномочиях федеральных органов исполнительной власти по поддержанию, развитию и использованию глобальной навигационной спутниковой системы ГЛОНАСС в интересах обеспечения обороны и безопасности государства, социально-экономического развития Российской Федерации и расширения международного сотрудничества, а также в научных целях». В данном постановлении Правительство РФ возлагает на МВД России полномочия по внедрению систем, функциональных дополнений и аппаратуры спутниковой навигации в интересах обеспечения общественной безопасности, правопорядка, защиты жизни, здоровья, прав и свобод граждан от преступных посягательств; по разработке отраслевых нормативных актов, а также по проведению научно-исследовательских работ для внедрения и использования систем, функциональных дополнений и аппаратуры спутниковой навигации в интересах обеспечения общественной безопасности, правопорядка, защиты жизни, здоровья, прав и свобод граждан от преступных посягательств; обеспечению сертификации аппаратуры спутниковой навигации, предлагаемой для использования МВД России; а также по участию в работах по метрологическому обеспечению аппаратуры спутниковой навигации, применяемой в МВД России [6].

Также Правительство РФ приняло постановление от 25 августа 2008 г. № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS», в соответствии с которым технические средства и системы, специальная техника МВД России подлежат обязательному оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS [7].

В МВД России в целях выполнения вышеуказанного постановления Правительства РФ был издан приказ МВД России от 10 марта 2009 г. № 204 «Об оснащении транспортных средств отдельных подразделений органов внутренних дел Российской Федерации», которым утверждена комплектация аппаратурой спутниковой навигации ГЛОНАСС/GPS патрульных автомобилей строевых подразделений патрульно-постовой службы полиции, вневедомственной охраны, дорожно-патрульной службы, специальных

автомобилей изоляторов временного содержания подозреваемых и обвиняемых, подразделений охраны и конвоирования подозреваемых и обвиняемых [8]; а также приказ МВД России от 26 сентября 2009 г. № 737 «О порядке и этапах оснащения транспортных средств органов внутренних дел Российской Федерации и внутренних войск МВД России аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» [9].

Дополнительно для методического обеспечения сотрудников ОВД в 2009 г. ГУ НПО «СТиС» МВД России были разработаны Методические рекомендации по применению спутниковых навигационно-мониторинговых систем на основе радионавигационной системы ГЛОНАСС в интересах органов внутренних дел [10].

Вышеперечисленные нормативные правовые акты регулируют общественные отношения, возникающие в ходе осуществления навигационной деятельности, что способствует более эффективному внедрению и использованию спутниковых навигационно-мониторинговых систем. Однако применение геоинформационных систем в деятельности правоохранительных органов не ограничивается лишь использованием данных систем совместно со спутниковыми навигационными системами, что диктует необходимость в нормативном правовом регулировании сферы применения геоинформационных технологий как самостоятельной отрасли. Это способствовало бы более эффективному внедрению и использованию современных геоинформационных технологий в деятельности государственных органов в целом и ОВД в частности.

Список литературы

1. Географические информационные системы. Термины и определения. ГОСТ Р 52438-2005 (утв. приказом Ростехрегулирования от 29 декабря 2005 г. № 423-ст).
2. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».
3. Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России: приказ МВД России от 31 декабря 2008 г. № 1197 // СТРАС «Юрист».
4. О навигационной деятельности: федер. закон от 14 февраля 2009 г. № 22-ФЗ // СПС «КонсультантПлюс».
5. Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации: Указ Президента РФ от 17 мая 2007 г. № 638 // СПС «Гарант».
6. Об утверждении Положения о полномочиях федеральных органов исполнительной власти по поддержанию, развитию и использованию глобальной навигационной спутниковой системы ГЛОНАСС в интересах обеспечения обороны и безопасности государства, социально-

экономического развития Российской Федерации и расширения международного сотрудничества, а также в научных целях: постановление Правительства РФ от 30 апреля 2008 г. № 323 // СПС «Гарант».
7. Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS: постановление Правительства РФ от 25 августа 2008 г. № 641 // СПС «Гарант».
8. Об оснащении транспортных средств отдельных подразделений органов внутренних дел Российской Федерации: приказ МВД России от 10 марта 2009 г. № 204 // СТРАС «Юрист».
9. О порядке и этапах оснащения транспортных средств органов внутренних дел Российской Федерации и внутренних войск МВД России аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS: приказ МВД России от 26 сентября 2009 г. № 737 // СТРАС «Юрист».
10. Методические рекомендации по применению спутниковых навигационно-мониторинговых систем на основе радионавигационной системы ГЛОНАСС в интересах органов внутренних дел (2009).

Е. Л. ЛОГИНОВ,
заместитель директора Института экономических стратегий,
доктор экономических наук, профессор РАН,
дважды лауреат премии Правительства РФ
в области науки и техники

Использование технологий Big Data для противодействия массовым беспорядкам в условиях недостатка информации и неопределенности развития ситуации

Введение

Последний период развития нашей страны показал разрастание рисков и угроз, связанных с инициируемыми и поддерживаемыми из-за рубежа, организованными в России антигосударственными проявлениями, в т. ч. массовыми беспорядками и иными действиями различных групп людей, направленными на дестабилизацию обстановки и перехват управления в центре и (или) на местах [2, 11]. В сложившихся условиях считаем необходимым предложить следующие подходы к решению проблемы блокирования наиболее опасных форм таких проявлений со стороны силовых ведомств России на основе использования технологий Big Data [4, 7].

Организационные проблемы противодействия массовым беспорядкам

Недостатком правоохранительной стратегии является то, что при внезапных массовых проявлениях деструктивного характера конкретная задача оперативного (непосредственно в ходе этих беспорядков) выявления их организаторов, в т. ч. латентных, для их нейтрализации перед сотрудниками силовых ведомств не ставится. Предполагается, что это потом будут делать следственные органы на основании показаний задержанных и данных видео- и фотосъемки, если таковые будут в распоряжении правоохранительных органов.

Таким образом, система противодействия со стороны силовых ведомств попыткам перехвата управления прямого характера (майданы, демонстрации), а также косвенного характера (забастовки «дальнобойщиков», волнения мигрантов, выступления футбольных фанатов и пр.) изначально сформирована как ситуационное отставание от активных действий деструктивно настроенных лиц.

Общая система мер противодействия массовым беспорядкам со стороны силовых ведомств не сделала ключевых выводов по перестройке своей деятельности исходя из событий майданов на Украине и пр. Активные меры противодействия массовым беспорядкам со стороны силовых ведомств заведомо медлительны, растянуты во времени и пространстве и предполагают медленное постепенное развитие критических событий

как минимум в течение 3-6 часов, а в реальности это растягивается, особенно в выходные и праздничные дни, до значительно более длительных сроков.

Кроме того, она рассчитана, прежде всего, на противодействие противоправным проявлениям активности сравнительно «мирных» граждан, не подготовленных к вступлению в прямое силовое столкновение с органами правопорядка.

Интеллектуальный видеомониторинг, позволяющий использовать технологии Big Data в режиме реального времени

Необходимо введение обязательного требования наличия на объекте такого-то класса комплексного стандартизированного охранного видеомодуля объекта (с конкретными параметрами), обеспечивающего контроль площади пространства, идентификацию физических лиц и транспортных средств, передачу информации в информационные узлы силовых ведомств в режиме онлайн.

Целесообразно также сформировать пакет аналогичных требований к оборудованию, устанавливаемому в подъездах жилых домов компаниями, оказывающими услуги подключения Интернета, кабельного телевидения и пр.

Фактически основной задачей проекта является формирование и апробация типовой схемы создания и взаимодействия распределенной группы информационных узлов силовых ведомств, получающих, обрабатывающих информацию с камер видеонаблюдения в режиме онлайн (а также возможно от пулов датчиков: радиоактивности, пожарных, звуковых и пр.) и передающих ее или итоговые резюмирующие данные в ситуационные центры органов госуправления [8, 10].

Оперативная деструктуризация агрессивной толпы

Для противодействия успешной деятельности участников массовых беспорядков необходимо формирование компактных небольших групп оперативников силовых ведомств, ориентированных именно на выбивание (в толпе или в малых активных группах деструктивно настроенных лиц) операторов этих групп, состоящих в постоянной связи со скрытыми удаленными руководителями деструктивных действий. Необходимо максимально быстрое устранение явных и латентных операторов, а также публично проявивших себя лидеров толпы с одновременным выявлением действительных (а не подсовываемых) каналов связи и на этой основе установление удаленных мест нахождения реальных управляющих деструктивными действиями лиц для их идентификации и обезвреживания.

Таким образом, эти группы оперативников силовых ведомств должны действовать абсолютно по-другому, автономно от основных сил правопорядка, не защищать стационарные объекты, а выделять лидеров и операторов деструктивной активности толпы, нейтрализовывать их, вытаскивать из толпы не с целью последующего отдаленного во времени расследования, а с целью немедленного, крайне быстрого проведения дознания и выявления у участников массовых беспорядков: центров

управления, концентрации средств связи, денег и оружия. Таких лидеров и операторов деструктивной активности толпы не может быть много: на весь город не более нескольких десятков, а управляющих центров – не более десятка. Рассматриваемые группы оперативников силовых ведомств должны быть нацелены не на доставку выявленных и задержанных лидеров и операторов деструктивной активности толпы по бушующему городу в места допроса (их могут отбить, убить, теряется время, могут быть реализованы меры реакции на задержание, в т. ч. замещения выбитых операторов-лидеров и пр.). Первоначальный допрос необходимо делать на месте, с фиксацией по возможности на видео- и аудионосители и передачей данных в режиме онлайн в аналитический центр соответствующего силового ведомства и только потом по возможности доставлять туда задержанных.

Отработка информационного взаимодействия

Необходимо при этом предусмотреть, что передача от рассматриваемых групп оперативников силовых ведомств информации в аналитический центр соответствующего силового ведомства может быть блокирована, информация может быть подслушана (например, из посольства какой-либо западной страны), передана оттуда атакующим с их ответными мерами. Или, например, центр соответствующего силового ведомства не сможет быстро и эффективно среагировать на полученную информацию от оперативников.

Кроме того, помимо рассматриваемых мобильных групп оперативников силовых ведомств, работающих по операторам и лидерам в привязке к конкретной активности бунтующей толпы в одном или многих местах ее расположения, необходимо предусмотреть наличие групп оперативников силовых ведомств, действующих по заранее разработанному сценарию. Эти группы должны устранять заранее выявленных вероятных лидеров или тех, кто может стать лидером или заместить задержанных органами правопорядка. Таких лиц в любом городе сравнительно немного, не более 200-250 человек, можно и нужно оперативно отслеживать их нахождение, перемещение и контакты в текущий момент и за последние неделю, месяц, три месяца. Средства информационно-вычислительной техники и технологии обработки больших данных позволяют это сделать.

Оперирование мобильной и стационарной связью

Отключение сотовой связи считается одним из основных действий для того, чтобы парализовать управляющую активность бунтующей массы людей. Это правильно, но только в случае, если противоправные проявления активности таких лиц изначально ориентированы на сравнительно мирную конфронтацию с властью. Отключение сотовой связи будет действительно эффективно, если атакующие заранее не предусмотрят альтернативную систему связи между собой и с управляющими центрами противоправных действий. В таком случае система организации противоправных действий

будет продолжать работать и блокировать ее активность имеющимися небольшими силами органов правопорядка будет невозможно.

Целесообразно предусмотреть, что реальные организаторы беспорядков готовились к ним заранее, что у них намечены пути отхода и отработаны методы введения в заблуждение оперативников, осуществляющих мониторинг за их действиями (например, специально передав средства связи – мобильные телефоны, планшеты и пр. – лицам, которые будут отвлекать и вводить в заблуждение оперативников силовых ведомств, осуществляющих мониторинг).

Необходимо выделение операторами сотовой телефонии группы номеров (номерной емкости) по заказу государственных ведомств, которые не отключаются в случае отключения связи и обслуживаются в первую очередь при переполнении сети разговорами и сообщениями. Желательно предусмотреть сервис, при котором при звонке с такого номера на любой другой номер, который в этот момент занят, идущий разговор рассоединяется и происходит подключение приоритетного звонящего. Предлагается предусмотреть кодировку номеров (включая блуждающую кодировку) для исключения подслушивания таких номеров со сканера (т. е. в ходе разговора происходит постоянная автоматическая смена кодировки и сканер утрачивает контроль за разговором).

Предлагаемые меры должны быть дополнены возможностью использования силовыми ведомствами для стационарной и мобильной связи различных информационных сетей общего пользования и ведомственных сетей (гражданских ведомств, предприятий и пр.) для осуществления электронных коммуникаций в режиме онлайн [3]. Это особенно важно в сложных условиях (теракт, массовые беспорядки, стихийное бедствие и пр.), в которых обычные системы связи отключаются, «глючат», а специальные линии связи могут быть отключены по различным причинам.

Методика коррекции поведенческой агрессивности людей в условиях нарастания протестной активности

Для противодействия массовым беспорядкам на основе технологии Big Data:

– реализуется мониторинг релевантности информационных сигналов от различных участников организованных проявлений поведенческой агрессивности для выявления мнений при проявлении их информационной активности в механизмах электронной демократии [12];

– осуществляется кластеризация мнений как формы выражения политических интересов на основе коррелирующих проявлений информационной активности политических агентов в доступном для анализа электронном контенте;

– выявляется семантика связей между агентами в рамках кластеров выявленных проявлений информационной активности [9];

– формируются матрицы вариантов связанности политических интересов в рамках выделенных проявлений информационной активности и взаимосвязей между ними;

– выделяется организационное ядро политических интересов как основы формирования организованных протестных групп;

– производится структурирование ключевых сил в форме сложившихся политических объединений формального и неформального характера, организационно «упаковывающих» политические интересы;

– анализируется структура логических цепочек организационного участия политических агентов в нарастании протестной активности;

– выделяется кластер наиболее активных участников (политических агентов) деструктивных проявлений поведенческой агрессивности. К этому кластеру можно применить агрегирующие или дезагрегирующие методы с использованием модели самоорганизации и распада коллективов и кооперативного поведения людей. Если через анализ данных на основе технологии Big Data о состоянии всех потенциально опасных личностей и их групп применить к ним агрегирующие или дезагрегирующие методы с последующим выпадением 10-15 % наиболее активных членов каждой группы, то выпадение этого сегмента трудно, а иногда и невозможно компенсировать, что резко снижает социальную опасность группы [1].

Заключение

Таким образом, для коррекции поведенческой агрессивности людей в условиях нарастания протестной активности целесообразно обеспечить как можно лучшую наблюдаемость участников политической действительности.

Список литературы

1. *Агеев А. И., Логинов Е. Л.* Нейроменеджмент личности. М., 2019.

2. *Вайднер Е. В., Толмачев А. В.* Социологический анализ методов государственных переворотов // Наука и образование. 2019. № 2. С. 369.

3. *Евсеев В. О.* Моделирование вероятности государственно-политических переворотов и их экономических последствий // ЦИТИСЭ. 2019. № 2. С. 11.

4. *Иванова М. И., Мощенко И. Н.* Анализ групповой протестной активности // Инженерный вестник «Дона». 2015. № 3 (37). С. 78.

5. *Коротаев А. В., Цирель С. В., Билюга С. Э.* Коррупция, ценности и попытки насильственных изменений государственной власти в странах с различным уровнем ВВП на душу населения: опыт количественного компаративного и корреляционного анализа // Сравнительная политика. 2019. Т. 10. № 1. С. 98–123.

6. *Логинов Е. Л., Борталевич С. И., Шкута А. А., Логинова В. Е.* Подходы к использованию модели самоорганизации и распада нейронно-сетевых структур для повышения живучести информационных систем органов государственного управления вследствие природных, техногенных катастроф

или военных атак // Вестник Московского университета МВД России. 2017. № 4. С. 187–194.

7. *Логинов Е. Л., Грабчак Е. П., Григорьев В. В., Райков А. Н., Шкута А. А.* Планирование мер поддержания интерактивной коммуникации информационных систем с учетом угроз возможного коллапса управления экономикой в особый период // Проблемы безопасности и чрезвычайных ситуаций. 2019. № 3. С. 79–86.

8. *Логинов Е. Л., Матвеев А. Г., Шкута А. А.* Определение параметров локализованных состояний неявных групп с собственной компонентой активного поведения, не совпадающего с вектором действий государственной суперсистемы // Искусственные общества. 2019. Т. 14. № 1. С. 5.

9. *Лосева Е. Д., Антамошкин А. Н.* Алгоритм автоматизированного формирования ансамблей нейронных сетей для решения сложных задач интеллектуального анализа данных // Известия Тульского государственного университета. Технические науки. 2017. № 4. С. 234–243.

10. *Манойло А. В.* Концептуальные и организационные основы противодействия цветным революциям в Российской Федерации и на постсоветском пространстве // Мировая политика. 2016. № 1. С. 1–5.

11. *Семченков А. С.* Технологии противодействия внутренним и трансграничным угрозам политической стабильности // Новая наука: от идеи к результату. 2016. № 2–3. С. 53–56.

12. *Фомин В. Н.* Рекуррентное оценивание и адаптивная фильтрация. М., 1984.

В. Ф. МАКАРОВ,
профессор кафедры прикладной информатики,
доктор технических наук, профессор
(Московский гуманитарный университет)

Д. Ю. НЕЧАЕВ,
заведующий кафедрой прикладной информатики,
кандидат технических наук, доцент
(Московский гуманитарный университет)

Методика ортогонального кодирования в сетевых компьютерных технологиях

На применение ортогональных кодов как одного из наиболее эффективных методов повышения достоверности обработки информации было указано в работах академика В. А. Котельникова. Основным достоинством методов помехоустойчивого кодирования является обнаружение и исправление ошибок, возникающих за счет воздействия помех в кодовых комбинациях. Эта возможность обнаружения и исправления ошибок достигается за счет введения избыточности при построении кодовых таблиц. Причем ошибки могут обнаруживаться и исправляться только лишь в пределах, ограниченных корректирующей способностью кода.

Одним из методов уплотнения и разделения канальных сигналов и отдельных элементов ортогональных кодов, позволяющих не только устранять избыточность, но и обеспечивать высокую достоверность обработки информации, является применение ортогональных кодов с последующей обработкой их приемными корреляционными устройствами. По своей структуре такие сигналы относятся к сложным составным сигналам, база которых много больше единицы ($B=F_{max}*T>>1$, где: F_{max} – максимальная частота в спектре передаваемого сигнала, T – период сигнала) и которые являются разновидностью шумоподобных сигналов.

При построении систем теледоступа к вычислительным ресурсам, использующим ортогональные коды, математическими элементами которых являются множества различных ортогональных кусочно-постоянных или непрерывных ортогональных функций или полиномов, необходимо создать базис первообразных ортогональных функций или полиномов. Известно, что при построении многоканальных систем передачи данных с уплотнением и разделением канальных сигналов по форме применяются различные ортогональные кодовые последовательности, построенные на основе ортогональных функций или полиномов Лежандра, Чебышева, Лагерра, Эрмита, Якоби, Бесселя, Гегенбауэра, Радемахера, Хаара, Уолша. Из всех перечисленных функций и полиномов необходимо выбрать только те,

которые наиболее эффективны для образования канальных сигналов или отдельных элементов кодовых комбинаций.

Так, полиномы Лагерра и Эрмита ортогональны на интервале -∞ … +∞ и 0 …+∞, и ограничение периода передачи сообщений связано с нарушением ортогональности, а следовательно, и с появлением взаимовлияния канальных сигналов.

Функции Гегенбауэра и Якоби удовлетворяют условию конечных пределов ортогональности, но их техническая реализация связана со значительными сложностями. Функции Бесселя первого и второго родов не полностью ортогональны, и их применение также связано с появлением ошибок за счет взаимовлияния.

Наиболее приемлемыми функциями в качестве сигналообразующих являются ортогональные полиномы Чебышева и Лежандра и ортогональные функции Радемахера и Уолша. Однако техническая и программная реализация сигналов, математическими моделями которых являются ортогональные полиномы Чебышева и Лежандра, также затруднительна из-за применения в передающих и приемных устройствах сложных аналоговых устройств умножения.

Наиболее приемлемыми для построения ортогональных сигналов и ортогональных кодов являются ортогональные функции Радемахера и Уолша. Однако при выборе тех или иных ортогональных функций и полиномов в качестве математических моделей ортогональных сигналов и ортогональных кодов при построении систем теледоступа к вычислительным ресурсам необходимо руководствоваться не только степенью сложности их реализации, но также и степенью подверженности таких сигналов различному виду помех, несанкционированному восприятию и распознаванию.

Внешними возмущающими воздействиями являются импульсные и флуктуационные помехи, помехи типа «пакет», помехи, сосредоточенные по спектру или по времени. Наиболее устойчивыми сигналами к воздействию помех будут такие сигналы, у которых степень соответствия с помехами будет минимальной. Так, для случая импульсных помех, преобладающих в каналах теледоступа, такую оценку можно производить по коэффициентам аппроксимации реакции линии связи на ударные возбуждения от импульсных помех. В этом случае реакция линии связи на ударное возбуждение может быть выражена линейной комбинацией взаимно ортогональных функций, если последние образуют полный базис.

Для тех функций, у которых при одинаковом числе членов суммы аппроксимирующего ряда коэффициенты аппроксимации будут минимальными, соответствие между функциями, описывающими информационные сигналы и помехи, также будет минимальным. Следовательно, и сигналы, описываемые этими ортогональными функциями, будут наиболее устойчивыми к разрушающему воздействию помех.

$$\beta = \frac{\int_0^T U_{\text{п}}(t) * U_{\text{с}}(t)dt}{\int_o^T U_{\text{с}}^2(t)dt} \quad (1),$$

где: $U_п(t)$ – система ортогональных функций, описывающих помеху; $U_с(t)$ – система ортогональных функций, описывающих полезный сигнал.

Анализ существующих методов организации системы теледоступа к вычислительным ресурсам показал, что они используют в основном временное уплотнение и разделение канальных сигналов, которое по достоверности проигрывает иным способам многоканальной передачи данных. В этом плане наиболее перспективной является организация теледоступа с уплотнением и разделением канальных сигналов по форме, в которой в качестве канальных сигналов используются ортогональные коды, построенные на основе ортогональных функций Уолша, в совокупности с оптимальной обработкой их в приемных корреляционных устройствах.

В рассматриваемой системе для построения канальных кодообразующих сигналов используется обобщенная полная система ортогональных кусочно-постоянных функций Уолша. Такой подход требует новых качественных изменений в построении общей теории связи, основанной на синусно-косинусных функциях и цифровых методах обработки информации. В этом случае описание методов обработки сигналов происходит не в частотно-временной плоскости, а в функционально-временной плоскости.

Любая последовательность ортогональных сигналов, построенных на полной системе ортогональных функций, занимает конечную часть функционально-временной плоскости.

Под полной ортонормированной системой функций понимается такая система, в которой для любой функции $F_i(t)$ предел квадратично интегрируемой разности устремляется к нулю. Для такой системы неравенство Бесселя $\sum_{k=1}^{\infty} F_m^2 \le \|a\|^2$ в предельном переходе обращается в равенство Парсеваля. Подобное представление позволяет оценивать в физическом смысле энергию несинусоидальных колебаний как сумму энергий отдельных спектральных составляющих:

$$\int_0^T F^2(t)\,dt = \sum_{k=1}^{\infty} (a_k^2 + b_k^2) \quad (2).$$

Такой подход позволяет вычислять значения сигналов на выходах отдельных корреляционных устройств многоканальных систем передачи данных с разделением каналов по форме, канальные сигналы которых построены на основе несинусоидальных сложных составных ортогональных функций или полиномов.

Построение каналообразующей аппаратуры компьютеризированных комплексов, защита преобразуемых и передаваемых данных с использованием в качестве элементов кодовых комбинаций ортогональных сигналов, построенных на основе множеств ортогональных функций или полиномов, до настоящего времени не получило широкого распространения из-за относительно малой степени изученности по сравнению с классическими методами обработки данных.

В данной статье рассматриваются вопросы организации системы передачи и защиты данных в компьютерных технологиях с использованием методов уплотнения и разделения элементов кодовых комбинаций по форме, математическими моделями которых являются ортогональные функции Уолша, относящиеся ко множеству ортонормированных кусочно-постоянных ортогональных функций.

Следует отметить, что система {f(j, x)} действительных и ненулевых функций называется ортогональной на конечном интервале $x_0 \le x \le x_1$, если выполняются следующие условия:

$$\int_{x_0}^{x_1} f(j,x)\cdot f(k,x) = x_j \cdot \delta_{jk}, \quad \delta_{jk} = \begin{cases} 1, & j = k \\ 0, & j \neq k \end{cases} \tag{3}$$

Эти условия ортогональности определены в метрике гильбертова пространства. В евклидовом пространстве условие ортогональности определяется как:

$f(j, x)$ x $f(k, x) = f(j, x) \cdot f(k, x) \cdot \cos\varphi = x_j \delta_{jk}$

$$\delta_{jk} = \begin{cases} 1, \varphi = 0^{\circ} \\ 0, \varphi = 90^{\circ} \end{cases} \tag{4}$$

Из выражений (3, 4) следует, что векторы, описывающие элементы сигналов или кодовых комбинаций, являются ортогональными, если их скалярное произведение равно 1 в случае полного их совпадения и 0 в противном случае.

В исследованиях, проведенных Уолшем, показана возможность формирования полной системы ортогональных кусочно-постоянных функций на основе базисных ортогональных функций Радемахера, являющихся подмножеством полного кусочно-постоянного множества ортогональных функций Уолша.

В такой системе базовыми ортогональными функциями Радемахера являются функции вида $M_r \Rightarrow \{Y_1, Y_2, Y_4, Y_8, Y_{16}, \ldots Y_{2^n}\}$. Полная система ортогональных функций Уолша формируется из базисной ортонормированной системы кусочно-постоянных функций Радемахера путем их алгебраического перемножения, например из ортогональных функций Радемахера Y_1 и Y_2 функция Уолша Y_3 определится как $Y_3 = Y_1 * Y_2$. Каждые последующие производные функции Уолша образуются согласно алгоритму: $Y_5 = Y_1 * Y_4$; $Y_6 = Y_2 * Y_4$; $Y_7 = Y_1 * Y_2 * Y_4$; $Y_9 = Y_1 * Y_8$; … $Y_{15} = Y_1 * Y_2 * Y_4 * Y_8$ (5).

При определении необходимого и достаточного числа ортогональных функций Уолша для построения отдельных элементов ортогональных кодов в системах защиты и передачи данных необходимо выявить максимальный нижний предел номера базисной функции Радемахера sup K_j. После чего определяются и сами базисные функции выбранного подмножества, из которых на основе перемножения формируется полная система ортогонального подмножества Уолша. Порядковый номер каждой такой функции определяется в соответствии со следующей формулой:

$$m = \sup K_j + \sum_{j=1}^{2^{n-1}} K_j \qquad (6),$$

где: m – порядковый номер производной функции Уолша;

K_j – номера базисных образующих функций Радемахера.

В свою очередь, порядковый номер производной функции Уолша определяет ее структурный состав, т. е. подмножество образующих функций Радемахера.

В общем виде алгоритм образования сигналообразующих кусочно-постоянных ортогональных функций Уолша определится как

$$Y_m = Y_{\sup Kj} * \prod_{j=1}^{2^n} Y k_j \{ \forall Y_m, \sup K_j + \sum_{j=1}^{2^n} K_j \} \qquad (7).$$

В соответствии с формулой (3) на рис. 1 представлен фрагмент множества ортогональных кусочно-постоянных ортонормированных функций Уолша для построения кодовых ортогональных комбинаций, состоящих из 64 элементов ортогональных кодов, отображенных в кусочно-постоянном ортогональном множестве Уолша.

Y1=-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+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+1+1+1+1+1+1+1
Y2=-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+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+1+1+1+1+1+1
…….
Y62=-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-
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
Y63=+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-
1-1+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

Рис. 1. Фрагмент 63 ортогональных функций Уолша в двоичной форме

Необходимо отметить, что эта система отличается от классической системы ортогональных функций Уолша. Автору статьи удалось получить модернизированное множество кусочно-постоянных функций Уолша в том отображении, при котором все сложные составные элементы отдельных функций Уолша строго фазированы, т. е. начинаются с одной фазы, что имеет существенное значение как при технической, так и программной реализации полной совокупности кодовых ортогональных сигналов

в системах теледоступа к вычислительным ресурсам. Это преимущество определяется, прежде всего, тем, что не требуется введение специальных блоков распознавания начальной фазы как отдельных канальных сигналов, так и сложного составного суммарного сигнала, форма которого будет определять текущее состояние параллельного интерфейса вычислительного комплекса.

Как видно из рис. 1, полная система ортогональных функций Уолша состоит из четных и нечетных функций, принимающих на всем периоде значения «+1» или «–1». Однако при этом необходимо осуществить проверку полученных ортогональных функций на отсутствие нарушения их ортогональности. Проверка полученных и построенных функций Уолша показывает, что, какая бы комбинация ни была взята, условие ортогональности полностью сохраняется. Последнее утверждение позволяет сохранить сепарабельность построенного множества, а следовательно, осуществить распознавание и выделение каждого элемента приведенного множества кусочно-постоянных ортогональных функций.

Пример отображения образования подмножества Уолша из базисных функций Радемахера представлен в виде графа (рис. 2), на котором прослеживается алгоритм формирования производных функций на основе базисных функций Радемахера (для случая Y_1; Y_2; Y_4; Y_8), причем необходимо отметить, что номер каждой производной функции Уолша определяется суммой номеров функций Радемахера, входящих в рассматриваемый узел.

Преобразованный граф характерен тем, что каждая последующая функция образуется в результате перемножения одной из базовых и производных функций или двух базовых функций, т. е. в этом случае каждый узел графа имеет только два входа. Полученное условие является весьма важным при технической реализации генератора ортогональных колебаний, т. к. в этом случае его построение ориентировано на применение двухвходовых схем совпадения в устройствах умножения ортогональных сигналов.

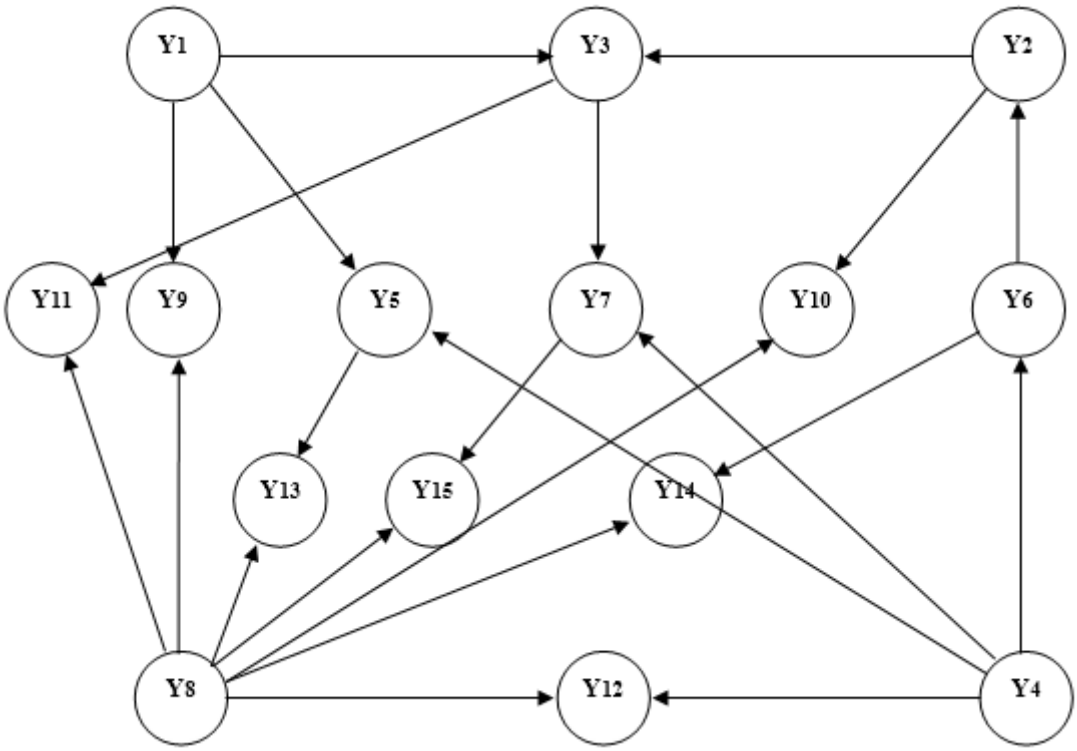

Рис. 2. Пример преобразованного графа

Последнее преобразование также важно и при программной реализации генератора ортогональных колебаний, математическими моделями которых является множество кусочно-постоянных ортогональных функций Уолша, т. к. в этом случае производится поэлементное умножение только лишь двух функций, что резко сокращает время формирования разрешенного ортогонального множества кодовых элементов.

При последовательном построении множества ортонормированных функций Уолша каждая последующая функция строится по алгоритму:

1) строятся две первые ортогональные функции Радемахера Y_1 и Y_2;

2) путем поэлементного их перемножения определяется и строится функция Y_3;

3) вводится еще одна функция Радемахера Y_4;

4) путем поэлементного перемножения функций $Y_{1\,и}\,Y_4$, $Y_{2\,и}\,Y_4$, Y_3 и Y_4 строятся функции Y_5, Y_6, Y_7.

Этот процесс дополнения множества Уолша продолжается до получения необходимого количества ортонормированных функций для построения множества кодообразующих ортогональных сигналов или элементов ортонормированного кода Уолша.

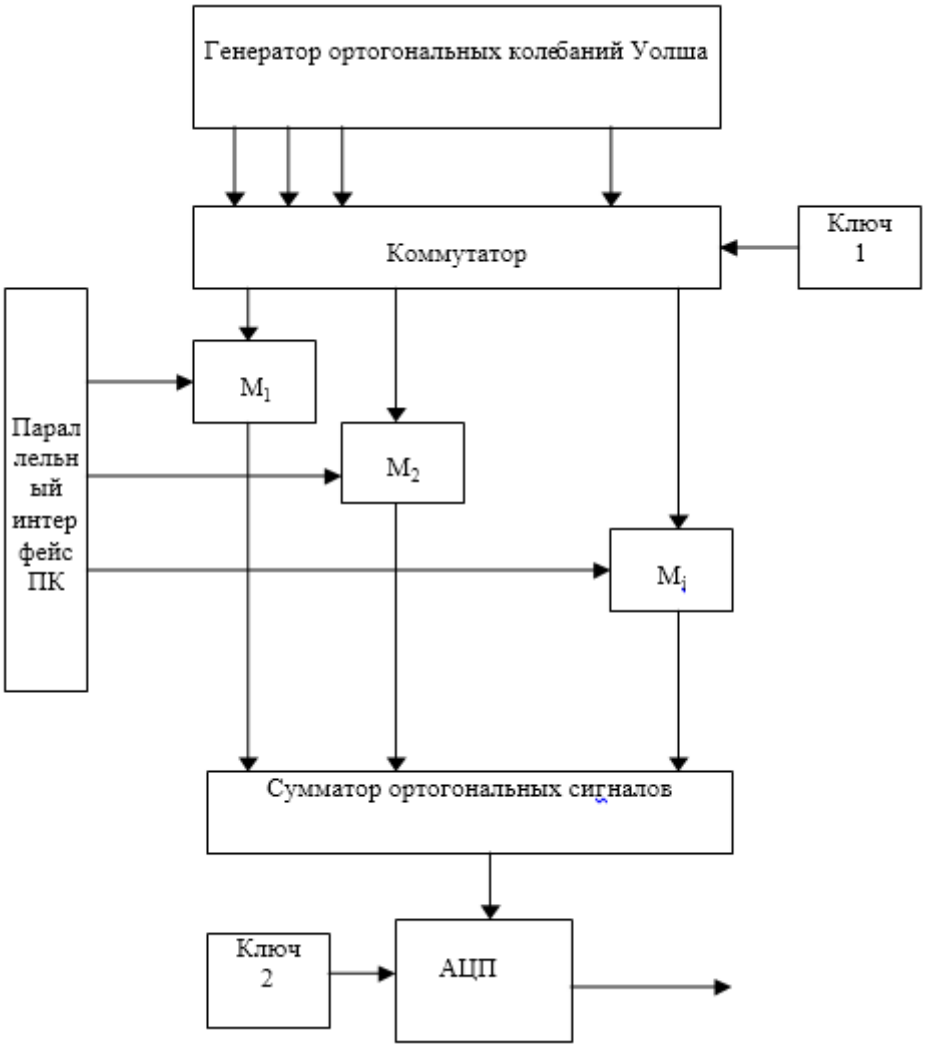

Рис. 3. Структурная схема системы ортогонального кодирования

Производится временное закрепление элементов выбранного ортогонального множества за элементами байта Windows-кода в соответствии с таблицей кодирования, представленной $Y_k \rightarrow W_k$.

Такое закрепление динамично и может изменяться при каждом сеансе передачи данных. В силу того, что ортогональные сигналы, являющиеся моделями ортогональных функций Уолша, параллельны во времени, возможна передача не последовательности битов Windows-кода, а сложного составного многоуровневого суммарного сигнала, состоящего из множества ортогональных сигналов Уолша и отображающего состояние параллельного интерфейса вычислительного комплекса в едином временном интервале – Т.

Последнее дает возможность формирования на кодирующем устройстве сложного составного многоуровневого сигнала, несущего информацию о кванте передаваемых данных. Таким семантическим квантом может быть не один, а несколько символов естественного алфавита. В рассматриваемом примере таким семантическим квантом является слово, часть слова, фраза, состоящие из семи семантических элементов (букв). Для отображения любой семизначной комбинации естественных символов

кириллицы, цифрового алфавита и знаков пунктуации, интерпретируемых в Windows-кодах, потребуется порядка 64 ортогональных сигналов Уолша.

Причем изначально любые восемь функций Уолша закрепляются за разрядами восьмиэлементного Windows-кода, отображающими первый символ естественного алфавита, затем из оставшихся ортогональных сигналов восемь закрепляются за разрядами второго символа кодируемого текста и т. д. В результате такого преобразования все семь символов кодируемого текста отображаются на множестве ортогональных функций Уолша

$$\forall x_i \in X \rightarrow \{a_w\}|8 \rightarrow \{y_i \in Y\}|64 \quad (8).$$

Такое отображение производится с помощью оператора преобразования, устанавливающего правила соответствия между элементами Windows-кодов и элементами множества ортогональных функций Уолша.

После установления соответствия между множеством элементов байта Windows-кода, отображающих семантический символ естественного алфавита, и множеством ортогональных сигналов Уолша по графику соответствий, который определяется задаваемой и динамически изменяемой таблицей преобразований, производится суммирование выбранных ортогональных сигналов. В результате такого преобразования формируется сложный составной суммарный многоуровневый сигнал, отображающий в текущий момент времени состояние параллельного интерфейса вычислительного комплекса. Структурная схема системы ортогонального кодирования представлена на рис. 3.

На рис. 4 отображен сложный составной многоуровневый суммарный сигнал слова «Криптон», состоящий из 56 ортогональных сигналов Уолша ($Y_1 \ldots Y_{56}$).

Следующим шагом преобразования параллельного Windows-кода является отображение сложного составного многоуровневого сигнала выбранного ортогонального множества в двоичном коде. Для этого формируется динамическая таблица преобразования, устанавливающая соответствие между отдельными уровнями суммарного многоуровневого сигнала и множеством двоичных кодовых комбинаций.

В случае выбранного разрешенного ортогонального множества Уолша количество уровней суммарного сигнала, отображающего состояние параллельного интерфейса вычислительного комплекса, на рассматриваемом примере составит 64 кванта. Причем график установления соответствий между кодовыми комбинациями и квантованными уровнями сложного составного суммарного сигнала задается программным методом или устанавливается самим пользователем.

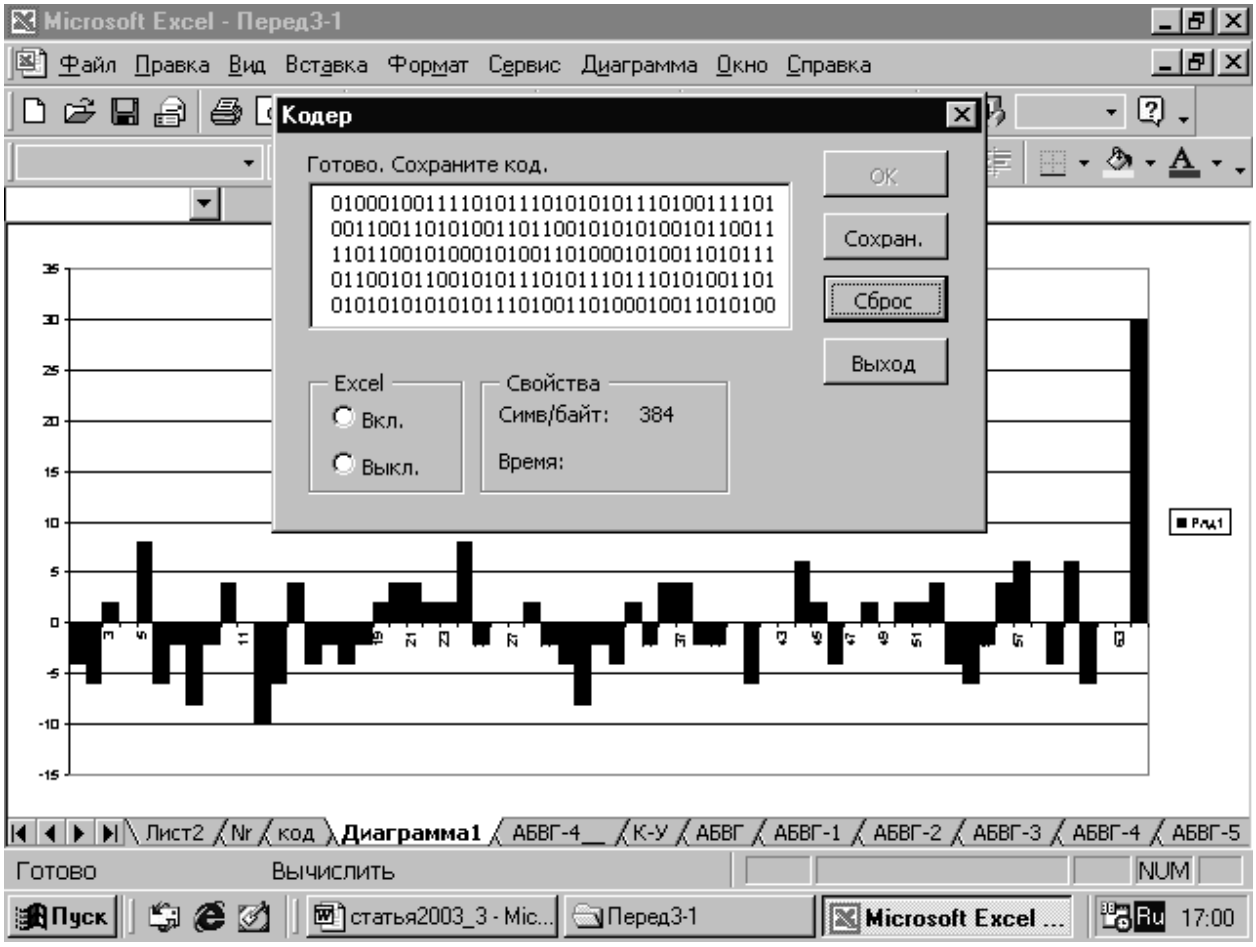

Рис. 4. Отображение слова «Криптон» сложным составным многоуровневым сигналом, состоящим из 56 ортогональных сигналов Уолша

Список литературы

1. *Качмаж С., Штейнгауз Г.* Теория ортогональных рядов. М., 1958.
2. *Макаров В. Ф. и др.* Математические основы защиты информации: учебник. Орел, 2016.
3. *Макаров В. Ф.* Проблемы комплексной защиты информации // Безопасность информационных технологий. М., 1994.
4. *Макаров В. Ф.* Обеспечение защиты информации на основе ортогональных преобразований // Безопасность информационных технологий. М., 2000.

И. П. МОЖАЕВА,
главный научный сотрудник отдела по исследованию проблем отраслевого управления научно-исследовательского центра, доктор юридических наук
(Академия управления МВД России)

Современные цифровые технологии оптимизации документооборота в деятельности ОВД

Документооборот является непременным атрибутом любой предметной деятельности, в том числе правоохранительной. Без него невозможна реализация управленческих функций как на стадии выработки и принятия управленческих решений, так в ходе их исполнения.

Комплексное изучение состояния документооборота в ОВД, выработка предложений по его совершенствованию на основе научных знаний в области теории организации правоохранительной деятельности, теории научной организации труда, как представляется, будут способствовать формированию организационно-правового и научно-методического механизмов оптимизации документооборота в деятельности ОВД. В настоящее время проведена целенаправленная системная работа и принят комплекс мер по оптимизации документооборота в системе МВД России. Усилия Министерства направлены на совершенствование правового, организационного, технического, методического и иного обеспечения делопроизводства.

Одним из актуальных направлений оптимизации документооборота в деятельности ОВД является внедрение современных цифровых технологий. В современных условиях цифровизации общества вопрос о необходимости автоматизации управления документооборотом уже перешел в практическую плоскость, и все больше российских организаций и государственных учреждений внедряют у себя системы электронного документооборота, позволяя на собственном опыте оценить преимущества новой технологии работы с документами.

Необходимость в автоматизации управления документооборотом разные специалисты сегодня видят по-разному: одни – в повышении эффективности организационно-распорядительного документооборота, другие – в повышении эффективности работы функциональных специалистов, создающих документы и использующих их в повседневной работе, и лишь немногие уделяют внимание обоим аспектам[25].

[25] *Куняев Н. Н.* Конфиденциальное делопроизводство и защищенный электронный документооборот / А. С. Демушкин, А. Г. Фабричнов. М., 2011; *Старостенко И. Н., Шарпан М. В.* Об организации электронного документооборота в органах внутренних дел // Вестник Краснодарского университета МВД России. 2013. № 2 (20).

Для подразделений ОВД, где количество документов и сложность их ведения значительны, становится первостепенной задача автоматизации документооборота с целью устранения данных недостатков.

Анализ деятельности территориальных органов МВД России свидетельствует об увеличивающемся документопотоке, тенденциях роста доли входящих документов, снижения доли исходящих, при одновременном росте их общего числа»[26]. При этом в территориальных органах МВД России на региональном уровне доля исходящих документов (51,1 %) существенно выше доли входящих документов (40,4 %). Одновременно отмечается значительная разница между долями документов, поступающих от федеральных органов государственной власти, не входящих в систему МВД России (33,2 %), и исходящих документов в их адрес (47,4 %) в органах и организациях, подчиненных территориальным органам МВД России на региональном уровне, что, по нашему мнению, требует дополнительного изучения.

Одним из наиболее востребованных сервисов единой системы информационно-аналитического обеспечения деятельности МВД России является сервис электронного документооборота (СЭД, Сервис).

В настоящее время действующими отчетами по делопроизводству, утвержденными приказом МВД России от 30 июня 2016 г. № 360 «О порядке организации работы по представлению органами, подразделениями и организациями системы МВД России сведений по вопросам делопроизводства, рассмотрения обращений граждан и организаций, состояния защиты государственной тайны», не предусмотрен сбор информации о количестве сотрудников МВД России, которым при исполнении служебных обязанностей необходим доступ к СЭД. Вместе с тем в 2013 и 2015 гг. в соответствии с указаниями руководства МВД России такие данные запрашивались отдельно. Их обобщение показало необходимость доступа к СЭД на постоянной основе порядка 450 тыс. сотрудников ОВД[27].

В ИСОД МВД России функционирует порядка 10 сервисов, накапливающих информацию по направлениям деятельности различных подразделений МВД России. При создании условий, позволяющих территориальным органам МВД России вносить данные в эти сервисы, возможна отмена ряда периодических отчетов.

Однако, как показывает анализ результатов проверок УМВД России по Калужской области, по Тверской области[28], иных органов и подразделений

---

[26] Информация, предоставленная ДДО МВД России в рамках подготовки к рассмотрению на заседании коллегии МВД России вопроса «О состоянии и мерах по совершенствованию и развитию информационных систем обеспечения деятельности территориальных органов МВД России» (исх. № 2/10132 от 01.09.2018, № 2/10722 от 10.09.2018).

[27] *Там же.*

[28] В УМВД России по Тверской области за полгода не воспользовались СЭД более половины (58,6 %) пользователей, имеющих учетные записи ИСОД МВД России.

МВД России, а также сведений о состоянии документооборота в МВД по республикам, ГУ (У) МВД России по иным субъектам РФ в период с 2012 по 2017 гг. [29], возможности ИСОД, СЭД, специализированных информационных баз данных (СИБД), баз данных ГИАЦ МВД России и ИЦ территориальных органов, а также шифроргана используются не в полном объеме и (или) не по назначению. Помимо отсутствия контроля их использование во многом осложняется узким назначением, (или) неудобным программным обеспечением, (или) недостаточной унификацией.

В целях реализации требований распоряжения МВД России от 9 ноября 2015 г. № 1/9112 «О мерах по переходу на электронный документооборот» необходимо изменить подход к формированию делопроизводства в подразделениях. В целях обеспечения использования возможностей ИСОД МВД России необходимо реализовать комплекс мероприятий, способствующих максимальному вовлечению существующих информационных массивов ИСОД МВД России в процесс организации и осуществления управленческой деятельности органов и подразделений МВД России.

Проблема дальнейшего совершенствования сервиса электронного документооборота (СЭД). Как показал анализ, в настоящее время документопотоки информационного, справочного характера (то есть докладные записки, рапорты, справки об исполнении и т. п.), направленные посредством СЭД и учтенные в различных провайдерах за новыми номерами, можно было бы оптимизировать за счет дальнейшей доработки СЭД.

Целесообразно использовать единый порядок учета информационной документации за одним регистрационным номером (сквозная нумерация для разных провайдеров), если информация поступает из нескольких структурных подразделений во исполнение одного и того же управленческого решения, оформленного одним документом. Реализовать это возможно по аналогии с алгоритмом учета (за единым регистрационным номером) всей документации при организации работы с обращениями граждан.

Использование СЭД должно позволить осуществлять автоматическую выгрузку статистических данных о документообороте [30]. Сервис в целом позволяет решать основные задачи, стоящие перед подразделениями делопроизводства, включая вопросы оперативного доведения решений руководства МВД России до исполнителей.

Из 593 действующих электронных подписей активировано всего 374 (63 %). Не более 20 % пользователей подготавливают, согласовывают и подписывают исходящие документы в электронном виде. Как следствие, основная часть корреспонденции подписывается на бумаге и регистрируется в СЭД делопроизводителями.

[29] Докладная записка заместителя Министра внутренних дел Российской Федерации генерал-полковника полиции А. А. Гостева от 27 апреля 2017 г. № 5/5-960 (п. 1).

[30] В настоящее время отчеты по делопроизводству, предусмотренные приказом МВД России от 30 июня 2016 г. № 360, подготавливаются путем обычных подсчетов документов с творческой интерпретацией их дифференциации, что приводит к умышленному «улучшению» показателей.

Резюмируя изложенное, следует подчеркнуть, что в условиях оптимизации МВД России, происходящих организационно-структурных преобразований, развития информационной инфраструктуры ОВД на основе современных инновационных подходов целесообразно продолжать совершенствование документооборота на основе системного подхода.

Институт документационного обеспечения управления в системе МВД России, постоянно развиваясь и совершенствуясь, в целом выполняет свое предназначение. Он позволяет получать необходимую информацию о происходящих процессах, соответствии функционирования системы МВД России заданным целям и поставленным задачам, производить оценку результатов воздействия субъекта на объекты управления, выявлять отклонения от заданных параметров, своевременно устранять обнаруженные недостатки. Вместе с тем изучение практики документационного обеспечения управления позволило выявить ряд существенных недостатков в этой сфере и одновременно показало наличие неиспользованных резервов и возможностей. Причины такого положения разные – как субъективного, так и объективного плана. Так, например, документационное обеспечение управленческой деятельности в правоохранительной сфере должно осуществляться по установленным правилам, заложенным в государственных стандартах, в соответствующих нормативах и методиках. А это в определенной степени ограничивает «простор для маневра», поскольку не учитывает правоохранительной специфики.

В связи с этим представляется актуальным дальнейшее познание обозначенных в научной статье рекомендаций и предложений по оптимизации документооборота в системе МВД России и их возможное внедрение в организационную деятельность.

А. В. МОРОЗОВ,
заместитель начальника управления,
кандидат юридических наук
(ГУНК МВД России)

О. В. ШУЛЬЖЕНКО,
начальник отдела
(УНК ГУ МВД России по Краснодарскому краю)

О некоторых вопросах борьбы с незаконным оборотом новых синтетических наркотических средств и психотропных веществ

«Наркобизнес, превратившийся в одну из наиболее агрессивных форм транснациональной преступности, представляет реальную опасность для государства и общества, уносит жизни и разрушает здоровье миллионов людей. Доходы наркокартелей также служат источником финансирования террористических и экстремистских группировок»[31].

Проводимый Главным управлением наркоконтроля МВД России [32] анализ наркоситуации показывает, что на протяжении последних лет наркорынок в России претерпевает серьезные изменения.

1. С 2016 г. отмечается устойчивая тенденция снижения изъятия героина (на 85 %, с 3 226,8 кг до 499,8 кг), причем не только в транзитных регионах, но и в так называемых «ямах». Так, в период с 2016 по 2018 г. в Пермском крае изъятия героина снизились на 83 % (с 45,2 кг до 7,9 кг), в Московской области – 90 % (с 1 055,7 кг до 108,1 кг), в Санкт-Петербурге и Ленинградской области – 61 % (с 112,7 кг до 44,4 кг), в Свердловской области – 88 % (с 55,1 кг до 6,8 кг), в Новосибирской области – 81 % (с 158,5 кг до 17,3 кг), в Омской области – 85 % (с 35 кг до 5,4 кг), в Челябинской области – 76 % (с 95,1 кг до 22,8 кг).

Кроме того, прослеживается снижение числа больных с диагнозом опийная наркомания, состоящих на учете. 230 576 человек состояли на таком учете в 2015 г., 203 621 – в 2016 г., 178 008 – в 2017 г., 152 059 – в 2018 г.

Однако по итогам 2018 г. отмечается незначительная тенденция прироста изъятий наркотических средств. Так, всеми правоохранительными органами из незаконного оборота изъято 1 161,511 кг наркотических средств опийной группы (АППГ – 18,4), из которых 721,733 кг героина (АППГ – 44,4 %).

---

[31] Из обращения Президента России В. В. Путина к участникам Специальной сессии Генеральной Ассамблеи ООН по мировой проблеме наркотиков 2016 г.
[32] Далее – ГУНК.

Вместе с тем удельный вес «синтетики» в общей массе изымаемых наркотических средств и психотропных веществ на протяжении последних нескольких лет увеличился в 7 раз и по итогам 2018 г. составил 4,2 т.

Наибольшее количество наркотических средств синтетического происхождения изымается в крупных регионах России: в Московской, Новосибирской, Тюменской, Челябинской, Самарской областях, республиках Татарстан и Башкортостан, а также в г. Москве.

Наиболее распространенными в незаконном обороте синтетических наркотиков являются стимуляторы амфетаминового ряда, в том числе метамфетамин и МДМА, N-метилэфедрон и мефедрон и их производные, в том числе α-PVP, наркотические средства фентаниловой группы, синтетические аналоги тетрагидроканнабинола (курительные смеси).

2. Особую озабоченность вызывают участившиеся случаи изъятия из незаконного оборота карфентанила. Фиксируются высокие темпы и постепенное расширение масштабов его распространения.

Так, если в период с июня по декабрь 2017 г. выявлены 64 факта изъятия карфентанила в 5 федеральных округах РФ (15 субъектов), то за 2018 г. зафиксировано 526 фактов его изъятия уже в 7 федеральных округах (27 субъектов).

О востребованности психостимулятора среди наркопотребителей свидетельствует увеличение массы изымаемого наркотика. За 2017 г. изъято 12,8 кг карфентанила, в то же время за 2018 г. – свыше 29,3 кг наркотика.

Учитывая внешнюю схожесть карфентанила с героином и его относительно низкую стоимость за счет высокой концентрации, он реализуется на наркорынке чаще всего в смеси с героином, метадоном, различными наполнителями, фармакологическими добавками и примесями. Нередко представляется как «синтетический героин», поскольку копирует его наркогенные эффекты.

Воздействие вещества на организм человека начинается уже с 1 микрограмма, что определяет его повышенную опасность. Употребление карфентаниловой смеси в соразмерном героину количестве приводит к летальным исходам.

Кроме того, в ходе анализа наркоситуации в 2018 г. помимо фактов изъятия 3-метилфентанила и карфентанила выявлены факты распространения новых видов фентаниловых наркотиков – фуранил-фентанила (Ивановская область), кротонилфентанила, ацетилфентанила (Новосибирская область).

По имеющимся сведениям, карфентанил поступает в Россию из прибалтийских стран, КНР (в том числе Гонконга). Экспорт карфентанила осуществляется из Китая в США, Канаду, Великобританию, Францию, Германию, Бельгию, Австралию, Россию посредством почтовых отправлений.

Основными фигурантами незаконного оборота карфентанила являются цыганские этнические преступные группы, созданные по родственному признаку и имеющие преступные связи за рубежом.

ГУНК в целях пресечения распространения карфентанила на территории РФ в УНК (УКОН) МВД России по республикам, ГУ (У) МВД России по иным субъектам РФ направлено информационное письмо о динамике незаконного оборота карфентанила, а также указание об активизации работы по выявлению каналов поставок наркотиков фентанилового ряда (в том числе карфентанила) и их прекурсоров, в ЭКЦ МВД России направлено письмо о направлении в территориальные органы МВД России методики определения наркотических средств фентанилового ряда.

На международных площадках сотрудники ГУНК выступают за внесение карфентанила и других наркотиков фентаниловой группы в списки контролируемых веществ в соответствии с антинаркотической Конвенцией ООН 1961 г.

3. Одним из основных источников поступления в Россию синтетических наркотиков является их контрабанда из-за рубежа. «Синтетика» в Россию поступает из Китая, Бельгии, Германии, Польши, Литвы, Голландии, Чехии, Словакии, Украины. Пути их доставки проходят через Эстонию, Латвию, Беларусь, Финляндию, Испанию, а также Казахстан. Причем в последнее время для этого становятся наиболее востребованными услуги курьерских, логистических компаний и почтовых каналов.

С учетом этого в 2018 г. ГУНК было организовано исполнение пунктов 8.10, 8.21 Плана основных организационных мероприятий МВД России, предусматривающих осуществление сотрудничества с компетентными органами иностранных государств, направленное на борьбу с контрабандой наркотических средств и психотропных веществ на территорию Российской Федерации, пресечение деятельности этнических и трансрегиональных преступных групп, а также проведение комплекса мероприятий, направленных на выявление участников преступных группировок, занимающихся изготовлением наркотических средств и психотропных веществ синтетического происхождения в условиях подпольных лабораторий.

Результатом стало увеличение на 141,5 % по сравнению с 2017 г. числа выявленных ОВД фактов контрабанды СДВ (с 241 до 582).

При непосредственном участии ГУНК удалось перекрыть ряд крупных каналов контрабанды наркотиков, организованных международными наркогруппировками.

Анализ проводимых мероприятий показывает, что к наиболее часто используемым относятся каналы поставок МДМА, ЛСД, амфетамина, метамфетамина из стран Евросоюза, синтетических наркотиков и новых психоактивных веществ – из Китая. В последнее время наметилась тенденция увеличения количества фактов пересылки международными почтовыми отправлениями сильнодействующих веществ, прежде всего веществ категории БАД и анаболических стероидов, из республик Беларусь и Казахстан.

В ходе проведенных МВД России в 2018 г. мероприятий выявлены 211 фактов (международных маршрутов)[33] и свыше 98 фактов (национальных маршрутов) поставок наркотиков посредством услуг почтовых, транспортных и логистических компаний. В посылках изъято около 353 кг наркотических средств, психотропных и сильнодействующих веществ.

В целом результаты проведенного мониторинга и работы МВД России в данной сфере деятельности позволяют обоснованно полагать, что пересылка наркотиков в почтовых отправлениях является наиболее востребованным и распространенным способом межрегионального наркосбыта и может рассматриваться в качестве контрабандного канала поставки различных видов наркотиков на территорию РФ.

Необязательность регистрации полных паспортных данных физических лиц, отправляющих и получающих грузы в логистических компаниях, недостаточная техническая оснащенность мест почтового обмена существенно снижают эффективность работы по установлению личности распространителей подконтрольных веществ и пресечению их противоправной деятельности.

В связи с этим необходимо совершенствование законодательства, регулирующего деятельность почтовых служб, логистических и транспортных компаний, в части установления обязательной идентификации и регистрации паспортных данных отправителя и получателя отправления (груза), а также оборудование почтовых отделений системами видеонаблюдения.

Данный вопрос нашел свое отражение в п. 1.6 решения заседания Государственного антинаркотического комитета[34]. Во исполнение этого поручения разработан проект поправок к проекту федерального закона № 418707-6 «О почтовой связи», пунктом 15 статьи 11 которого предусматривается процедура приема к пересылке и вручения регистрируемых почтовых отправлений, включающая идентификацию пользователя услугами почтовой связи и внесение соответствующих сведений в базу данных. Позиция МВД России по указанному проекту поправки поддержана и согласована.

4. Рост распространения синтетических наркотиков объясняется не только участившимися контрабандными поставками, но и увеличением объемов их подпольного производства непосредственно на территории России. Эти изменения в оперативной обстановке обусловлены простотой синтеза данного вида наркотиков, относительной доступностью приобретения необходимого для их изготовления сырья, реактивов и оборудования, увеличением количества специализированных магазинов их

[33] Зафиксированы факты контрабанды наркотиков из Украины (31), Нидерландов (19), ФРГ (17), Польши (9), Бельгии (5) и некоторых других стран Европы, а также из Китая (24) и Южной Америки (9).

[34] Протокол заседания ГАК от 23 июня 2017 г. № 33.

продажи, возможностью размещения подпольных лабораторий в квартирах, частных домах, гаражах, подсобных помещениях.

В настоящее время география незаконного производства «синтетики» расширяется в связи с ростом числа различных юридических организаций, в том числе интернет-магазинов, осуществляющих торговлю лабораторным оборудованием, химическими реактивами и прекурсорами с якобы допустимой концентрацией.

Помимо изложенного следует отметить, что в последние годы наметилась особенно негативная тенденция укрупнения производства синтетических наркотиков в подпольных лабораториях. Изготавливались в них в основном производные N-метилэфедрона (в частности, α-PVP), метамфетамин, метадон и мефедрон.

В связи с ухудшением социально-экономической обстановки, а также продолжением работы вербовочных центров в ряде регионов страны сохраняется тенденция вовлечения граждан соседних государств в изготовление и сбыт наркотических средств и психотропных веществ на территории России.

В 2018 г. в ходе проведенных совместных оперативно-разыскных мероприятий пресечена деятельность 4 организованных преступных групп, сформированных по этническому принципу, действовавших на территории Краснодарского края.

Так, в декабре 2018 г. в Краснодарском крае сотрудниками ГУНК МВД России совместно с УНК (УКОН) МВД России по Краснодарскому краю ликвидирована нарколаборатория, в которой из незаконного оборота изъято более 2 кг наркотического средства мефедрон, наркотическое средство метамфетамин, прекурсоры наркотических средств.

Проблема роста незаконного оборота психотропных веществ и наркотиков синтетического происхождения, произведенных в условиях подпольных лабораторий для «отечественного потребителя», связана с недостаточностью ответственности за изготовление и производство наркотиков, с отсутствием в законодательстве понятия «подпольная нарколаборатория» и ее «организация». Кроме того, имеется необходимость усиления контроля за оборотом прекурсоров как составляющей производства наркотических средств и психотропных веществ.

По официальным статистическим данным, в период с января по декабрь 2018 г. в России изъято 1 231 кг прекурсоров, что в 5,1 раза больше, чем АППГ (239), однако количество преступлений, связанных с незаконным оборотом прекурсоров, остается незначительным (зарегистрировано 35 преступлений, предусмотренных ст. 228.3 УК РФ, и 30, предусмотренных ст. 228.4 УК РФ).

Незначительность показателей изъятия прекурсоров объясняется объективными причинами:

– нормативно-правовыми требованиями к их концентрации [35], при которой данные вещества могут быть признаны предметом преступления;

– отсутствием в экспертно-криминалистических подразделениях современных методик исследования (определения процентного содержания прекурсоров) и контрольных образцов ряда веществ;

– бесконтрольным распространением, в том числе через Интернет, лабораторного оборудования, незапрещенных к обороту химических реактивов и прекурсоров курьерами через систему «закладок» (тайников);

– наркоторговцы, стремясь приспособиться к изменяющейся ситуации, становятся все более изобретательными и все чаще применяют для незаконного изготовления наркотиков альтернативные прекурсорам вещества.

В этой связи предлагается проработать вопрос о внесении изменений в законодательство, устанавливающих лицензирование деятельности по розничной торговле отдельными видами химического оборудования, закрепление обязательной регистрации и идентификации персональных данных их покупателей.

Также необходимо внесение изменений в Список I и таблицу I Списка IV Перечня, касающихся отмены разрешенной концентрации для прекурсоров наркотических средств и психотропных веществ. В настоящее время ГУНК разработан и рассматривается в Правительстве РФ первый проект соответствующего постановления об отмене установленной концентрации для двух наиболее используемых наркодельцами прекурсоров.

По остальным веществам вопрос пока не решен, что требует его дальнейшей проработки, в том числе научно-исследовательской, и рассмотрения в рамках межведомственных совещаний.

Список литературы

1. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ. Вена, 20 декабря 1988 г. // СПС «КонсультантПлюс».

2. О наркотических средствах и психотропных веществах: федер. закон от 8 января 1998 г. № 3-ФЗ // Собр. законодательства Рос. Федерации. 1998. № 2. Ст. 219.

3. О внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 1 марта 2012 г. № 18-ФЗ // СПС «КонсультантПлюс».

[35] Список I и таблица I Списка IV Перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в РФ, утвержденного постановлением Правительства РФ от 30 июня 1998 г. № 681.

4. Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2020 года: Указ Президента РФ от 9 июня 2010 г. № 690 // СПС «КонсультантПлюс».

М. А. МЫЛЬНИКОВ,
адъюнкт 3-го факультета
(Академия управления МВД России)

Информационные кадровые технологии по формированию профессионального состава полиции

В период проведения реформирования МВД России с 2011 г. одной из главных задач, как и прежде, остается формирование профессионального личного состава полиции, которая до настоящего времени окончательно не решена и поэтому продолжает и будет продолжать оставаться актуальной, пока идет процесс развития Министерства.

Предметом регулирования Федерального закона от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» являются правоотношения, связанные с поступлением на службу в ОВД, ее прохождением и прекращением. Основными направлениями формирования кадрового состава ОВД Федеральным законом определены:

– подготовка на плановой основе кадров для замещения должностей;

– создание условий для профессионального и должностного роста сотрудников;

– оценка результатов служебной деятельности;

– создание кадрового резерва и его эффективное использование;

– введение перечня должностей;

– применение современных кадровых технологий при приеме на службу в ОВД и ее прохождении.

Согласно Толковому словарю современного русского языка Д. Н. Ушакова технология (от греч. *techne* – «искусство» и *logos* – «учение») – совокупность наук, сведений о способах переработки того или иного сырья в фабрикат, в готовое изделие, совокупность процессов такой переработки[36].

Видится, что применительно к работе с персоналом современные кадровые технологии можно определить как процесс последовательных действий с целью изменения количественных и качественных характеристик личного состава ОВД, повышения уровня его профессионализма.

В настоящее время, с учетом развития техники и технологий, недостаточного количества и экономии ресурсов, ритма жизни «на высоких скоростях», требования к применяемым сегодня кадровым технологиям направлены на оптимизацию процессов решения проблем, на повышение качества и эффективности, изыскание резервов. Кроме того, технологии

[36] URL: http://ushakovdictionary.ru/word.php?wordid=76909 (дата обращения: 05.11.2019).

призваны минимизировать человеческий фактор, но оставлять право принятия окончательного решения все же за человеком. Хотелось бы отметить, что проверенные и где-то шаблонные кадровые технологии, в том числе применяемые с помощью современных информационных технологий, не должны расслаблять его и давать право уйти от ответственности за принятие решений.

Многие ученые выделяют три основные группы технологий – производственные, информационные и социальные. Существующие кадровые технологии имеют своей отличительной особенностью социальное предназначение, но направлены на определенный результат: повышение количественных и качественных характеристик персонала, своевременность, экономичность, целесообразность, согласованность целей организации и каждого сотрудника, обоснованность, информационную обеспеченность, правовую закрепленность и др.

В XXI в. информационными технологиями затронуты практически все сферы деятельности человека, в том числе и правоохранительная. На современном этапе развития ОВД они являются неотъемлемой частью взаимодействия как в едином внутреннем, так и внешнем информационном пространстве между правоохранительными и другими государственными органами, а также с юридическими и физическими лицами. Активное развитие информационных технологий в последние 10–15 лет позволяет сотрудникам ОВД, в частности по работе с персоналом, получать и обрабатывать большие объемы информации, а руководителям – принимать на ее основе своевременные и объективные управленческие решения, снимающие неопределенность и снижающие риск ошибочных выводов.

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации. В данном Федеральном законе даны определения основных понятий, таких как:

1) информация – сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Согласно ст. 5 указанного Федерального закона информация является объектом отношений – публичных, гражданских, правовых и может свободно использоваться и передаваться, если не установлены ограничения к ее предоставлению или распространению.

Основной целью информационных технологий работы с персоналом является получение, обработка и использование самой информации для принятия необходимых кадровых решений.

Информационные технологии позволяют решить несколько важных для работы с кадрами задач, таких как:

– удобство, быстрота и оптимизация кадровых процессов;

– накопление знаний и внедрение опыта;

– возможность работать дистанционно;

– разделение труда на ручное и техническое;

– экономичность и эффективность;

– доступность;

– возможность обработки больших массивов данных в минимальные сроки;

– совершенствование и прозрачность процессов взаимодействия;

– снижение риска ошибочных и неправомерных действий;

– поддержание репутации ОВД;

– снижение административных барьеров;

– дисциплина;

– безопасность электронного документооборота и др.

В ОВД в настоящее время внедрены и активно используются следующие информационные технологии в работе с личным составом:

– сервисы электронного документооборота;

– подача документов в электронном виде;

– видеоконференц-связь;

– СМС-информирование;

– сайты подбора персонала и др.

Очевидно, что внедрение информационных технологий оказывает существенное влияние на кадровые процессы, и в первую очередь на производительность труда. Информационные программы могут самостоятельно оперативно, своевременно и точно обрабатывать большие объемы данных. В результате на основе полученной достоверной информации предлагаются необходимые действия, различные сложившиеся ситуации сопоставляются с заданными критериями, после чего субъект кадровых технологий имеет возможность планировать, контролировать и корректировать процессы работы с персоналом и принимать окончательное решение.

Из всего вышеизложенного можно сделать вывод, что информационные кадровые технологии – это процесс последовательных, поэтапных действий субъекта кадровых технологий по поиску, сбору, хранению, обработке, предоставлению, распространению информации, а также способы осуществления таких процессов и методов.

Основной целью информационных кадровых технологий является получение объективной информации, объяснение происходящих процессов, экономия имеющихся ресурсов при поиске и выборе вариантов действий,

предложение оптимальных решений проблем по формированию профессионального состава полиции.

Актуальность данного вопроса обусловлена тем, что информация, поступающая к субъекту кадровых технологий, представляет собой такой массив, что без современных информационных технологий в области работы с кадрами становится невозможным ее переработать и принять правильное решение.

В завершение хотелось бы привести слова Президента России В. В. Путина, которые можно отнести и к информационным кадровым технологиям: «В общем и целом развитие технологическое идет неплохо, но нам нужен рывок. И нужно это обеспечить. Каменный век закончился не потому, что закончились камни, а потому, что появились новые технологии. Тот, кто опоздает в этом соревновании, мгновенно попадает в полную зависимость от лидеров этого процесса».

Список литературы

1. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 30 ноября 2011 г. № 342-ФЗ // СПС «КонсультантПлюс».
2. Толковый словарь Ушакова. URL: http://ushakovdictionary.ru/word.php?wordid=76909 (дата обращения: 05.11.2019).
3. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».
4. URL: https://ria.ru/economy/20170705/1497892989.html (дата обращения: 05.11.2019).

Н. А. ОВСЯННИКОВА,
старший научный сотрудник ЦООНД
(ФГКУ «ВНИИ МВД России»)

Современное информационное и технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей

Проблема сохранения объектов культурного наследия в условиях глобализации приобретает все большее значение. Масштабы нелегального рынка реализации культурных ценностей, увеличение противоправных посягательств на объекты культурного наследия, которые связаны с перемещением их через государственную границу, существование разветвленной сети транснациональной преступности в этой сфере обусловливают необходимость совершенствования информационного и технико-криминалистического обеспечения расследования преступлений в сфере культурных ценностей.

Мировая практика свидетельствует, что нелегальный оборот культурных ценностей занимает четверное место в «антирейтинге», уступая место незаконному обороту наркотических средств, оружия и отмыванию денежных средств, добытых преступным путем [10].

Раскрывая заявленную тематику научной статьи – современное информационное и технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей, которая в современных условиях борьбы с преступностью значительно актуализировалась, тезисно обозначим отправные точки познания вышеуказанных проблемных вопросов.

Рассматривая термин «обеспечение» в информационной среде в отношении деятельности по расследованию преступлений, Д. В. Лукьянов выделяет его в статике и в динамике. В статике обеспечение может быть определено как совокупность информационных средств и инструментов, которые служат для решения определенных задач, а также условий, способствующих процессу их решения, а в динамике – как процесс создания и представления указанных выше средств и условий для достижения поставленной цели [3].

Как отмечает В. В. Лунеев, средства, методы, приемы работы с доказательствами разрабатывает криминалистика, поэтому есть основания говорить об обеспечении именно криминалистикой расследования преступлений. Речь идет о комплексной деятельности, которая включает в себя учет многих факторов, обстоятельств, связанных с оптимальным предоставлением практике соответствующих средств раскрытия, расследования и предупреждения преступлений, в том числе и информационных. И поскольку криминалистика разрабатывает общие подходы, принципы, обобщающие рекомендации для расследования преступлений и предоставляет следователям необходимый практический инструментарий, такое обеспечение целесообразно

рассматривать как криминалистическое [5]. В связи с этим многие ученые отмечают, что информационное, научное и научно-методическое обеспечение – это составляющие криминалистического обеспечения расследования преступлений [6].

Е. Н. Паршина считает, что процесс выявления, анализа и оценки информации в ходе раскрытия и расследования преступлений является одним из главных познавательных аспектов предварительного расследования [9]. Проведя анализ мнений авторов, мы поддерживаем точку зрения Е. Н. Паршиной, так как основным элементом организации расследования преступлений является информационное обеспечение [7]. В данном контексте получение грамотно сформулированной и достоверной первичной информации является одним из главных элементов эффективной организации расследования преступлений. В этой связи информационные основы расследования преступлений, посягающих на культурные ценности, имеют обеспечительный характер по отношению к выявлению, расследованию и предупреждению данного вида преступлений.

Одним из источников информации, способствующей установлению истины при расследовании преступлений, являются многочисленные информационные системы, в которых концентрируется информация о разнообразных объектах материального мира. В современных условиях при расследовании преступлений используются данные, полученные из разнообразных по целевому назначению и ведомственной принадлежности систем, что в конечном итоге способствует эффективному осуществлению расследования, в том числе и преступлений в сфере культурных ценностей.

Представляя собой информационный процесс, расследование преступлений в полной мере зависит от имеющейся информации. Причем криминалистическое значение может приобрести любая информация об объектах и фактах.

Также не стоит забывать о том, что степень реалистичности и соответствия информационной модели факта или события напрямую зависит от качества и количества собранной о них информации. Это, в свою очередь, побуждает правоохранительные органы в процессе расследования обращаться не только к специально созданным для содействия расследованию информационным системам, но и к другим элементам информационного обеспечения, содержащим информацию, которая может приобрести криминалистическое значение в определенной ситуации. В процессе расследования существенное влияние на его ход, установление определенного объекта, культурной ценности или факта могут иметь не только специализированные данные – криминалистические, но и любые информационные системы независимо от их прямого целевого назначения и ведомственной принадлежности.

Информационное обеспечение международного розыска культурных ценностей является одним из направлений противодействия преступлениям

в сфере культурных ценностей, основную роль в котором осуществляет НЦБ Интерпола МВД России. К числу главных направлений деятельности Интерпола относится регистрация похищенных культурных ценностей и их международный розыск.

Нормативное закрепление информационного обеспечения борьбы с посягательствами на предметы, представляющие собой культурные ценности, нашло свое отражение в межведомственном приказе «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» [8].

В рамках расследования уголовных дел, оценивая содержание поступивших материалов с целью получения криминалистически значимой информации, следователь должен обращать внимание на то, какие факты, связанные с посягательствами на объекты, предметы и документы, представляющие историческую, научную, культурную, религиозную и художественную ценность, а также составляющие культурное наследие народов Российской Федерации, выявлены; имеются ли правовые основания и документы на распоряжение культурными ценностями, их хранение, ввоз и вывоз; представляет ли объект, предмет или документ историческую, научную, культурную, религиозную и художественную ценность, а также составляет ли культурное наследие народов Российской Федерации [1].

Использование инновационных технологий в процессе информационного обеспечения противодействия преступным посягательствам на культурные ценности, информационное сопровождение (ведомственного и межведомственного характера) противодействия преступным посягательствам на культурные ценности, причем как в масштабах страны, так и на международном уровне, в рамках сотрудничества в сфере обмена и получения информации о преступлениях и лицах, их совершивших, – все это требует дальнейшего развития с учетом современных достижений научно-технического прогресса.

С информационным обеспечением неразрывно связано технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей, которое само по себе имеет большое значение.

По мнению А. Ф. Волынского, технико-криминалистическое обеспечение представляет собой осуществляемую правоохранительными органами деятельность, направленную на создание условий их постоянной готовности к применению методов и средств криминалистической техники и реализацию этих условий в каждом конкретном случае раскрытия и расследования преступлений [3].

Следует согласиться с мнением Е. П. Ищенко, который отмечает, что одним из важных условий улучшения дел в области борьбы с преступностью является надлежащее криминалистическое обеспечение деятельности и расследования преступлений, что предусматривает четкое определение его понятия, содержания, структуры, субъектов осуществления [2].

Технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей играет большую роль. Так, понятие «технико-криминалистические средства» рассматривается в двух аспектах – узком и широком. В узком понимании – это приборы, приспособления и материалы, используемые для сбора, исследования и использования доказательств. В широком смысле – это не только технические приборы, приспособления и материалы, но и технические приемы, методы и методики их применения, которые используются для решения задач, связанных с раскрытием, расследованием и предупреждением преступлений.

Технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей можно охарактеризовать как систему теоретических положений и соответствующих технико-криминалистических рекомендаций по разработке, внедрению и применению технических средств в целях сбора, исследования, оценки и использования криминалистически значимой информации.

Информационное и технико-криминалистическое обеспечение расследования преступлений в сфере культурных ценностей является важным инструментарием оптимизации следственной деятельности и повышения ее эффективности, однако проведенный анализ научных исследований, статистических данных позволяет сделать вывод о наличии определенных недостатков и проблем на всех этапах раскрытия и расследования преступлений, что в конечном итоге приводит к снижению эффективности противодействия преступным посягательствам на культурные ценности.

Список литературы

1. *Власов П. Е., Степанищев А. В., Михайловская О. В., Власова В. С.* Особенности квалификации и расследования преступлений, посягающих на объекты культурного наследия (памятники истории и культуры): учеб. пособие. М., 2019.
2. *Ищенко Е. П.* Технико-криминалистическое обеспечение раскрытия и расследования преступлений. М., 2000. С. 15.
3. Криминалистика: учебник для вузов / под ред. проф. А. Ф. Волынского. М., 1999. С. 67.
4. Криминалистика: учеб. пособие / М. В. Савельева, А. Б. Смушкин. Ростов н/Д, 2015. С. 111.
5. *Лунеев В. В.* Тенденции современной преступности и борьбы с ней в России // Государство и право. 2004. № 1. С. 5–18.
6. *Махтаев М. Ш.* Проблемы криминалистического обеспечения предупреждения преступлений: дис. … д-ра юрид. наук. М., 2001.
7. *Можаева И. П.* Криминалистическое учение об организации расследования преступлений. Саратов, 2015.
8. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ

№ 333, ФТС РФ № 971 от 6 октября 2006 г. (ред. от 22 сентября 2009 г.) // СПС «КонсультантПлюс».
9. *Паршина Е. Н.* Проблемы информационного обеспечения и защиты информации в предварительном расследовании: автореф. дис. … канд. юрид. наук. Н. Новгород, 2004. С. 12.
10. *Тришкин А.* Безопасность наследия предков // Полиция России. 2018. № 9. С. 9.

В. Ю. ПЕТРОВА,
доцент кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

С. А. ОЛЬХОВИКОВ,
слушатель 2-го факультета
(Академия управления МВД России)

О некоторых аспектах использования искусственного интеллекта в ОВД

В современном мире технологии позволяют оптимизировать и усовершенствовать деятельность предприятия, организации, государственных, муниципальных образований и др. Новые технологии выходят на другой уровень, интенсивно замещая устаревшие системы как с технической стороны, так и с моральной.

Наша страна находится на стадии формирования информационного общества и в зависимости от внешних и внутренних факторов, тормозящих развитие цифровой технологии, процесс перехода информационной индустрии на новый уровень может продлиться не одно десятилетие. При этом необходимо отметить, что переход России к информационному обществу неизбежен – это просто вопрос национального выживания на мировой арене.

Построение в нашей стране и последующее развитие в ней информационного общества является весьма сложной проблемой, но вместе с тем объективной и существенной тенденцией в новом тысячелетии, составной частью (подсистемой) мировой тенденции. В связи с этим возникла острая необходимость в формировании единого информационно-телекоммуникационного пространства, без которого создать информационное общество невозможно.

Крайне желательно (просто необходимо), чтобы использование технологий искусственного интеллекта (ТИИ) в нашей стране соответствовало мировому уровню, поскольку это расширяет возможности решения определенных интеллектуальных задач.

Приведем несколько определений искусственного интеллекта:

– машины, выполняющие такие действия, для которых обычно требуется человеческий мозг [1, с. 217];

– условное обозначение кибернетических систем, моделирующих некоторые стороны интеллектуальной деятельности человека – логическое, аналитическое мышление [2, с. 513];

– область информатики, занимающаяся научными исследованиями и разработкой методов и средств для правдоподобной имитации отдельных

функций человеческого интеллекта с помощью автоматизированных систем [3, с. 141];

– техническое продолжение, усиление с помощью ЭВМ возможностей естественного интеллекта человека [4, с. 160];

– комплексная научно-техническая проблема, для решения которой исследования ведутся по четырем основным направлениям: моделирование отдельных функций творческих процессов; внешняя интеллектуализация ЭВМ; внутренняя интеллектуализация ЭВМ; целенаправленное поведение роботов [5, с. 12].

Развитие в ОВД технических, программных, программно-аппаратных комплексов, предназначенных для реализации основных функций, не стоит на месте.

Однако, по мнению ведомственных специалистов и научных сообществ, отмечается узкая направленность отдельных систем и программных комплексов. Несомненно, в условиях интенсивности развития различного рода современных технологий, постоянно меняющейся оперативной обстановки и необходимости реализации целей, стоящих перед МВД России и государством в целом, актуальным становится вопрос создания качественно новой системы, охватывающей все направления деятельности ОВД, реализация которой возможна посредством поэтапного внедрения платформы искусственного интеллекта (ИИ).

В основном работу искусственного интеллекта определяет программа, которую создал человек. Программа предполагает определенный, жесткий алгоритм поведения механизма или устройства, который управляется искусственным интеллектом.

Если проанализировать разные по своей сущности программы, которые и создавались в разные периоды, то можно увидеть, что все они сходятся к единому выводу: роботизация позволяет разрешить многие экономические и социальные проблемы. У нас в стране эти вопросы только начинают активно обсуждаться, но уже общепризнанным является факт, что развитие робототехники – приоритетное направление государственной политики.

Работы в области ИИ не ограничиваются экспертными системами. Они также включают в себя создание роботов, систем, моделирующих нервную систему человека, его слух, зрение, обоняние, способность к обучению.

Исследования в рамках искусственного интеллекта проводятся в двух направлениях:

– в бионическом, которое связано с исследованием и моделированием структур и процессов, характерных для мозга человека;

– в практическом, которое связано с созданием аппаратных и программных средств, с помощью которых можно решать интеллектуальные задачи.

Работы по первому направлению осуществляются на стыке электроники и бионики.

Электроника – наука об электронных процессах, а также область техники, связанная с производством и применением электронных устройств [5, с. 741].

Бионика – раздел кибернетики по использованию биологических процессов в решении инженерных задач [5, с. 42].

Второе направление – лидирующее. Здесь рассматривается только практическая сторона, т. е. конечный результат решения задач.

Для реализации идей ИИ разрабатываются системы искусственного интеллекта (СИИ).

Применительно к сотрудникам полиции использование искусственного интеллекта в служебной деятельности характеризуется некоторыми критериями. К таковым можно отнести: умение мобильно адаптироваться в новых условиях с учетом влияния внешних и внутренних факторов; высокую стрессоустойчивость; высокую работоспособность и т. д.

Учитывая новизну применения искусственного интеллекта как с технической стороны, так и со стороны моральных аспектов, необходимо справедливо отметить, что первыми этапами развития системы искусственного интеллекта в ОВД являются:

– создание отдельной системы, регулирующей конкретное направление деятельности;

– проведение анализа реализации данной системы;

– реагирование на негативные аспекты, влияющие на работоспособность системы ИИ.

Считаем, что определяющим этапом развития ИИ является работа над созданием удобного интерфейса, посредством которого сотрудники ОВД смогут наполнять базу новыми данными, получать логические выводы на основе ранее принятых решений, получать широкий спектр рекомендаций и др. Интегрируя накопленные знания и информацию, современные СИИ смогут находить наиболее верное решение для тех задач, которые слишком сложны и на реализацию которых необходимо затратить большое количество ресурсов и т. д.

Исходя из того, что искусственный интеллект пока не умеет мыслить как индивидуальная личность, но может полноценно обучаться, необходимо задуматься над вопросами обучения, контроля и безопасности внедрения ИИ в повседневную деятельность государства в целом и ОВД в частности.

Список литературы

1. *Кондаков Н. И.* Логический словарь-справочник. 2-е изд. М., 1975.
2. Советский энциклопедический словарь. М., 1990.
3. *Дорот В. Л., Новиков Ф. А.* Толковый словарь современной компьютерной лексики. СПб., 1999.
4. *Извозчиков В. А. и др.* Информатика в понятиях и терминах. М., 1991.

5. *Ожегов С. И.* Словарь русского языка. 20-е изд. М., 1988.
6. *Поспелов Г. С.* Искусственный интеллект – основа новой информационной технологии. М., 1988.

Д. В. ПОПОВ,
начальник кафедры философии и политологии
Омской академии МВД России,
кандидат философских наук, доцент

В. Е. ДИВОЛЬД,
начальник кафедры информационных технологий
в деятельности ОВД

М. В. БАТЮШКИН,
преподаватель кафедры информационных технологий
в деятельности ОВД

Практические преимущества и потенциальные издержки в применении алгоритмов больших данных в правоохранительной деятельности

Под модным сегодня термином «большие данные» буквально понимают огромный объем хранящейся на каком-либо носителе информации. Причем данный объем настолько велик, что обрабатывать его с помощью привычных программных средств нецелесообразно, а в некоторых случаях невозможно. Причем большие данные – это не только сами данные, но и технологии их обработки и использования, методы поиска необходимой информации в больших массивах. Для их определения консалтинговая компания Forrester предлагает следующую формулировку: «Большие данные объединяют техники и технологии, которые извлекают смысл из данных на экстремальном пределе практичности». Но на сегодняшний день термин «большие данные» стал настолько модным, что многие эксперты считают его дискредитированным и предлагают вообще от него отказаться. Более того, в октябре 2015 г. компания Gartner исключила из отчета «Цикл зрелости технологий 2015» сведения о больших данных. Свое решение аналитики компании объяснили размыванием термина. По их мнению, в состав понятия «большие данные» входит большое количество технологий, уже активно применяемых на предприятиях, они частично относятся к другим популярным сферам и тенденциям и стали повседневным рабочим инструментом [1]. Вместе с тем термин «большие данные» продолжает употребляться, а технологии хранения и обработки развиваться, предлагая новые решения [2].

В системе МВД России уже накоплены и продолжают ежедневно увеличиваться массивы данных, аккумулирующих сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В документах первичного учета, в учетных журналах, на других носителях, а также в информационных системах накапливаются данные оперативно-разыскного

и оперативно-справочного назначения, в которых содержатся сведения о правонарушителях и преступниках, о владельцах автомототранспортных средств и огнестрельного оружия, о событиях и фактах криминального характера, правонарушениях, похищенных и изъятых вещах, предметах антиквариата, паспортных данных лиц, а также другая информация, подлежащая хранению. С момента создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России весь массив этих данных хранится и обрабатывается централизованно. Кроме структурированных данных большое значение имеет хранение массы неструктурированных документов, возникающих в ходе оперативно-служебной деятельности подразделений, таких как рапорты, протоколы, акты и другие документы, отражающие ход и результат работы по различным направлениям. Программно-технический комплекс (ПТК) «Розыск-Магистраль» ежедневно пополняется внушительными массивами данных о передвижениях лиц железнодорожным, воздушным, морским, речным транспортом и рейсовыми междугородними автобусами. В системах фото- и видеофиксации комплексов «Безопасный город» и «Поток» накапливаются данные о передвижениях автотранспорта, дорожной обстановке, состоянии дорожной сети. Кроме того, события, происходящие на городских улицах, дорогах, во дворах и в подъездах домов, фиксируются видеокамерами наружного наблюдения государственных, а также различных негосударственных организаций, учреждений и частных лиц. Немаловажным элементом деятельности как МВД России, так и ряда других государственных органов является предоставление широкого спектра государственных услуг. Результатом данной деятельности является, в частности, постоянное возникновение и накопление большого объема данных социального характера. Социальные сети, форумы, сайты государственных органов, общественных организаций, информационно-справочные системы сети Интернет, данные о местонахождении абонентов мобильных сетей также являются поставщиками ценной информации.

Весь этот огромный информационный потенциал необходимо грамотно использовать в деятельности ведомства как для предупреждения, пресечения, раскрытия и расследования преступлений, так и для повышения качества принимаемых решений. Но сырые, необработанные и неструктурированные данные, если они потом не превращаются в знания, сами по себе бесполезны, поэтому их необходимо анализировать и использовать в интересах лиц, принимающих решения. Но уже сегодня без применения специализированных технологий, средств программной аналитики и инструментов, подходящих для принятия решений, обработать множество разнообразных хранилищ, структурированных и неструктурированных баз данных, фотомассивов, текстовых документов, видеозаписей практически невозможно. Полноценно возможности анализа всей совокупности вышеназванных данных, пожалуй, могут предоставить только технологии обработки больших данных. Например, компания McKinsey предлагает

к использованию следующий набор методов и техник анализа, применимых к большим данным: Data Mining, краудсорсинг, смешение и интеграцию данных, машинное обучение, искусственные нейронные сети, распознавание образов, прогнозную аналитику, имитационное моделирование, пространственный анализ, статистический анализ, визуализацию аналитических данных.

Из всего вышесказанного следует, что среда больших данных гетерогенна и табличное хранилище, построенное на реляционных принципах для хранения и проведения анализа, по многим параметрам не подходит. Разработчиками соответствующих решений предлагаются *платформы больших данных* [4], которые объединяют в себе приложения и средства для решения задач обработки больших объемов данных. Платформа BDP состоит из хранилищ данных, баз данных, серверов, средств управления данными и средств для аналитики.

Применение анализа больших данных позволяет проводить мероприятия по выявлению мошеннических схем в сети Интернет, пресечению деятельности террористической и экстремистской направленности, деятельности, связанной с незаконным оборотом наркотических средств, психотропных веществ, оружия и других запрещенных к обороту предметов, осуществляемой с использованием сетевых технологий.

По нашему мнению, используя большие данные в правоохранительной деятельности, можно в короткие отрезки времени осуществлять анализ разнородной информации, получая на ее основе ценные аналитические выводы для принятия управленческих решений в сфере охраны общественного порядка и общественной безопасности.

Представляется, что применение алгоритмов больших данных имеет не только выгоды и преимущества, но и определенный риск. Все более совершенные алгоритмы больших данных предоставляют невиданные возможности в аналитике данных, и поэтому их использование неизбежно. Многие задачи найдут и уже находят решение. Попутно возникает круг задач, которыми никто ранее не интересовался, – и эти задачи также находят решение! Лавинообразное расширение возможностей порождает эффект паноптизма – потенциальной возможности всевидения и всеведения [3]. В подобных условиях необходимо учесть, что, во-первых, применение технологии влечет неизбежные издержки; во-вторых, издержки не должны нивелировать выгоды применения технологии; в-третьих, в ряде случаев требуется намеренное ограничение в использовании технологии, способной породить существенные негативные последствия.

Так, следствиями эффекта паноптизма могут стать: 1) исчезновение приватного пространства личности; 2) искушение от использования методов профайлинга с целью запастись информацией несанкционированно и «впрок»; 3) накопление обширных досье на граждан на основе обработки электронных следов в сети в условиях отсутствия контроля

над конфиденциальностью данной информации; 4) дискриминация на основании данных профайлинга.

Например, неприятным и неожиданным следствием развития системы видеонаблюдения «Безопасный город» в Москве стали появившиеся в СМК сообщения об утечке данных и возможных злоупотреблениях персональной информацией в неизвестных целях [4].

Во избежание возникновения подобных проблем законодатель спешно принимает нормы, охраняющие от негативных последствий шагающей семимильными шагами технологии. «Совершенно не случайно резолюция Европейского Парламента от 14 марта 2017 г. «О последствиях применения технологий больших данных для основополагающих прав человека: неприкосновенность частной жизни, защита персональных данных, недискриминация, безопасность и обеспечение правопорядка» предостерегает от нетранспарентного использования технологий больших данных как несущих потенциальную угрозу правам и свободам человека. Так, еврозаконодатель предостерегает правоохранительные органы от использования обработки и анализа данных без соответствующих – ясных, четко определенных и законных – целей и соизмеримых и нечрезмерных средств. Предостерегая от дискриминации в форме профайлинга, резолюция одобряет использование анонимизации, псевдонимизации, шифрации для обеспечения безопасности личных данных и создания условий невозможности реидентификации личности по электронным следам коммерческими или иными структурами с непрозрачными целями» [6].

Алгоритмы больших данных в случае их повсеместного неограниченного использования могут обеспечить такого рода вторжение в частную жизнь и такого рода масштабирование, при которых произойдет имплозия приватности и смешение гражданского общества, полиции и специальных служб, имеющих равный доступ к всевидящим палантирам [3].

«В мире, где публичная интимность – норма, а трассы электронных следов от рождения до смерти создают электронную копию жизни, возникает соблазн утверждения тотального цифрового паноптизма в качестве парадигмы. Мир Замятина уже не выглядит фантастикой. Разоблачения Э. Сноудена, применение деонтологии И. Бентама в Синьцзяне, где в форме социальных кредитов ведется строгий цифровой учет пользы и вреда поведения индивидуума для общества, говорят о том, что цифровой паноптизм становится атрибутом реального нецифрового государства. Безусловно, безопасность человека – ценность. Впрочем, ценностью остается и индивидуальная свобода. Представляется, что «дисциплинарная мечта» абсолютного паноптизма ради общего блага не должна породить мир «идеальных заключенных», а остаться в рамках разумно предусмотренной законом сферы, ограниченной соблюдением основополагающих начал жизни человека: индивидуальности, свободы, выбора, творчества и т. д.» [3].

Применение технологий больших данных должно учитывать, что «человек, будучи человеком несовершенным – существом естественным, а не цифровым алгоритмом, в своей жизни допускает ошибки, неточности, что приводит к углубляющемуся противоречию его образа жизни и среды, основанной на цифровых – высокоскоростных, высокоточных, безошибочных – технологиях. В таких условиях существует реальная возможность проложить благими намерениями дорогу в ад – создать высокотехнологичную клетку, ментально, психологически, телесно не рассчитанную на человека» [6].

Алгоритмы больших данных – эффективное решение многочисленных проблем, в том числе в правоохранительной деятельности. Однако применение данной технологии должно быть глубоко сбалансированным и целесообразным. В противном случае сюжеты антиутопии могут стать жизненными сценариями. Осознание данной проблематики уже приводит к пересмотру использования больших данных в деятельности полиции. Например, по сообщениям СМК, власти Сан-Франциско запретили использование технологий распознавания лиц в связи с обеспокоенностью общественности по поводу того, что применение данной технологии может привести к нарушению неприкосновенности частной жизни и гражданских прав жителей [7].

Список литературы

1. URL: http://www.tadviser.ru/index.php/Статья:Большие_данные_(Big_Data) (дата обращения: 15.12.2019).
2. Как бороться с опасной болезнью цифровой эпохи – безудержным накопительством данных? URL: http://www.tadviser.ru/index.php (дата обращения: 15.12.2019).
3. *Попов Д. В.* История паноптизма: от оракулов к палантирам. Манускрипт. Тамбов, 2019. С. 166–171.
4. Глаз – народу! URL: https://novayagazeta.ru/articles/2019/11/05/82618-glaz-narodu/ (дата обращения: 16.12.2019).
5. Андрей Каганских о том, как полицейский искал его по системе распознавания лиц. URL: https://mbk-news.appspot.com/sences/andrej-kaganskix-o-tom/ (дата обращения: 16.12.2019).
6. *Попов Д. В.* Человек ошибающийся и большие данные: от головного мозга к искусственному интеллекту // Интеллект. Инновации. Инвестиции. 2019. № 2. С. 89–96.
7. Власти Сан-Франциско запретили использование технологий распознавания лиц. URL: https://www.forbes.ru/tehnologii/376099-vlasti-san-francisko-zapretili-ispolzovanie-tehnologiy-raspoznavaniya-lic (дата обращения: 16.12.2019).

С. А. ПОПОВ,
слушатель 2-го факультета
(Академия управления МВД России)

Информационное обеспечение выработки управленческого решения по снижению неукомплектованных штатных должностей в территориальном органе МВД России на региональном уровне

Развитие системы МВД России в современных условиях напрямую зависит от качества и эффективности принимаемых управленческих решений. Одним из условий принятия таких решений является обработка больших информационных массивов относительно проблемного вопроса служебной деятельности. В эпоху цифровых технологий и всеобъемлющей компьютеризации не использовать современные достижения науки и техники в служебной деятельности ОВД – означает отказаться от эффективного управления и сбалансированной работы всей системы.

Под эффективностью управленческой деятельности понимается ее результативность, способность при наименьших затратах кадровых, финансовых, материальных, временных и иных ресурсов обеспечить достижение целей, стоящих перед ОВД [1].

В толковом терминологическом словаре под информационным обеспечением понимается «получение, накопление, обработка и реализация вновь поступивших информационных данных, необходимых для решения каких-либо задач» [3].

Как управленческая функция организация информационного обеспечения в ОВД имеет ряд особенностей:

– имеет целесообразный характер и осуществляется в рамках конкретного органа;

– относительно самостоятельна по отношению к системе управления органом в целом;

– носит координационный характер, позволяющий согласовывать порядок сбора, накопления и передачи информации по горизонтали (например, организация обмена информацией между различными службами и подразделениями органа) [2].

Процесс принятия управленческих решений подвержен влиянию различных факторов, которые отражают особенности руководителя, внутренней и внешней среды, в том числе условия неопределенности и риска, информационные ограничения, взаимосвязь принимаемых решений и другие факторы.

Для снижения влияния негативных факторов в ходе выработки эффективных управленческих решений необходимо разрабатывать и внедрять в практическую деятельность ОВД современные информационные технологии, в том числе по обработке и анализу информационных источников,

характеризующих социально-экономическое развитие того или иного региона. Функционирование ОВД на региональном уровне происходит в различных условиях внешней социальной среды, недооценивать степень ее влияния на происходящие процессы внутри системы является недопустимым.

Применительно к проблемному вопросу служебной деятельности ОВД по снижению количества неукомплектованных должностей в территориальном органе МВД России на региональном уровне источниками получения информации могут являться:

– демографические данные о рождаемости в регионе от 18 до 39 лет назад, а также сведения по оттоку (притоку) трудоспособного населения региона;

– статистические данные о среднем размере денежного довольствия сотрудников, среднем размере заработной платы по региону (по отдельным территориальным органам на районном уровне), а также среднем размере заработной платы по заявленным вакансиям в центре занятости населения;

– сведения сервисов, предоставляющих услуги по поиску работы, о ситуации на рынке труда и ее изменении за определенный период (например, HeadHunter), а также сведения налоговой инспекции о количестве хозяйствующих субъектов, осуществляющих свою деятельность в регионе;

– информация о количестве обучающихся и выпускников средних профессиональных и высших образовательных организаций, осуществляющих свою деятельность на территории региона;

– сведения из военных комиссариатов о количестве граждан, подлежащих увольнению в запас по окончании срочной военной службы;

– сведения о количестве выпускников ведомственных образовательных организаций МВД России, прибывающих в распоряжение территориального органа;

– информация об уровне осведомленности граждан, проживающих на территории региона, о потребности ОВД в комплектовании вакантных должностей и основных условиях прохождения службы;

– информация о количестве неукомплектованных должностей в других федеральных органах исполнительной власти, имеющих схожие условия прохождения службы и социальное обеспечение;

– учетно-отчетная документация за определенный период, характеризующая движение кадров;

– статистические данные о работе с кандидатами на службу;

– информационные сведения о дисциплинарной практике, морально-психологическом климате и рейтинге руководителей подразделений.

Перечень приведенных источников информации не является исчерпывающим и исходя из изменений оперативной обстановки может быть дополнен.

Как отмечал М. А. Москалев [2], информационное обеспечение в ОВД предполагает особые требования:

– информация должна быть комплексной;

– информация должна быть проверенной, достоверной и объективной;

– информация должна быть релевантной, т. е. непосредственно относящейся к делу;

– информация должна быть репрезентативной, т. е. отражать все основные характеристики изучаемой совокупности явлений.

Этап сбора информации имеет важное значение в механизме выработки и принятия управленческого решения, поскольку его результаты используются на всех последующих этапах и напрямую влияют на качественное и эффективное решение проблемы.

Форма предоставления информации влияет на доступность ее понимания субъектом управления и относимость к существующей проблеме. На практике нередко возникают ситуации, при которых ключевые сведения о проблеме скрываются за «ворохом» другой информации, не имеющей ключевого значения для решения вопроса. Задачей лица, осуществляющего сбор и систематизацию информации, является расставление правильных акцентов и ранжирование по приоритетам собранных сведений.

Техническое перевооружение на основе новых информационных программ и искусственного интеллекта, использование сетевых технологий преобразования данных в нужную форму позволят в значительной степени сократить количество времени, затрачиваемого на данный процесс, и повысить качество предоставляемой информации.

Кроме того, работа с информацией с применением искусственного интеллекта позволит повысить ее объективность, исключив влияние субъективных факторов при оценке причин и условий появления проблемы.

Примером влияния субъективного фактора при работе с информацией по проблемному вопросу служебной деятельности может являться оценка «вклада» в формирование проблемы собственных ранее принятых управленческих решений. С точки зрения психологии провести объективную оценку собственных действий может далеко не каждый человек. Стремление оправдать себя в любой ситуации, удачи приписать себе, а неудачи свалить на другого – это одно из свойств человеческой натуры. Не желая признавать свои ошибки, человек не осознает необходимости в том, чтобы исправлять их, а это уже чревато дальнейшими неприятностями [5].

Отсутствие объективной оценки ранее принятых управленческих решений ведет к нарушению одного из основополагающих принципов науки управления – преемственности управленческих решений. Руководители пытаются найти оптимальное решение проблемы методом проб и ошибок, тем самым усугубляя ее состояние.

Так, к просчетам в принятых управленческих решениях в сфере кадрового обеспечения МВД России можно отнести количество сотрудников, проработавших в должности менее года, от числа сменившихся [4]:

– по начальникам территориальных органов МВД России на районном уровне их доля составила 7,6 %;

– по заместителям начальников территориальных органов МВД России на районном уровне – 9 %;

– по руководителям подразделений уголовного розыска – 14,6 %.

Применение новых информационных технологий, создание алгоритма действий руководителя при разработке управленческого решения на базе искусственного интеллекта позволит свести к минимуму просчеты в управленческой деятельности, повысить ее эффективность и сократить издержки на содержание дополнительного аппарата сотрудников, обеспечивающих данную работу.

Список литературы

1. *Клушин О. З.* Оперативная обстановка: понятие, анализ, прогноз: учеб. пособие. М., 2010.
2. *Москалев М. А.* Информационное обеспечение планирования в территориальных органах МВД России: учеб. пособие. М., 2014.
3. Бизнес и безопасность: толковый терминологический словарь / под ред. А. И. Гурова, Б. С. Тетерина. М., 1995.
4. Сведения о состоянии работы с кадрами органов внутренних дел Российской Федерации за 2018 год: сборник аналитических и информационных материалов. М., 2019.
5. URL: http://www.tinlib.ru/delovaja_literatura/psihologija_biznesa_upravlenie_yemocija mi/p3.php (дата обращения: 11.11.2019).

А. Г. РОМАНОВ,
адъюнкт факультета подготовки научных и научно-педагогических кадров (Академия управления МВД России)

Б. А. ТОРОПОВ,
доцент кафедры информационных технологий, кандидат технических наук, доцент (Академия управления МВД России)

Актуальные вопросы применения интеллектуального анализа данных для предупреждения преступлений в информационно-телекоммуникационной среде

Привычные сферы жизни человека и общества, которые еще несколько лет назад успешно функционировали в реальной действительности, в настоящее время по меньшей мере неполноценны без интеграции в виртуальное пространство Интернета. С момента создания и по ходу развития виртуального пространства наметился отчетливый тренд на цифровизацию обмена и хранения информации, следствием чего стала стремительная популяризация общедоступных открытых источников информации и платформ для обмена ею. Необходимо отметить, что доступ к таким ресурсам характеризуется относительной анонимностью пользователей и, как следствие, – формированием благоприятной социальной площадки, которая оказалась не защищена от преступных посягательств и, более того, во многих случаях, наоборот, способствует совершению преступлений. Условно безопасный и открытый доступ к многообразию сведений позволяет квалифицированной преступности находить способы анализировать сферу электронной коммерции и, как следствие, реагировать на изменения спроса на товары и услуги. Расставляя приоритеты, продиктованные реалиями настоящего времени, целесообразно определить, что стабильное функционирование финансово-экономической сферы государства во многом зависит от качественного и эффективного выполнения правоохранительных задач, в том числе и в виртуальном пространстве. В данной статье предлагается рассмотреть возможные направления совершенствования деятельности ОВД, нацеленные на превентивное противодействие преступлениям, совершаемым посредством сети Интернет, и основанные на выявлении и изучении закономерностей в действиях пользователей.

Широко известен тезис о том, что Интернет «помнит» все. Действительно, интернет-сервисы различной природы предлагают пользователям формализованные наборы действий и фиксируют выбираемые ими опции. История ранее предпринятых пользователем действий позволяет

с некоторой точностью предполагать его предпочтения и прогнозировать его дальнейшие действия, а также идентифицировать и/или классифицировать их. Подобные методы хорошо известны в сфере маркетинга, они позволяют на основе интеллектуального анализа данных выстраивать модели активности клиентов электронного рынка и прогнозировать их поведение в сфере онлайн-услуг, а как следствие – и покупательский спрос.

Предлагаемая модель с определенной точностью предсказывает категорию наиболее вероятных покупаемых и просматриваемых товаров на рынке онлайн-покупок со стороны клиента и в соответствии с этим дает возможность правоохранительным органам прогнозировать и своевременно предупреждать преступления, где объектом являются товары, пользующиеся повышенным спросом, при этом необходимо заметить, что положительной информативной стороной будет являться обратный спрос – в том смысле, что, зная конкретный товар, возможно отследить динамику спроса. Характерными примерами являются отдельные товары, которые имеют свободный гражданский оборот, но при необходимости могут служить комплектующими для разных систем и механизмов, являющимися в целом орудием преступления, как пример – в области экстремизма (химические составы), компьютерных преступлений (скимминговые устройства, негласное наблюдение) и иное.

Определяя понятие интеллектуального анализа данных, необходимо указать, что рассматривается процесс обнаружения значимых поведенческих шаблонов в огромном количестве наборов данных, которые хранятся на серверном оборудовании провайдеров. Основная идея использования метода интеллектуального анализа данных заключается в классификации данных клиента по апостериорной вероятности. В модели выполняется классификация обучающих данных, которые используются для дальнейшего прогнозирования. Данными выступают зафиксированные записи о различных действиях пользователя на информационном ресурсе в сети, базовыми из которых являются движения мышью и нажатия на ее клавиши, условно обозначаемые как клики. Вводя определение потоков кликов, укажем, что это щелчки мышью или действия мыши, которые пользователь выполняет, когда просматривает содержимое информационного ресурса, именно на их основе прогнозируется его поведение как клиента. Применительно к деятельности правоохранительных систем подобная модель может быть чрезвычайно востребована для предупреждения и раскрытия противоправных деяний.

Существует целый ряд исследований, посвященных сбору и анализу данных, интеллектуальному анализу данных и анализу данных о кликах в частности. В [1] авторы представили модель для анализа потоков кликов по электронной почте. Модель прогнозирует, будут ли покупатели покупать товары, добавленные в корзины для покупок на цифровом рынке покупок. Для анализа и прогнозирования дерева решений и многослойных нейронных сетей были использованы модели интеллектуального анализа данных. В [2] исследовано правило ассоциации воспитания родителей и способность

повлиять на поведение и опыт использования Интернета подростками по алгоритму «априори». Эффективный алгоритм интеллектуального анализа правил ассоциации используется для поиска связей между продуктом и транзакцией клиента [3]. Рассматривая процессы аналитики, нужно пояснить, что они могут быть осуществлены с помощью методов интеллектуального анализа данных, таких как классификация, кластеризация, прогнозирование и т. д. Таким образом, с точки зрения поведения пользователя его профиль может быть создан посредством анализа данных потока кликов. Поэтому, прежде чем приступить к анализу, необходимо создать модель с соответствующей базой данных или хранилищем данных, так как последние играют важную роль в модели интеллектуального анализа данных.

Обозначим используемые атрибуты для сбора данных и сохранения их в базе данных:

– «день» и «дата»: атрибут представляет дни недели и дату, когда пользователь проявлял активность;

– «временной интервал»: атрибут представляет интервал суточного времени дня, при этом предусмотрена классификация: «0» – утро, «1» – день и «2» для вечера/ночи;

– «идентификатор категории»: продукты, представленные на информационном ресурсе, предварительно классифицированы на электронику, одежду, обувь и т. д., при этом товару предварительно присвоен уникальный идентификатор: «1» – электроника, «2» – одежда, «3» – обувь и т. д.;

– «количество корзин»: атрибут включает в себя количество различных товаров в корзине, помещенных пользователем. Товары могут обладать одинаковой категорией, но отличаться по размеру и цвету;

– «количество покупок» – показывает общее количество товаров или товаров определенной категории, приобретенных пользователем;

– «количество кликов» – атрибут индексирует момент нажатия на определенный элемент, при этом данная запись будет рассчитываться как количество кликов. Необходимо пояснить, что в рассматриваемой модели считывается и в дальнейшем фиксируется только количество кликов, сделанных для товара или продуктов;

– «количество запросов» – представляет действия пользователя на информационном ресурсе, в том числе когда производится поиск по ключевым словам.

Описывая архитектуру предлагаемой модели, необходимо пояснить, что существуют три модуля, образующие систему, такие как модуль администратора, модуль клиента и модуль сервера. Клиенты уполномочены открывать информационный ресурс и выполнять различные действия в его пределах, а именно регистрацию, вход в систему, поиск товаров, оставлять комментарии с регистрами «нравится»/«не нравится», выделять и просматривать товары. Серверный модуль производит логирование

в журнал активности пользователя. Модуль администратора используется для предоставления предложений на основе анализа и прогнозирования.

Модуль администратора состоит из частей, сопряженных с процессами обработки, определим их как этапы. Первый этап состоит из добавления и управления продуктами, где администратор уполномочен добавлять, удалять и управлять продуктами в целом. Вторая часть предусматривает анализ, в рамках которого реализуется фактический алгоритм. Существует связь между модулем администратора и базой данных, которая используется в системе. На основании сделанного прогноза предложения, исходя из заложенного ранее алгоритма, будут переданы отдельным заинтересованным клиентам, при этом администратор не сможет выполнять запросы к базе данных для управления продуктами. Клиентский модуль используется для действий клиентов, таких как регистрация, поиск, просмотр и т. д. Во-первых, клиентам предлагается пройти регистрацию в созданном программном приложении. При успешной регистрации им предоставляется доступ к поиску товаров по названию, категории, комментариям «нравится»/«не нравится», рейтинг конкретного продукта. Сервер, который использован в рассматриваемой модели, является сервером MySQL. Соединение JDBC используется для соединения баз данных. Сервер отвечает за аутентификацию пользователя, а также предоставляет услуги, запрошенные пользователями. Он также поддерживает логирование в журналы пользователей на основе кликов и активности. Администратор выполняет анализ журналов и прогнозирует интерес на отдельную клиентскую категорию продуктов.

Обращаясь к работе непосредственно алгоритма, необходимо указать, что процесс классификации данных включает в себя два этапа. Первый состоит из процесса обучения, где данные анализируются с помощью алгоритма классификации. Второй этап процесса проводит классификацию, в которой тестовые данные проверяются по алгоритму классификации для оценки точности алгоритма. Когда обучение завершено, эта модель используется для классификации данных по различным классам. В данном случае пользователи, они же клиенты, классифицируются по категориям интереса, таким как электроника, одежда и аксессуары, спортивные товары, предметы коллекционирования, косметические товары, книги и т. д. Но перед этим необходимо провести анализ активности пользователя на основе данных его истории из журналов. На данном этапе для анализа и прогнозирования поведения пользователей по выставленным меткам для классов, указанных выше, будет использоваться наивный байесовский классификатор.

Наивный байесовский алгоритм основан на теореме Байеса с допущением о независимости признаков, выполняет статистическую классификацию [4]. Именно допущения образуют название алгоритма – «наивный». Рассматриваемый алгоритм предполагает, что наличие какого-либо признака в классе не связано с наличием какого-либо другого признака. При этом, если даже эти признаки зависят друг от друга или от других

признаков, в любом случае они вносят независимый вклад в вероятность того, что объект принадлежит к конкретному классу. Другими словами, данный вид классификатора используется для прогнозирования вероятностей членства в классе, таких как вероятность того, что данный кортеж принадлежит какому-либо конкретному классу. Данный алгоритм удобен для создания моделей, где необходима обработка больших наборов данных. Байесовская классификация основана на теореме (или правиле) Байеса, которая позволяет рассчитать апостериорную вероятность (условную вероятность) случайного события, а именно: возможность некоторого вывода *C*, учитывая некоторое наблюдение *E*, где существует зависимость между *C* и *E*. Эта вероятность обозначается как *P(C|E)*, где

$$P(C|E) = \frac{P(E|C)P(C)}{P(E|C)} \quad (1)$$

Наивный байесовский классификатор работает следующим образом.

1. Пусть *D* будет обучающим набором кортежей и связанных с ними меток классов. Каждый кортеж представлен *n*-мерным вектором атрибута, $X = (x_1, x_2, x_3 \ldots, x_n)$ показывает *n* измерений на кортеже из *n* атрибутов, соответственно, $A_1, A_2, \ldots, A_n$.

2. Предположим, что у нас есть *m* классов $C_1, C_2 \ldots, C_m$. Наивный байесовский алгоритм позволяет на основании наличия у классифицируемого объекта характеристики X отнести этот объект к одному из классов согласно выражению:

$$P(C_i|X) = \frac{P(X|C_i)P(C_i)}{P(X)} \quad (2)$$

3. Поскольку *P (X)* постоянна для всех классов, только $P(X|C_i)P(C_i)$ должна быть максимальна. Если априорные вероятности класса неизвестны, то обычно предполагается, что вероятность классов одинакова, т. е. $P(C_1) = P(C_2) = \ldots P(C_m)$, и поэтому необходимо максимизировать $P(X|C_i)$. В противном случае необходимо максимизировать $P(X|C_i)P(C_i)$. Обратим внимание, что класс априорных вероятностей может оцениваться по формуле $P(C_i) = |C_i, D| / |D|$, где $|C_i, D|$ – число обучающих кортежей класса C_i в D.

4. Если заданные наборы данных имеют много атрибутов для вычисления $P(X|C_i)$, может потребоваться дорогостоящее вычисление. Чтобы уменьшить вычисления при оценке $P(X|C_i)$, делается наивное предположение об условной независимости класса. Это предполагает, что значения атрибутов условно независимы друг от друга, учитывая метку класса кортежа. Таким образом,

$$P(X|C_i) = \prod_{k=1}^{m}(X_K|C_i) = P(X_1|C_i) * P(X_2|C_i) * \ldots P(X_m|C_i) \quad (3)$$

Мы можем легко оценить вероятности $P(X_1|C_i), P(X_2|C_i), \ldots, P(X_m|C_i)$ из обучающих данных. Здесь X_k относится к значению атрибута A_k

для кортежа *X*. Для каждого атрибута смотрим, имеет ли он категориальное или непрерывное значение. Например, для вычисления $P(X|C_i)$ рассмотрим следующее:

а) если A_k категоричен, то $P(X_k|C_i)$ – это число кортежей класса C_i в *D*, имеющих значение X_k для A_k, деленное на $|C_i, D|$ число кортежей класса C_i в *D*.

b) если A_k имеет непрерывное значение, то расчет довольно прямолинейный. Атрибут, имеющий непрерывное значение, обычно считается Гауссовым распределением [5] со средним μ и стандартным отклонением σ, определенным *b*.

$$g(x, \mu, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (4),$$

так чтобы

$$P(X_k|C_i) = g(X_k, \mu_{C_i}, \sigma_{C_i},) \quad (5)$$

Мы должны вычислить μ_{C_i} и σ_{C_i}, которые являются средним и стандартным отклонением значений атрибута A_k для обучающих кортежей класса C_i. После этого необходимо поместить их в приведенное выше уравнение.

5. Для соотнесения объекта классификации, обладающего характеристикой X, с одним из классов C_1–C_m необходима проверка степени его принадлежности к каждому из этих классов:

$$P(X|C_i)P(C_i) > P(X|C_i)P(C_i) for 1 \le j \le m, j \ne i \quad (6)$$

Другими словами, предсказанная метка класса – это класс C_i, для которого $P(X|C_i)P(C_i)$ является максимумом.

По результатам возможно констатировать факт, что рассмотренная модель на основе наивного байесовского алгоритма работает эффективно или дает лучшую точность в среднем для больших наборов данных, и, наоборот, ее производительность снижается, если размер набора данных меньше. Поскольку заранее были сохранены журналы кликов и активности пользователей, эти массивные данные были проанализированы и в дальнейшем классифицированы, после чего возможно сделать прогноз с помощью наивного алгоритма на основе теоремы Байеса. Рассмотренный пример показывает, что с помощью метода интеллектуального анализа данных возможно спрогнозировать и определить тренд спроса и предложения на определенную группу товаров. Применяя данную модель в правоохранительной деятельности, возможно осуществлять превентивные меры, основанные на спросе и предложении в глобальной сети Интернет, проводя анализ потенциальных объектов преступного посягательства, что укладывается в комплексный методический подход к организации и планированию деятельности ОВД России [6].

Список литературы

1. *Silahtaroglu G., Donertasli H.* Analysis and prediction of E-customers' behavior by mining clickstream data // 2015 IEEE International Conference on Big Data. 2015. P. 1466–1472.

2. *Rodmorn C., Panmuang M., Potiwara K.* Analysis of the Internet using behavior of adolescents by using data mining technique // 2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE). 2015. P. 398–402.

3. *Zhao C., Tu S., Chen H., Huang Y.* Efficient association rule mining algorithm based on user behavior for cloud security auditing // 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS). Chongqing, 2016. P. 145–149.

4. *Бурлаков М. Е.* Применение в задаче классификации смс-сообщений оптимизированного наивного байесовского классификатора // Известия Самарского научного центра Российской академии наук. 2016. № 4 (4). С. 705–709.

5. *Чернышев В. Л., Толченников А. А.* Свойства распределения гауссовых пакетов на пространственной сети // Наука и образование. 2011. № 10. С. 1–10.

6. *Дубинин М. П., Дубинина Н. М.* Методологические аспекты постановки задачи анализа результатов деятельности органов внутренних дел // Вестник Московского университета МВД России. 2013. № 11. С. 254–260.

В. Е. СИДОРОВА,
начальник отдела по работе с обращениями граждан
(Управление по вопросам миграции ГУ МВД России по г. Москве)

Законодательное регулирование личного приема при осуществлении контрольно-разрешительных функций в сфере миграции

В соответствии с требованиями подп. «з» п. 26 Концепции государственной миграционной политики Российской Федерации [6] совершенствование административных процедур в сфере миграции представлено одним из приоритетных направлений деятельности Российского государства на ближайшие 6 лет, что, безусловно, актуализирует вопрос эффективности законодательного регулирования процедуры личного приема при осуществлении государственными органами своих функций в сфере миграции.

Личный прием является важным инструментом в процессе взаимодействия населения с государственными органами по вопросам миграции. Право на личный прием является неотъемлемым правом российского гражданина, закрепленным в ст. 33 основного закона Российской Федерации [1]. Законодатель установил обязанность иностранных граждан и лиц без гражданства лично обращаться в компетентные органы внутренних дел в сфере миграции по соответствующим вопросам (прим. п. 9 ст. 6, абз. 4 п. 16, п. 20, п. 26 ст. 13.3; п. 10 ст. 13.4 и т. д.) [3].

Следует подчеркнуть, что рассматриваемая форма взаимодействия характерна не только для иностранных граждан и лиц без гражданства, учитывая их правовой статус, но и в целом широкого круга граждан, являясь наиболее распространенной и наиболее часто применяемой на практике, однако на сегодняшний день как в научных исследованиях, так и в законодательстве акцент сделан преимущественно на письменные способы подачи обращений, поступающих от граждан [7].

На федеральном уровне можно отметить несколько законодательных актов, в той или иной мере затрагивающих вопросы личного приема граждан. Так, например, требованиями ст. 2 Федерального закона № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» закреплено право граждан лично обращаться в государственные и муниципальные учреждения, а также к должностным лицам [4].

Вместе с тем там же закреплены требования единственной статьи (ст. 13), посвященной вопросу непосредственного взаимодействия заявителя

и должностного лица. Положения рассматриваемой правовой нормы регламентируют лишь некоторые, на наш взгляд, самые общие вопросы, а именно: место проведения личного приема, необходимость подтверждения заявителем своей личности, способ фиксации содержания устного обращения и т. д.

Этим же положением закреплено право на личный прием в первоочередном порядке в соответствии с требованиями ст. 16 Федерального закона № 3-ФЗ «О статусе члена Совета Федерации и статусе депутата Государственной Думы Федерального Собрания Российской Федерации» [2].

Вступившими в силу положениями Федерального закона № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [5] личный прием закреплен в качестве правового способа обращения с жалобой (п. 2 ст. 11.2) либо как процедура, в ходе которой заявитель вправе получить информацию о предоставлении той либо иной услуги или о подготавливающемся в рамках запроса документе (п. 10 ст. 15.1).

Примечательно, что не любое обращение заявителя к должностному лицу будет подпадать под категорию личного приема. Данное утверждение разъясняется письмом Роспотребнадзора № 01/2555-8-32 2008 г., в котором отдельно упоминаются «обращения на личном приеме» и «иные устные консультации» (п. 7) [8]. Данные категории различаются по значению: только в первом случае информация заявителя заносится в карточку личного приема и может служить основанием для проведения контрольных мероприятий, рассматриваться в качестве основания для возбуждения уголовного дела либо дела об административном правонарушении.

При этом в действующем федеральном законодательстве понятие личного приема, его функции, цели и особенности отсутствуют. Такое положение дел влечет за собой отсутствие унифицированного подхода к проведению личного приема на региональном уровне, где происходит более детальное регулирование процедуры [9]. Это может негативно сказываться на осуществлении государственными и муниципальными органами, а также отдельными должностными лицами своих контрольно-разрешительных функций в сфере миграции.

Список литературы

1. Конституция РФ: принята всенародным голосованием 12 декабря 1993 г. // Собр. законодательства Рос. Федерации. 2014. № 31. Ст. 4398.
2. О статусе члена Совета Федерации и статусе депутата Государственной Думы Федерального Собрания Российской Федерации: федер. закон от 8 мая 1994 г. № 3-ФЗ (в ред. от 3 июля 2019 г.) // Собр. законодательства Рос. Федерации. 1994. № 2. Ст. 74.
3. О правовом положении иностранных граждан в Российской Федерации: федер. закон от 25 июля 2002 г. № 115-ФЗ (в ред. от 2 августа 2019 г.) // Собр. законодательства Рос. Федерации. 2002. № 30. Ст. 3032.
4. О порядке рассмотрения обращений граждан Российской Федерации: федер. закон от 2 мая 2006 г. № 59-ФЗ (ред. от 27 декабря 2018 г.) // Собр. законодательства Рос. Федерации. 2006. № 19. Ст. 2060.
5. Об организации предоставления государственных и муниципальных услуг: федер. закон от 27 июля 2010 г. № 210-ФЗ (в ред. от 1 апреля 2019 г.) // Собр. законодательства Рос. Федерации. 2010. № 31. Ст. 4179.
6. О Концепции государственной миграционной политики Российской Федерации на 2019–2025 годы: Указ Президента РФ от 31 октября 2018 г. № 622 // Собр. законодательства Рос. Федерации. 2018. № 45. Ст. 6917.
7. *Савоськин А. В.* Личный прием граждан: проблемы правового регулирования и практики реализации // Lex Russica. 2019. № 10 (155). С. 72.
8. Об оптимизации форм и методов работы по рассмотрению обращений потребителей: письмо Роспотребнадзора от 24 марта 2008 г. № 01/2555-8-32. URL: https://legalacts.ru (дата обращения: 01.12.2019).
9. *Савоськин А. В.* Правовые и организационные проблемы проведения личного приема граждан в России // Вестник Уральского юридического института МВД России. 2019. № 2. С. 64–65.

Ф. И. СТРЕЛЬНИКОВ,
начальник 5-го отдела
Вычислительного центра
(ФКУ «ГИАЦ МВД России»)

О некоторых аспектах управления системами больших данных

Характеристики больших данных, связанные с объемом, скоростью, разнообразием и изменчивостью, требуют универсальной платформы для хранения, обработки и управления сложными данными. Управление системами больших данных должно обрабатывать как системные, так и связанные непосредственно с самими данными аспекты среды больших данных. Структура управления большими данными включает две общие группы операций: управление системой и управление жизненным циклом больших данных. Управление системой включает в себя такие операции, как выделение ресурсов, конфигурирование, управление пакетами, управление программным обеспечением, управление резервным копированием, управление возможностями, управление ресурсами и управление производительностью. Управление жизненным циклом больших данных включает в себя сбор, подготовку/обработку, анализ, визуализацию и доступ.

Управление жизненным циклом больших данных представляет собой широкий спектр систем больших данных – от тесно связанных корпоративных решений, интегрированных посредством стандартных или собственных интерфейсов, до слабо связанных вертикальных систем, поддерживаемых различными заинтересованными сторонами или органами, связанными соглашениями, стандартными или де-факто стандартными интерфейсами. Поэтому в различных случаях применяются различные соображения и технические решения.

Инфраструктура больших данных может содержать устройства хранения данных SAN или NAS, облачные хранилища, базы данных NoSQL, кластеры распределения/свертки, функции аналитики данных, механизмы поиска и индексирования и платформы обмена сообщениями. Поддерживающая корпоративная вычислительная инфраструктура может быть традиционным центром обработки данных, облачным сервисом и рассредоточенными вычислительными узлами сети. Управление системой основывается:

– на стандартных протоколах, таких как простой протокол управления сетью (SNMP), которые используются для передачи компонентам матрицы управления информации о состоянии ресурсов и об отказах;

– развертываемых агентах или соединителях управления, которые позволяют матрице управления как контролировать, так и управлять элементами инфраструктуры.

Эти два элемента помогают отслеживать состояние различных типов вычислительных ресурсов и справляться с инцидентами, связанными с производительностью и сбоями, сохраняя при этом качество обслуживания, необходимое поставщику приложений больших данных. Соединители управления необходимы для сценариев, в которых поставщики облачных сервисов предоставляют возможности управления через API. В некоторых случаях элементы инфраструктуры содержат возможности автономной, самостоятельной настройки и самовосстановления, тем самым сокращая централизованную модель управления системой. В крупных инфраструктурах, содержащих много тысяч вычислительных узлов и узлов хранения данных, выделение средств и приложений должно быть максимально автоматизировано. Установка программного обеспечения, конфигурация приложений и регулярное обслуживание исправлений должны быть запущены и реплицированы по узлам автоматизированным образом на основе знаний о топологии инфраструктуры. С появлением виртуализации использование виртуальных образов может ускорить процесс восстановления и обеспечить эффективную установку исправлений (патчей), что позволит минимизировать время простоя при плановом обслуживании.

В корпоративной среде платформа управления обычно обеспечивает общекорпоративный мониторинг и администрирование распределенных компонентов больших данных. Это включает в себя управление сетью, управление отказами, управление конфигурацией, учет системных ресурсов, управление производительностью и управление безопасностью.

В свободно связанной вертикальной системе каждая независимая заинтересованная сторона несет ответственность за управление собственной системой, ее безопасность и интеграцию.

Управление жизненным циклом больших данных сталкивается с большим количеством проблем по сравнению с традиционным управлением жизненным циклом данных, которое требует меньших объемов передачи, обработки и хранения данных. Однако оно по-прежнему наследует фазы традиционного управления с точки зрения сбора, распределения, использования, миграции, технического обслуживания и удаления данных, но в значительно большем масштабе обработки. Поставщикам приложений больших данных может потребоваться гораздо больше вычислительных мощностей для сбора, подготовки/обработки, анализа, визуализации и доступа, чтобы иметь возможность использовать аналитические результаты. Другими словами, сфера управления жизненным циклом больших данных включает проверку правильности обработки данных другими компонентами эталонной архитектуры больших данных в каждом процессе в течение жизненного цикла данных – с момента их поступления в систему от Поставщика данных до тех пор, пока данные не будут обработаны или удалены из системы.

Важность управления жизненным циклом больших данных продемонстрирована посредством следующих соображений.

1. Объем данных может быть чрезвычайно большим, способным переполнить вместимость хранилища данных или сделать сохраняемые поступающие данные предельно дорогими.

2. Скорость данных – темп, с которым данные могут собираться и поступать в систему, может переполнить доступное место для хранения в любой момент времени. Даже с сервисом эластичного хранения, предоставляемого облачными вычислениями для обработки динамических потребностей хранения, неконтролируемое управление данными может также быть излишне дорогостоящим для определенных эксплуатационных требований.

3. У различных приложений больших данных, вероятно, будут различные требования времени жизни частей данных. Различные требования влияют на то, как часто данные должны обновляться, чтобы результаты обработки были действительными и полезными. При обновлении данных старые данные удаляются и не передаются в программы аналитики или обнаружения. В то же время новые данные воспринимаются и учитываются вычислениями. Например, для приложений в режиме реального времени потребуется очень короткое время жизни данных, однако исследование рынка интересов потребителей к линейке продуктов может потребовать сбора данных в течение продолжительного времени.

Поскольку задача управления жизненным циклом больших данных может быть распределена между различными организациями и/или отдельными лицами в вычислительной среде больших данных, координация обработки данных между компонентами эталонной архитектуры больших данных имеет большие трудности с соблюдением политик, правил и требований безопасности. В этом контексте управление жизненным циклом больших данных может потребовать включить следующие подпроцессы:

– управление политиками: фиксирует требования к жизненному циклу данных, которые позволяют распределять старые данные и рассматривать новые данные в приложениях больших данных. Поддерживает стратегии переноса и удаления, которые определяют механизм преобразования и размещения данных, включая перекодирование данных, передачу старых данных в хранилище нижнего уровня с целью архивирования, удаление данных или маркировку данных на месте;

– управление метаданными: активирует управление жизненным циклом больших данных после использования метаданных для сохранения информации, которая определяет управление данными в системе. Обязательная информация метаданных включает: постоянную идентификацию данных, фиксированность/качество и права доступа. Задача состоит в том, чтобы найти минимальный набор элементов

для эффективного выполнения требуемой стратегии управления жизненным циклом больших данных.

Вместе с тем в эталонной архитектуре больших данных в явном виде прослеживается междисциплинарный характер ее компонентов. Компоненты представляют функциональные роли в экосистеме больших данных. В разработке системы агенты и роли имеют те же отношения, как в фильмах, но агенты разработки системы могут представлять собой людей, организации, программное обеспечение или аппаратные средства. При этом единственный агент может играть несколько ролей и несколько агентов могут играть одну и ту же роль.

Однако для определенного варианта использования, когда роли связаны с определенными бизнес-заинтересованными сторонами, функциональные компоненты рассматриваются как внутренние или внешние – в зависимости от применяемого подхода. Также эталонная архитектура больших данных обеспечивает представление составления или объединения в цепочку систем больших данных. Например, потребитель данных одной системы мог служить поставщиком данных к следующей системе вниз по цепочке.

Основная ценность больших данных лежит в результатах исследований, которые помогают организациям выявлять паттерны, смысловые взаимосвязи, принимать решения и, наконец, интеллектуально реагировать на события. По мере развития технологий и расширения дискуссий организации будут разрабатывать все новые способы получения результатов, задействуя такие подходы к большим данным, которые до сих пор лежали за пределами возможностей основной деятельности организации.

Например, организации обращаются к прогнозному анализу, чтобы улучшить степень взаимодействия с заказчиками, оптимизировать процессы и сократить эксплуатационные расходы. Сочетание потоковой передачи данных в режиме реального времени и прогнозного анализа, которое иногда называется «безостановочной обработкой», может дать бизнесу значительное конкурентное преимущество.

Подходы к работе с системами больших данных в разных организациях могут существенно отличаться. Однако хотя бы несколько специалистов в области анализа данных должны работать внутри организации, поскольку заказчику важно уметь общаться с внешним подрядчиком на языке, который ему понятен. В случае применения 100-процентного аутсорсинга существует риск, что все будет решаться абсолютно верными средствами, но при этом изначально будут решаться «не очень правильные» задачи. При этом затраты на получение первичного результата в случае использования внешних ресурсов специалистов анализа данных будут существенно выше по сравнению с тем, что можно получить за счет использования внутренних ресурсов либо грамотного управления всем процессом в целом. Продвинутых специалистов по анализу данных можно задействовать на более поздних этапах, чтобы улучшить уже достигнутые результаты. Также будет видна

производительность работы внешних специалистов, так как им надо будет улучшить полученный собственными силами результат.

Необходимо понимать, что специалисты, занимающиеся анализом данных, довольно дорого стоят, и даже не с точки зрения абсолютной стоимости ресурса в рублях, а просто потому, что их время жалко тратить на рутинные задачи.

В сложившейся ситуации будет идеально добиться баланса сочетания использования внутренних ресурсов и аутсорсинга. В то же время не очень правильно, когда все сконцентрировано на внутренних ресурсах. Очевидно, что возникают ситуации, когда необходимо использовать большие технологические ресурсы, имеющиеся на внешнем рынке. И, по большому счету, для специалиста в области статистики и анализа данных неважно, как называется конкретная площадка, на которой он будет работать. Сегодня они могут заниматься, условно, металлами, а завтра – чем-то связанным с банковской деятельностью и при этом все равно обеспечивать нужный заказчику результат.

Нет особого секрета, откуда приходят такого рода специалисты, – это либо математическое, либо физическое профильное образование, те, кто по основной специальности занимался математикой либо математической статистикой. При прочих равных хорошими ориентирами могут являться мехмат МГУ, ВМиК (факультет вычислительной математики и кибернетики МГУ), МФТИ. Можно ожидать, что успешно окончившие их студенты окажутся вполне грамотными специалистами, даже если ранее и не занимались конкретной областью анализа данных.

Следует учитывать, что инициативы больших данных не могут формироваться в вакууме. ИТ-подразделение должно сформировать тесные партнерские отношения с руководителями функциональных департаментов и отделов, чтобы определять возможности больших данных и двигаться вперед в нужных направлениях и с необходимой поддержкой всей команды организации.

О. А. УЛЬЯНИНА,
ведущий научный сотрудник
отдела по исследованию проблем
отраслевого управления
научно-исследовательского центра,
кандидат социологических наук, доцент
(Академия управления МВД России)

Интеллектуальный анализ данных в сфере оценки эффективности профессиональной подготовки выпускников образовательных организаций МВД России

Ежегодно образовательные организации МВД России выпускают молодых специалистов, которые направляются в различные подразделения ОВД. Наличие объективной информации об успешности службы выпускников на начальном этапе их профессиональной деятельности дает возможность своевременно скорректировать образовательный процесс в соответствии с актуальными требованиями, предъявляемыми к профессиональному уровню кадров ОВД.

В целях изучения, прогнозирования и удовлетворения потребности ОВД в высококвалифицированных специалистах Волгоградская академия МВД России ежегодно проводит анкетирование руководителей экспертных, следственных и оперативных подразделений ГУ МВД России по Волгоградской области, а также анкетирование выпускников академии на предмет удовлетворенности качеством подготовки для осуществления оперативно-служебной деятельности [2].

Опрос руководителей и выпускников проводится через год после окончания образовательной организации. В период с 2007 по 2018 год в опросе приняли участие 319 руководителей и 348 выпускников Волгоградской академии МВД России, среди которых 200 юношей и 148 девушек. Среди опрашиваемых и оцениваемых 204 выпускника по специальности «Правовое обеспечение национальной безопасности», 53 – «Судебная экспертиза» и 91 – «Правоохранительная деятельность» 2008–2012 годов набора.

Опрос руководителей проводился по трем разделам [10]. В первом разделе оценивалась готовность выпускников к осуществлению профессиональной деятельности в качестве эксперта-криминалиста (следователя, оперуполномоченного) по видам профессиональной деятельности. Во втором разделе оценивались общекультурные, деловые и личностные качества выпускников [8]. В третьем разделе непосредственные руководители выпускников указывали недостатки и положительные стороны их подготовки. Анкета самоанализа выпускника имела аналогичную структуру.

Анализ отзывов руководителей следственных подразделений в отношении выпускников по специальности «Правовое обеспечение национальной безопасности» позволяет сделать вывод о высоком уровне профессиональной подготовки большинства молодых специалистов – 61 %, готовность 39 % выпускников к осуществлению профессиональной деятельности в качестве следователя оценивается на среднем уровне.

Высокий уровень готовности руководители отмечают по следующим видам профессиональной деятельности [9]:

– взаимодействие с работниками служб ОВД – 75 %;

– установление психологического контакта с участниками предварительного следствия, обеспечение информационной безопасности и режима секретности – 67 %;

– проведение очной ставки – 63 %;

– обеспечение прав и законных интересов участников предварительного следствия, допрос – 58 %;

– использование информационных технологий, криминалистических учетов, баз данных – 54 %.

Следует отметить, что общекультурные, деловые и личностные качества более чем у половины выпускников оценены руководителями на высоком уровне, оставшаяся часть – на среднем уровне. Так, среди выраженных компетенций, сформированных на высоком уровне у основной части выпускников, следующие:

– творческая инициатива в проблемных ситуациях, способность принимать решения – 75 %;

– способность к профессиональному и личностному саморазвитию – 74 %;

– осведомленность в событиях политической, социальной и экономической жизни государства – 73 %;

– культура устной и письменной речи – 72 %;

– адекватность самооценки и восприятия критики – 70 %;

– исполнительская дисциплина и ответственность – 69 %;

– нацеленность на соблюдение принципа законности, устойчивость к коррупционным проявлениям; ориентация на общечеловеческие ценности и принципы морали – 68 %;

– умение работать в коллективе и коммуникативные качества – 66 %;

– соблюдение профессиональной этики и субординации в подразделении – 62 %.

В ходе анализа анкет выпускников по специальности «Правовое обеспечение национальной безопасности» выявлено, что 98 % выпускников имеют высокий и средний уровень удовлетворенности знаниями по профильным дисциплинам: 69 % – высокий уровень, 29 % – средний уровень, 2 % – ниже среднего. 99,6 % выпускников имеют высокие и средние

показатели владения основными видами профессиональной деятельности. Из них 65 % отмечают высокий уровень навыков, 35 % – средний.

Общекультурные, деловые и личностные качества оценены выпускниками достаточно высоко. Общие результаты следующие: высокий уровень подготовки – 64 %, средний уровень подготовки – 36 %.

Высокий и средний уровень стремления продолжать службу в ОВД отметили 69 % и 31 % выпускников соответственно. Эти показатели соотносятся с мотивационной зрелостью: так, 68 % выпускников отмечают высокий уровень мотивации, а 12 % – средний. Порядка 68 % опрошенных считают, что уровень их подготовленности полностью соответствует квалификационным требованиям по приобретенной специальности и требованиям практики, 30 % указали на средний уровень такого соответствия, 2 % отметили уровень соответствия ниже среднего.

Указанные результаты подтверждаются результатами анкетирования руководителей следственных подразделений ГУ МВД России по Волгоградской области. Коэффициент парной корреляции Пирсона в среднем составляет 0,75, что позволяет говорить о прямой взаимозависимости оцениваемых показателей.

Выпускники отметили ряд направлений обеспечения образовательного процесса, требующих внимания со стороны педагогических работников:

– повышение доли практических занятий – 76 %;

– издание необходимой учебной литературы, методических материалов по отдельным дисциплинам – 32 %;

– повышение уровня материально-технического обеспечения образовательного процесса – 10 %;

– компьютеризация учебного процесса – 5 %.

Выпускники предлагают шире использовать в образовательном процессе методы моделирования различных следственных ситуаций, расширить перечень ситуационных задач по осмотру места происшествия, допросу с последующим составлением процессуальных документов [1].

Качество образовательных услуг по специальности «Правовое обеспечение национальной безопасности» оценили по десятибалльной шкале на 8,9 балла.

Результаты анализа отзывов руководителей экспертно-криминалистических центров указывают, что 60 % и 39 % выпускников по специальности «Судебная экспертиза» имеют соответственно высокий и средний уровень владения основными видами профессиональной деятельности, из них 78 % имеют высокий уровень владения производством почерковедческих экспертиз, 56 % – технико-криминалистических экспертиз, экспертиз холодного и метательного оружия. Почти у 80 % молодых специалистов непосредственные руководители отмечают средний уровень владения такими видами профессиональной деятельности эксперта-криминалиста, как производство баллистических и портретных экспертиз.

По мнению опрошенных руководителей, 89 % выпускников обладают средним уровнем ведения делопроизводства, обеспечения режима секретности, 78 % обладают средним уровнем ведения экспертно-криминалистических учетов и участия в качестве специалиста в осмотрах мест происшествий в целях обнаружения, фиксации, изъятия материальных следов.

Проанализировав все отзывы руководителей экспертно-криминалистических подразделений, можно сказать, что выпускники имеют достаточно высокий уровень готовности к осуществлению профессиональной деятельности в качестве эксперта-криминалиста.

Общекультурные, деловые и личностные качества выпускников по специальности «Судебная экспертиза» также, по мнению руководителей, в большинстве своем имеют высокий уровень сформированности. Так, среди выраженных качеств отмечены:

– способность к профессиональному и личностному саморазвитию – 79 %;

– соблюдение профессиональной этики и субординации в подразделении – 72 %;

– творческая инициатива в проблемных ситуациях, способность принимать решения – 70 %;

– устойчивость к коррупционным проявлениям – 66 %;

– осведомленность в событиях политической, социальной и экономической жизни государства – 64 %;

– ориентация на общечеловеческие ценности и принципы морали; способность применять в своей работе информационные технологии – 60 %;

– культура устной и письменной речи – 62 %;

– умение работать в коллективе – 58 %;

– нацеленность на соблюдение принципа законности; соблюдение служебной дисциплины и правил внутреннего распорядка в подразделении – 55 %;

– коммуникативные качества – 53 %.

На основе анализа отзывов руководителей можно сделать вывод, что в оценке профессиональной готовности выпускников они были достаточно требовательны, поэтому далеко не все выпускники имели высокую степень выраженности профессиональных качеств, остальная часть респондентов была оценена на уровне выше среднего и среднем.

На основании анализа анкет выпускников по специальности «Судебная экспертиза» 96 % респондентов имеют высокие и средние показатели владения основными видами профессиональной деятельности. Из них 56 % оценивают уровень владения профессиональными знаниями и навыками как высокий, 40 % – как средний.

Общекультурные, деловые и личностные качества выпускников по специальности «Судебная экспертиза» оценены выпускниками достаточно

высоко: так, 60 % выпускников оценили их на высоком уровне, 39 % – на среднем.

Стремление продолжать службу в ОВД изъявили 59 % выпускников. В равной степени проявляется мотивация к служебной деятельности у 62 % выпускников, 10 % опрошенных считают, что их представления о профессии не оправдались. В среднем 57 % опрошенных считают, что уровень их подготовленности полностью соответствует квалификационным требованиям по приобретенной специальности и требованиям практики, 43 % указали на средний уровень такого соответствия и на оправданность их представлений о профессии.

Результаты самоанализа выпускников и отзывов руководителей экспертно-криминалистических подразделений ГУ МВД России по Волгоградской области имеют положительную взаимозависимость – коэффициент парной корреляции Пирсона составляет 0,7.

Несмотря на общий положительный результат в образовательном процессе при подготовке по специальности «Судебная экспертиза» необходимо обратить внимание на следующие направления деятельности, которые указаны выпускниками в качестве проблемных аспектов:

– повышение доли практических занятий – 90 %;

– издание необходимой учебной литературы, методических материалов по отдельным дисциплинам (баллистическая экспертиза, ТКЭД) – 60 %;

– повышение уровня материально-технического обеспечения образовательного процесса и компьютеризация учебного процесса – 50 %.

В предметных областях у выпускников вызывают сложности следующие виды экспертиз:

– осмотр места происшествия при расследовании различных видов преступлений – 80 %;

– фиксация и изъятие следов и вещественных доказательств на месте происшествия – 60 %;

– производство трасологических, баллистических экспертиз и экспертизы холодного и метательного оружия – 50 %;

– ведение учетов и делопроизводство – 40 %.

Качество образовательных услуг по специальности «Судебная экспертиза» выпускники оценили по десятибалльной шкале на 9,2 балла.

В основном уровень готовности выпускников по специальности «Правоохранительная деятельность» к осуществлению профессиональной деятельности в качестве оперуполномоченного полиции оценивается руководителями оперативных подразделений как высокий – 59 % *и* средний – 40 %.

Наставниками оценен высокий уровень владения такими видами профессиональной деятельности выпускников, как:

– выполнение поставленных задач в составе группы – 88 %;

– выявление, предупреждение, пресечение и раскрытие преступлений и иных правонарушений – 76 %;

– соблюдение информационной безопасности и режима секретности, ведение дел оперативного учета – 75 %;

– обеспечение законности в профессиональной деятельности, умение использовать полученную информацию для борьбы с преступностью, использование в оперативно-служебной деятельности учетов, ведущихся в ОВД, исполнение судебных, прокурорских и иных решений, указаний, составление оперативно-служебных документов – 63 %.

У 61 % выпускников по специальности «Правоохранительная деятельность» общекультурные, деловые и личностные качества оценены руководителями на достаточно высоком уровне:

– умение работать в коллективе и коммуникативные качества – 87 %;

– способность к профессиональному и личностному саморазвитию – 68 %;

– творческая инициатива в проблемных ситуациях, способность принимать решения – 66 %;

– осведомленность в событиях политической, социальной и экономической жизни государства – 63 %;

– культура устной и письменной речи – 58 %;

– ориентация на общечеловеческие ценности и принципы морали; исполнительская дисциплина и ответственность – 56 %;

– адекватность самооценки и восприятия критики – 54 %;

– нацеленность на соблюдение принципа законности, устойчивость к коррупционным проявлениям – 52 %;

– соблюдение профессиональной этики и субординации в подразделении – 44 %.

Анализ результатов анкетирования выпускников по специальности «Правоохранительная деятельность» выявил, что около 82 % имеют высокие и средние показатели владения основными видами профессиональной деятельности. Из них 52 % отмечают высокий уровень знаний по профильным дисциплинам, 45 % – средний уровень и 3 % – низкий уровень знаний.

Практические навыки оценены выпускниками следующим образом: высокий уровень владения – 55 %, средний – 43 %.

Выраженное стремление продолжать службу в ОВД отметили 59 % выпускников, средний показатель – 41 %. Эти показатели соответствуют уровню мотивации: высокий у 57 %, средний у 42 %. В среднем 54 % опрошенных считают, что уровень их подготовленности полностью соответствует квалификационным требованиям по приобретенной специальности и требованиям практики, 46 % указали на средний уровень такого соответствия. Удовлетворенность профессией у 51 % выражена на высоком уровне, у 48 % – на среднем.

Указанные результаты подтверждаются результатами анкетирования начальников полиции оперативных подразделений ГУ МВД России по Волгоградской области. Коэффициент парной корреляции Пирсона в среднем составляет 0,70, что позволяет говорить о прямой взаимозависимости оцениваемых показателей.

Необходимо обратить внимание на следующие вопросы при подготовке обучающихся по специальности «Правоохранительная деятельность»:

– повышение доли практических занятий – 78 %;

– повышение уровня материально-технического обеспечения образовательного процесса – 11 %;

– издание необходимой учебной литературы, методических материалов по отдельным дисциплинам (по предварительному следствию, уголовному праву, уголовному процессу, по расследованию преступлений, связанных с незаконным оборотом наркосодержащих, психотропных и сильнодействующих веществ) – 11 %.

Выпускники рекомендуют обратить внимание на формирование практических навыков по ОРД и режиму секретности, производству отдельных следственных действий и составлению процессуальных документов, увеличить срок практики на 3-м курсе.

Качество образовательных услуг по специальности «Правоохранительная деятельность» оценили по десятибалльной шкале на 9 баллов.

Таким образом, из представленных анкет-отзывов руководителей экспертных, следственных и оперативных подразделений об уровне профессиональной подготовки выпускников академии мы видим, что она оценивается на высоком уровне. У оперуполномоченных полиции – это 59 % выпускников, у следователей – 61 %, у экспертов – 60 %.

Средний уровень подготовки наставниками отмечен у 39 % окончивших академию по специальности «Судебная экспертиза», «Правовое обеспечение национальной безопасности» и 40 % – «Правоохранительная деятельность».

В целом же руководители экспертных, следственных и оперативных подразделений отметили высокую мотивацию у выпускников академии к прохождению службы и профессиональному росту в ОВД, а также хорошее взаимодействие молодых специалистов с коллегами.

В то же время прослеживается низкий уровень владения такими направлениями деятельности, как:

– ведение работы по подбору граждан для оказания содействия ОВД – 29 %;

– выявление преступлений и иных правонарушений – 24 %;

– использование в работе информационных источников и ресурсов – 22 %;

– реализация мероприятий по получению значимой информации – 22 %;

– ведение дел оперативного учета – 19 %.

Результаты сравнительного анализа экспертной оценки руководителей и самооценки показали, что выпускники способны достаточно адекватно самостоятельно оценить уровень сформированности у себя необходимых компетенций. Данный вывод подтверждается итогами корреляционного анализа (самый низкий коэффициент корреляции составил 0,55).

Следует отметить, что в первый год службы у выпускников формируется социально-психологическая основа поведения, обеспечивающая успешность их последующего профессионального роста и карьеры [3; 4; 5; 6; 7]. В этой связи необходимым и значимым является осуществление системного анализа эффективности образовательной и психологической подготовки, результативности профессиональной деятельности выпускников образовательных организаций МВД России.

Список литературы

1. *Аветисян А. Д., Рясов А. А., Жигалова Г. Г.* Отдельные аспекты компетентностно-ориентированного обучения следователей в образовательных организациях системы МВД России // Мир науки, культуры, образования. 2019. № 1 (74). С. 5–6.

2. *Бадаев А. Г., Усачева И. В.* Социально-психологическое исследование профессиональной идентичности выпускника образовательного учреждения МВД России // Вестник Московского университета МВД России. 2017. № 1. С. 187–190.

3. *Базулина А. А.* Современные подходы к повышению качества высшего образования в системе МВД России // Актуальные вопросы совершенствования деятельности правоохранительных органов внутренних дел Российской Федерации. Тюмень, 2019. С. 14–16.

4. *Гривенная Е. Н.* Курсанты и слушатели образовательной организации МВД России как объекты системы потребительского мониторинга удовлетворенности образовательными услугами // Международный журнал психологии и педагогики служебной деятельности. 2018. № 4. С. 11–15.

5. *Зайцева Н. В.* Особенности адаптации молодых специалистов, выпускников образовательных учреждений МВД России к профессиональной деятельности // Прикладная психология и педагогика. 2016. Т. 1. № 2. С. 6–12.

6. *Исаев Р. А.* Инновационные аспекты подготовки к профессиональной деятельности курсантов и слушателей в высших учебных заведениях МВД России // Общество: социология, психология, педагогика. 2019. № 2. С. 88–90.

7. *Кустов П. В.* Вопросы успешной адаптации выпускников образовательных организаций МВД России к самостоятельной профессиональной деятельности // Материалы X Международной научно-практической конференции «European Scientific Conference» (Пенза, 7 июня 2018 г.). Пенза, 2018. С. 164–166.

8. *Михайлова Т. Н., Маланов И. А.* К вопросу определения понятия «Общекультурная компетентность курсанта вуза МВД России» // Научно-педагогическое обозрение. 2019. № 3 (25). С. 41–47.

9. *Медведицкова Л. В.* Профессионально значимые качества следователя: структура и содержание // Мир науки, культуры, образования. 2018. № 3 (70). С. 56–57.

10. *Пугач П. В., Лигута В. Ф.* Параметры готовности выпускников вузов МВД России к оперативно-разыскной деятельности // Ученые записки университета им. П. Ф. Лесгафта. 2015. № 2 (120). С. 130–133.

К. М. ХОЛОСТОВ,
заместитель начальника центра командно-штабных учений,
кандидат технических наук, доцент
(Академия управления МВД России)

Решение задач ситуационного анализа оперативной обстановки

Введение

Ситуационный подход в управлении сконцентрирован на рассмотрении текущей ситуации, в которой находится управляемый объект (система), на выборе варианта управленческого воздействия из имеющихся альтернатив, при этом выбор полностью определяется ситуацией [5, 8]. Существует такое обилие факторов как внутри самого управляемого объекта, так и в окружающей его среде, но не существует «абсолютно хорошего» управленческого решения, позволяющего применить единственно верное управляющее воздействие. Все решения имеют определенную степень близости к идеальному решению. И данная степень тем дальше, чем менее достоверны результаты анализа текущей ситуации и чем больше ошибка ее классификации. В связи с этим задача лица, принимающего решения (ЛПР), состоит в том, чтобы на основе всестороннего анализа определить подходящие приемы и методы преодоления возникших проблем, с учетом того, что результаты одних и тех же управленческих действий в различных ситуациях могут очень сильно отличаться друг от друга.

В связи с этим поиск модели, позволяющей эффективно различать различные типы ситуаций, формировать прототипы ситуаций, а затем устанавливать степень близости конкретной ситуации к одному или нескольким прототипам, – является ключевой задачей, требующей решения в рамках ситуационного управления.

Ситуационная осведомленность лица, принимающего решение

Очевидно, что одна из основных сложностей в применении методов ситуационного управления лежит именно в полном, адекватном описании ситуаций, а также в верном отнесении их к соответствующим классам. Органы внутренних дел являются сложной иерархической системой, функционирующей в постоянно изменяющихся условиях, в связи с чем на наличие полных аналогов ситуаций не приходится рассчитывать, это влечет за собой необходимость привлечения интеллектуальных методов принятия решений. В частности, перспективным представляется переход от анализа классических категорий явлений и процессов, основанных на отношениях эквивалентности, к методам когнитивной (семантической) категоризации [4], которые учитывают прототипичность ситуаций внутри

одного класса, а также используют семантические меры близости категорий, моделируемых в так называемых концептуальных пространствах [6].

Применимость общего метода ситуационного управления можно существенно повысить путем его адаптации к конкретным моделям предметных областей. В настоящее время для эффективного решения задач классификации ситуаций предложена концепция ситуационной осведомленности, которая описывает наиболее общие принципы подготовки и обработки информации для реализации ситуационного подхода в конкретных предметных областях [9]. Ситуационная осведомленность включает в себя осознание того, что происходит вне и внутри управляемого объекта, чтобы понять, как информация, события и собственные действия будут влиять на цели и задачи в текущий момент и в ближайшем будущем. Формальное определение СО разделяется на три компонента:

1) восприятие и оценка элементов внешней среды и внутренних факторов управляемой системы;

2) осознание и понимание ситуации;

3) прогноз будущего состояния управляемого объекта.

На всех этапах формирования СО присутствуют ошибки, которые ведут к накоплению обобщенной ошибки СО

$$\xi_{\Sigma осв} = \xi_{вос} + \xi_{пон} + \xi_{прог}, \quad (1)$$

где $\xi_{вос}$ – ошибка восприятия информации о внешних и внутренних условиях существования для управляемого объекта;

$\xi_{пон}$ – ошибка понимания ситуации и верного отнесения ее к классу по управлению;

$\xi_{прог}$ – ошибка прогноза изменения ситуации после применения управляющего воздействия.

Очевидно, что существует некая ошибка $\xi_{\Sigma осв0}$, которую ЛПР может принять в качестве допустимой. Тогда критерий допустимости ошибки СО будет

$$К_{СО} = \frac{\xi_{\Sigma осв}}{\xi_{\Sigma осво}}. \quad (2)$$

При этом значение $К_{СО} \leq 1$ для суммарной ошибки СО, допустимой ЛПР, и $К_{СО} > 1$ в случае превышения допустимого уровня ошибки.

Исследователями в области разработки систем СУ неоднократно показывалось [1, 6, 8, 9], что важны не абсолютные, а относительные значения СО. Исходя из этого, примем, что значения общей степени СО и каждой из трех ее компонент (восприятие элементов окружающей обстановки, понимание ситуации и прогноз будущего) характеризуются неотрицательным числом с максимальным значением, равным 1.

$$У_{СО} = У_{ВОС} * У_{ПС} * У_{ПБ}, \quad (3)$$

где $У_{ВОС}$ – уровень восприятия информации о внешних и внутренних условиях существования управляемого объекта, равный отношению количества τ контролируемых ЛПР показателей к общему количеству $(\tau + \mu)$

показателей, характеризующих условия существования управляемого объекта $У_{ВОС} = \frac{\tau}{\tau+\mu}$;

μ – не контролируемые ЛПР показатели;

$У_{ПС}$ – уровень понимания ситуации, выражается через меру близости реального текущего состояния управляемого объекта к идеальному. В системе СУ данная мера зависит от вектора невязок собственных критериев качества управляемого объекта $\vartheta_{вн} = \sqrt{\sum_j^{\tau}(\frac{y_i - y_{io}}{\Delta y_i})^2}$ и вектора невязок выходных показателей управляемого объекта $\alpha_{вх} = \sqrt{\sum_i^{\mu}(\frac{a_i - a_{io}}{\Delta a_i})^2}$;

$У_{ПБ}$ – уровень прогноза будущего, определяется скоростью изменения ситуации на управляемом объекте, т. е. приращениями $\Delta К_i$ значения критерия качества управления.

Критерий качества, в свою очередь, можно представить в виде:

$$K_{/} = \sqrt{\frac{1}{\mu}\sum_i^{\mu}(\frac{a_i - a_{io}}{\Delta a_i})^2 + \frac{1}{\tau}\sum_j^{\tau}(\frac{y_i - y_{io}}{\Delta y_i})^2}. \quad (4)$$

Оперативная обстановка как объект ситуационного анализа

Информационно-аналитическая функция в составе управленческой деятельности руководителя любой организационной структуры – одна из важнейших. Именно на ней базируются все остальные элементы управления: прогноз, принятие решений, организация исполнения, контроль и др.

Обратимся к специфике деятельности ОВД, где текущую ситуацию принято описывать в виде оперативной обстановки [3], которую можно рассматривать как комплексную характеристику конкретных ситуаций применительно к практике служебной деятельности ОВД, декомпозируемую следующим образом.

1. Внешние факторы – характеристика среды функционирования, за исключением криминальной обстановки, выделяемой в качестве специального фактора. В состав данных факторов входят общие показатели региона (включая географические, социально-экономические, демографические и социально-политические).

2. Специальный внешний фактор (по отношению к деятельности ОВД) – это фактор преступности и правонарушительства (криминальная обстановка).

3. Внутренние факторы (за исключением результатов деятельности ОВД) состоят из показателей информационного, кадрового, нормативно-правового и всех видов ресурсного обеспечения в рамках существующей структуры управления ОВД.

4. Результаты деятельности ОВД выделяются из состава внутренних факторов и включают в себя показатели, характеризующие результаты деятельности ОВД по основным направлениям.

Разнородный состав анализируемых данных затрудняет проведение анализа статистическими методами, применение методов кластерного и факторного анализа, поскольку неочевидность связей между теми или иными факторами не позволяет формировать связанные группы данных для последующего анализа. Анализ всех возможных связей нереализуем, поскольку их количество приведет к выявлению огромного числа истинных и ложных зависимостей, рассмотрение и попытка использования которых полностью дискредитирует результаты проводимого анализа. В этих условиях решением может стать предварительная обработка данных (преданализ), которая должна производиться с применением электронно-вычислительных машин, эффективных моделей и алгоритмов обработки больших данных.

Формально оперативную обстановку можно представить в виде открытого кортежа:

$$<B, X, R, Y; U>, \qquad (5)$$

где B – множество общих показателей региона (включая географические, социально-экономические, демографические и социально-политические);

X – множество показателей преступности и правонарушительства;

R – множество показателей информационного, кадрового, нормативно-правового и всех видов ресурсного обеспечения;

Y – множество результатов деятельности ОВД;

U – множество возможных управляющих воздействий со стороны ЛПР.

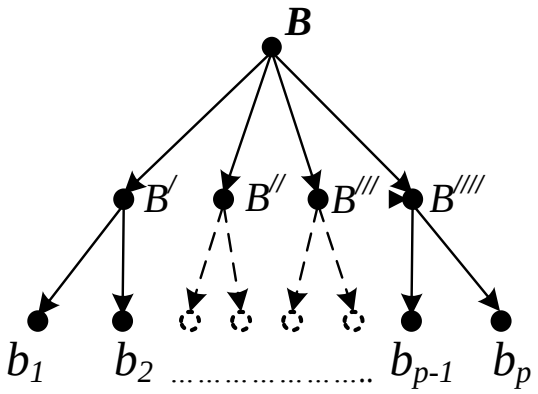

Рис. 1. Структура множества общих показателей региона

Представленный кортеж (5) отражает описанную выше модель оперативной обстановки. Наиболее объемной и сложной по составу является компонента B – множество общих показателей региона. Данное множество целесообразно представить в виде иерархического дерева (см. рис. 1), где корень узла – комплекс показателей региона (B), нетерминальные узлы –

в соответствии с функциональной схемой – укрупненные факторы (B', B'', B''', B''''), терминальные узлы – частные показатели (b_r, $r=1..p$) [2].

Анализ показывает, что определенная однородность и ограниченное число других элементов кортежа, таких как показатели преступности и правонарушительства (x_α), показатели информационного, кадрового, нормативно-правового и всех видов ресурсного обеспечения ОВД (r_β), результаты деятельности ОВД (y_γ), *а* также множество возможных управляющих воздействий со стороны ЛПР, вполне допускает их одноранговое отображение, а именно:

– показатели преступности и правонарушительства $x_\alpha \in X$, где $\alpha = 1\ldots v$; v – число показателей преступности и правонарушительства;

– показатели организационно-штатного, кадрового и всех видов ресурсного обеспечения $r_\beta \in R$, где $\beta = 1\ldots w$; w – число показателей внутренних факторов ОВД;

– показатели результатов деятельности ОВД $y_\gamma \in Y$, где $\gamma = 1\ldots g$; g – число показателей результатов деятельности ОВД;

– множество возможных управляющих воздействий ЛПР $u_k \in U$.

Применяемые сведения о состоянии общих показателей региона (B), показателей преступности и правонарушительства (X) неоднородны и обладают несколькими характерными различиями:

– различиями, возникающими за счет влияния отдельных факторов при неизменном влиянии других;

– структурными различиями объясняющих переменных, измеренных по интервальной или порядковой шкале.

Определенная однородность и ограниченное число показателей преступности и правонарушительства (X), показателей организационно-штатного, кадрового и всех видов ресурсного обеспечения (R), результатов деятельности ОВД (Y) вполне допускает их одноранговое отображение.

Следует отметить, что для целей анализа оперативной обстановки и дальнейшего принятия (выбора) управленческого решения из множества U значения конкретных показателей из множеств B, X, R, Y *не* имеют решающей роли. Достижению целевого состояния характера деятельности системы ОВД может способствовать только формирование адекватных выводов из оценки оперативной обстановки и построение основанных на анализе прогнозов ее развития. В связи с этим целесообразно подвергать анализу не абсолютные значения показателей, а набор из предлагаемых основных видов производных оценочных факторов.

1. *Относительный уровень показателя*, вычисляется (на примере общих показателей региона) как:

$$L(b_r) = b_r \Big/ \overline{b_r}, \tag{6}$$

где $\overline{b_r}$ – среднее значение данного показателя по субъекту Российской Федерации, федеральному округу или в группе однотипных территорий.

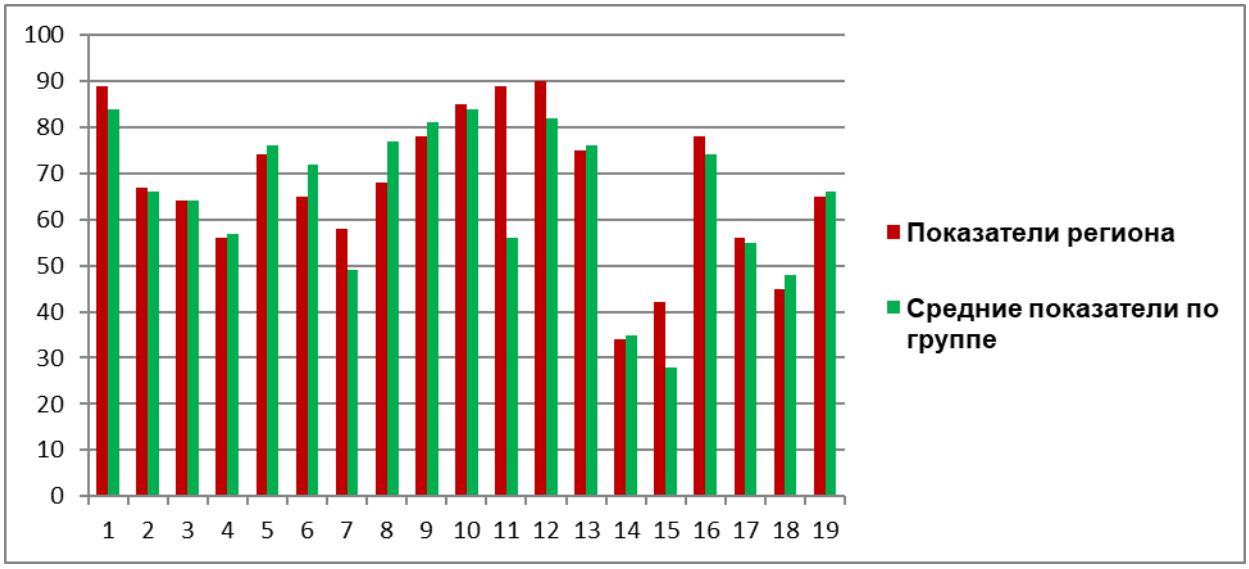

Рис. 2. Диаграмма показателей оперативной обстановки в сравнении со средними по группе

На диаграмме приведен пример сравнения значений показателей конкретного региона и среднерегиональных (групповых) значений для тех же показателей. Сравнительный анализ данных сведений позволяет установить текущее состояние оперативной обстановки с точки зрения наличия проблемных направлений в деятельности и особенностей региональной ситуации, опираясь на средние данные по аналогичным показателям соседних (входящих в одну группу) регионов или территорий.

2. Динамическая характеристика – *прирост значения* соответствующего показателя (на примере показателей преступности и правонарушительства) за отчетный период:

$$G(x_\alpha) = \frac{x_{\alpha 1} - x_{\alpha 2}}{x_{\alpha 1}}, \qquad (7)$$

где $x_{\alpha 1}$ – значение показателя преступности и правонарушительства в текущем отчетном периоде на обслуживаемой территории;

$x_{\alpha 2}$ – значение того же показателя преступности и правонарушительства в предыдущем отчетном периоде на той же территории.

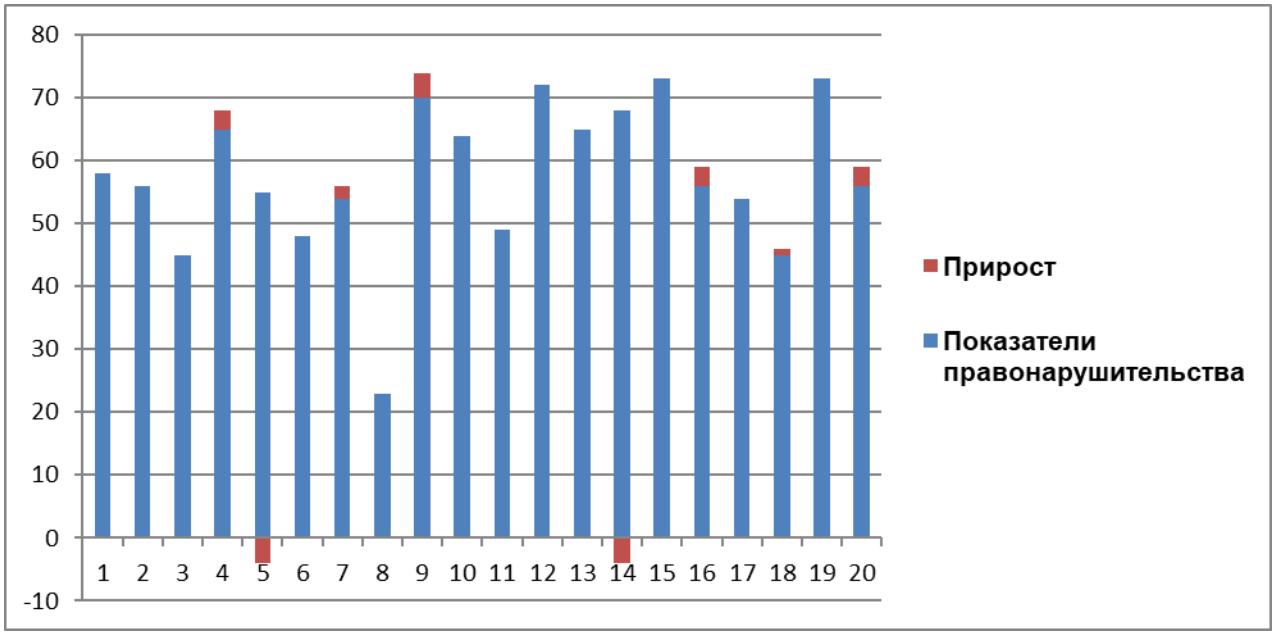

Рис. 3. Диаграмма изменений оперативной обстановки в части фактора правонарушительства

В зависимости от характера развития оперативной обстановки производный оценочный показатель $G(x_\alpha)$ может принимать как положительное, так и отрицательное значение. Во втором случае имеет место не прирост, а снижение уровня соответствующего показателя. При этом следует отметить, что характер изменения различных показателей имеет противоположное воздействие: одни показатели в случае увеличения ухудшают общую оценку оперативной обстановки, другие, наоборот, – увеличивают. В целях получения адекватной общей оценки следует учитывать негативный или позитивный характер влияния показателей.

Заключение

Прирост значений показателей в отчетном периоде дополнительно к оценке текущей ситуации дает возможность анализировать тенденции и направления изменения оперативной обстановки. На рис. 3 представлена диаграмма изменений оперативной обстановки, в качестве примера выбраны показатели преступности и административного правонарушительства. Из диаграммы видно, что отдельные показатели имеют тенденцию к росту, иные – к уменьшению. Объем прироста также может разниться – как по показателям, так и в динамике. Анализ прироста значений показателей дает возможность оценивания характера и объема изменений в оперативной обстановке за отчетный период.

Предложенные производные оценочные показатели позволяют успешно реализовать следующие задачи информационно-аналитического обеспечения процесса принятия управленческих решений:

– анализ значений относительных уровней всей совокупности показателей из множеств B, X, R, Y позволит сделать выводы о текущем состоянии оперативной обстановки на обслуживаемой территории в сравнении с аналогичными территориями;

– анализ значений относительных уровней отдельных показателей или группы показателей из множеств B, X, R, Y позволит сделать выводы о текущем состоянии соответствующих внешних и внутрених факторов, результатов деятельности ОВД, также в сравнении с аналогичными показателями соседних ОВД;

– рассмотрение прироста (снижения) значения отдельных показателей позволит выявить тенденции к улучшению либо к осложнению оперативной обстановки.

При наличии достаточного количества наблюдений (данных, соответствующих последовательным отчетным периодам) на основании комплексной оценки данных о приросте значения показателей и ускорении прироста значения показателя появляется возможность получать прогнозные значения по оцениваемым показателям.

Построение векторов невязок, состоящих из совокупности относительных значений показателей оперативной обстановки, позволяет типизировать ситуации, формировать прототипы ситуаций, служащие базой для их классификации или поиска фрагментов совпадений.

Список литературы

1. *Гонов Ш. Х., Макаров В. Ф., Гурлев И. В.* Модель анализа оперативной обстановки на основе производственной функции Кобба-Дугласа // Вестник Воронежского института ФСИН России. 2018. № 3. С. 57–64.
2. *Горошко И. В., Гонов Ш. Х.* Разработка алгоритма оценки результатов деятельности органов внутренних дел с использованием моделей бинарного выбора // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 2 (21). С. 368–378.
3. *Клушин О. З.* Оперативная обстановка: понятие, анализ, прогноз: учеб. пособие. М., 2010.
4. *Кучуганов В. Н.* Ассоциативная семантика ситуаций и сюжетов // Искусственный интеллект и принятие решений. 2014. № 2. С. 42–51.
5. *Поспелов Д. А.* Ситуационное управление: теория и практика. М., 1986.
6. *Фридман А. Я.* Концептуальные пространства как средство оценки ситуационной осведомленности при моделировании динамических иерархий // Вестник Кольского научного центра РАН. 2018. № 1 (10). С. 98–108.
7. *Холостов К. М.* Методы и алгоритмы работы автоматизированных комплексов подготовки руководителей органов внутренних дел. М., 2016.
8. *Холостов К. М.* Понятие ситуации в контексте управления в правоохранительной сфере // Вестник Воронежского института МВД России. 2016. № 2. С. 191–202.

9. *Endsley M. R.* Situation awareness: progress and directions // A cognitive approach to situation awareness: theory and application. Aldershot, 2004. P. 317–341.

А. М. ЦЕПКО,
слушатель Академии управления МВД России

В. Ю. ПЕТРОВА,
доцент кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

Основные проблемы предоставления государственных услуг в ОВД в электронном виде и пути их решения

Из всех задач, которые выполняют ОВД, самой важной является предоставление услуг гражданам в электронном виде.

Государственные услуги – это услуги, которые предоставляют органы государственной власти и неправительственные организации в порядке выполнения делегированных полномочий [1, с. 11].

По субъектам, которые несут ответственность с точки зрения поддержки процесса предоставления услуги, государственные услуги делятся на: полностью автоматизированные (электронные услуги), автоматизированные частично, услуги, выполняемые вручную [2, с. 59].

Электронные государственные услуги – это услуги, которые предоставляются органами государственной власти физическим и/или юридическим лицам через электронные средства связи с использованием информационно-коммуникативных технологий и являются основой электронного управления в России.

Вопросу о предоставлении государственных услуг в ОВД в электронном виде уделено недостаточно внимания. Поэтому важным является исследование особенностей предоставления государственных онлайн-услуг ОВД России [3, с. 61].

Важно понимать, что составление и закрепление перечня государственных услуг, предоставляемых ОВД России в электронном виде, и четкая регламентация соответствующих административных процедур имеют целью не только упорядочение общественных отношений в заданном направлении, четкое распределение прав и обязанностей сторон, но и (что наиболее важно) создание качественного механизма эффективного взаимодействия государства как поставщика услуг (с одной стороны) и гражданина как потребителя этих услуг (с другой). При такой постановке проблемы ее решение предполагает необходимость смещения акцентов с жесткой регламентации перечня предоставляемых документов на результат: обращаясь в государственный орган за предоставлением услуги (и при этом часто оплачивая стоимость такой процедуры), гражданин имеет цель приобрести соответствующее благо в виде услуги или юридической фиксации административного акта (фактически – получение документа). Для

удовлетворения требований гражданина в рамках административной процедуры законодатель устанавливает перечень документов, которые ему надлежит предоставить в соответствующий орган (организацию) [4, с. 28].

Вместе с тем отечественное законодательство об административных процедурах в значительной степени отличается отсутствием гибких механизмов, позволяющих оказывать такие услуги в электронном виде в условиях отсутствия реальной возможности со стороны гражданина к выполнению требуемых от него действий (предъявлению документов). Решение такого рода проблем в организации деятельности ОВД России по оказанию административных процедур, полагаем, находится в плоскости дальнейшего совершенствования их нормативного регулирования в части предоставления государственным органам и организациям дополнительной возможности самостоятельного истребования информации и документов из иных государственных органов и организаций, если лицо, обратившееся за оказанием такой услуги, лишено реальной возможности личного предоставления соответствующих сведений [5, с. 213].

Совершенствование процедур обжалования отказа в оказании или некачественного оказания государственной услуги в контексте по-прежнему бытующего мнения о закрытости ОВД РФ обусловливает актуализацию вопроса перевода государственных услуг в электронную форму, связанного с реализацией проекта «Электронное правительство» и последующим переходом к концепции «Электронное государство». Важнейшим требованием последней выступает критерий проактивности государственных услуг, предполагающий следование правилу: все необходимые документы должны запрашиваться по единому идентификатору из электронных реестров государственных органов.

Реализация системы мер государственной программы «Электронное правительство» (а впоследствии и «Электронное государство») в контексте требования комплексного решения жизненных ситуаций гражданина на основании автоматизированных бизнес-процессов (сервисов), полагаем, предусматривает осуществление дальнейшего менеджеринга таких услуг на плановой основе посредством принятия программного документа, определяющего векторы развития правоохранительной системы, – концепции. Вместе с тем рассмотрение функций оказания государственных услуг ОВД в контексте субъектного состава правоохранительных органов позволяет констатировать, что в отличие от иных государственных органов в системе правоохранительных структур такие услуги нередко реализуются посредством категории государственных служащих, осуществляющих свою профессиональную деятельность в рамках военизированного вида государственной службы [6, с. 105].

Учитывая, что отличительной чертой государственных услуг в электронном виде, отграничивающей их от иных функций государственных органов, является их несвязанность с властно-распорядительными полномочиями, ситуация возложения таких функций на служащих

военизированных видов государственной службы в качестве основного направления их деятельности видится не только неоправданной, но и недопустимой. Данный вывод основан на очевидности, на наш взгляд, того факта, что сам статус служащего военизированной службы (с вытекающими из него социально-правовыми гарантиями) определяется не внешними атрибутами профессии, а содержанием – правоохранительным характером служебной деятельности, ее интенсивностью и рисковой предрасположенностью [7, с. 59].

Отмеченная особенность может вызвать вопрос об обоснованности включения таких услуг в систему выполняемых этими органами функций защиты человека и гражданина, интересов общества и государства от преступных и иных противоправных посягательств. Следует ли из этого, что приведенные выше обязанности могут образовывать специфическую функцию? Анализ позволяет рассматривать оказание таких услуг в качестве одного из направлений деятельности современной системы ОВД. Однако в отличие от иных функций ОВД, обладающих ярко выраженным правоохранительным характером, функция оказания государственных услуг по своему содержанию является в большей степени регулятивной, хотя и сохраняет при этом общие признаки правоохранительной, обладая правоохранительным потенциалом [1, с. 9].

Качественная работа по закреплению перечня таких функций и определению категорий лиц правоохранительных органов, которые могут и должны на постоянной основе осуществлять такие функции, будет способствовать определению направлений оптимизации и экономии бюджетных средств [8, с. 93]. Этому же будет способствовать определение в системе военизированных организаций категории должностей, которые могли бы быть переведены в аппаратную (гражданскую) государственную службу. В основу такой оптимизации должен быть положен ответ на вопрос о том, выполнение каких функций (охранительных или регулятивных) будет в основе служебно-должностных обязанностей сотрудника [5, с. 212].

Такая характеристика системы функций ОВД позволяет вести речь о целесообразности перевода в аппаратную (гражданскую) государственную службу должностей, основным видом деятельности которых является техническое обслуживание средств и систем охраны, документирование населения, обследование объектов и выдача рекомендаций по организации, осуществлению и совершенствованию их охраны, а также решение задач информационно-регистрационного характера и ряда других. Разрешение вопроса о совершенствовании процесса оказания правоохранительными органами государственных услуг в электронном виде при определенной степени их формализации затрагивает проблему их качества и обоснованности конкретными условиями.

В частности, наличие такого критерия оценки подразделений охраны ОВД РФ, как статистические данные о количестве подобранных и принятых под охрану объектов, способно привести к решению сотрудниками

несвойственных для строевых подразделений ОВД РФ задач (например, организация пропуска транспортных средств на территорию негосударственной организации, физическая охрана имущества коммерческой организации) [7, с. 56].

Такие задачи вполне разрешимы (и при этом за счет отсутствия необходимости обеспечения персонала дополнительными социальными льготами, например льготным периодом выхода на пенсию, – экономически эффективны) посредством гражданского персонала (сторожевого состава) территориальных подразделений ОВД РФ, иных государственных органов и организаций. Необходимо также учитывать, что следование отмеченному статистическому критерию ведет и к увеличению штатной численности строевых подразделений ОВД РФ. Потребность в обеспечении исполнения взятых на себя обязательств по охране объектов всех форм собственности сегодня обусловливает качественное снижение требований к кандидатам на службу в подразделения охраны.

Отмеченные обстоятельства возникли вследствие отсутствия системного подхода к качеству оказываемых услуг, а также нормативно определенных критериев, связывающих возможность их оказания с конкретными условиями. Решение данной проблемы предполагает разработку стандартов государственных услуг в электронном виде, что может быть реализовано путем поэтапного совершенствования действующей системы правового регулирования порядка и условий их оказания [2, с. 61].

Резюмируя сказанное, необходимо сделать следующие выводы:

1) государственные услуги в электронном виде, реализация которых возложена на ОВД РФ, необходимо рассматривать в системе функций таких государственных органов;

2) отечественное правовое регулирование государственных услуг в электронном виде, реализация которых возложена на ОВД РФ, носит непоследовательный характер, что связано не столько с отсутствием легальной дефиниции понятия «государственные услуги», сколько с отсутствием гибкости системы и механизма реализации таких услуг;

3) учитывая, что отличительной чертой государственных услуг в электронном виде, отграничивающей их от иных функций государственных органов, является несвязанность их с властно-распорядительными полномочиями, ситуация возложения таких функций на служащих военизированных видов государственной службы в качестве основного направления их деятельности является неоправданной, так как статус служащего военизированной службы определяется ее правоохранительной направленностью, интенсивностью и рисковой предрасположенностью;

4) совершенствование системы государственных услуг в электронном виде, оказываемых ОВД, предполагает разработку комплекса мер организационно-правового характера, осуществляемых на концептуальной основе на уровне стратегического планирования.

Итог. Эффективный менеджеринг таких услуг предполагает расширение их перечня и преимущественный перевод в электронную форму, а также оптимизацию их субъектного состава. Перспективными направлениями развития государственных услуг в электронном виде необходимо признать внедрение автоматизированной информационной системы обжалования действий и решений должностных лиц ОВД РФ; дальнейшее развитие межведомственного информационного взаимодействия в сфере оказания государственных услуг в электронном виде, масштабное внедрение электронных форм подачи заявлений на получение (истребование) государственных услуг.

Список литературы

1. *Грищенко А. Н.* Проблемы регламентации функции предоставления государственных услуг в сфере внутренних дел // Государство и право. 2019. № 3. С. 5–12.
2. *Нагоша В. А., Осяк А. Н., Капранова Ю. В.* Организационные основы предоставления государственных услуг в сфере обеспечения безопасности дорожного движения Министерством внутренних дел Российской Федерации // Юристъ-Правоведъ. 2019. № 1 (88). С. 55–64.
3. *Охохонин Е. М., Полищук Н. А.* Сервис электронного документооборота Единой системы информационно-аналитического обеспечения МВД России: вопросы реализации // Правоохранительные органы: теория и практика. 2019. № 1. С. 59–62.
4. *Безруков А. В., Савоськин А. В.* Особенности реализации в органах внутренних дел Российской Федерации конституционного права граждан на обращение // Юридическая наука и правоохранительная практика. 2019. № 2 (48). С. 25–35.
5. *Олимпиев А. Ю., Михайленко Н. В.* Проблематика предоставления государственных услуг полицией // Вестник Московского университета МВД России. 2019. № 4. С. 212–215.
6. *Затолокин А. А.* Предоставление государственных услуг ГИБДД в электронном виде // Общество и право. 2019. № 2. С. 102–105.
7. *Трунцевский Ю. В.* Предотвращение и урегулирование конфликта интересов в органах внутренних дел // Труды Академии управления МВД России. 2019. № 1 (49). С. 55–60.
8. *Линевич В. Л.* Формирование антикоррупционного поведения у сотрудников органов внутренних дел: психолого-педагогические аспекты // Вестник Уфимского юридического института МВД России. 2019. № 1 (83). С. 92–97.

А. Г. ЧИННОВ,
слушатель 2-го факультета
(Академия управления МВД России)

В. Ю. ПЕТРОВА,
доцент кафедры информационных технологий,
кандидат технических наук, доцент
(Академия управления МВД России)

Применение технологий анализа больших данных в оценке состояния служебной дисциплины и законности в ОВД

Анализ обзоров состояния служебной дисциплины и законности в органах и подразделениях внутренних дел вызывает серьезную обеспокоенность, поскольку происходит увеличение количества правонарушений со стороны личного состава: 2013 – 181 010; 2014 – 182 336; 2015 – 182 817; 2016 – 196 081; 2017 – 197 840; 2018 – 202 232. Основными причинами такого положения, по мнению руководства МВД России, являются: чрезмерная текучесть кадров в ОВД, ранняя профессиональная деформация сотрудников, снижение интеллектуального уровня кандидатов на службу в ОВД, недооценка необходимости воспитания чувства дисциплинированности у сотрудников полиции, отсутствие системного подхода к реализации воспитательных мер, направленных на повышение качества служебной дисциплины, недостаточная ориентация сотрудников на повышение уровня своей личной дисциплинированности.

Ключевым субъектом данной деятельности является руководитель подразделения (органа, организации) в сфере внутренних дел. Более того, на него возложена персональная ответственность за работу по укреплению служебной дисциплины и законности среди личного состава [1].

Данный вид деятельности руководителя в правовых документах МВД России определяется как комплексный вид морально-психологического обеспечения, представляющий собой ряд мероприятий, направленных на профилактику, предупреждение правонарушений и чрезвычайных происшествий (Методические рекомендации ДГСК МВД России от 10 октября 2018 г. № 21/8/10998), а именно:

– организация работы по предупреждению правонарушений и чрезвычайных происшествий среди личного состава;

– поддержание установленного порядка и правил осуществления служебной деятельности;

– повышение повседневной требовательности руководителей всех уровней к подчиненному личному составу в сочетании с уважением личного достоинства сотрудников и постоянной заботой о них;

– создание для сотрудников ОВД социально-бытовых условий, обеспечивающих высокую культуру труда;

– изучение причин и условий, способствующих совершению правонарушений личным составом, в ходе служебных проверок; организация взаимодействия с органами местного самоуправления, общественными объединениями по вопросам обеспечения служебной дисциплины и законности в деятельности ОВД [2].

Однако реализация данных положений возможна исключительно при решении руководителем территориального ОВД таких задач, как: обеспечение неукоснительного соблюдения сотрудниками требований Конституции РФ, законодательства федерального уровня при выполнении оперативно-служебных задач и в повседневной жизни; поддержание правопорядка, обеспечение правильного и точного исполнения сотрудниками требований нормативных правовых актов; воспитание у личного состава сознательного отношения к гражданскому и служебному долгу сотрудника ОВД; формирование правового сознания и высокой правовой культуры, выработка навыков служебной деятельности, соответствующих правовым нормам служебной дисциплины и профессионально-этическим правилам поведения; обеспечение личной ответственности каждого сотрудника за исполнение своих обязанностей, требований служебной дисциплины и законности, норм профессиональной этики; достижение соразмерности дисциплинарных мер воздействия совершенному проступку, индивидуализации дисциплинарной ответственности с учетом особенностей личности сотрудника, его прежнего поведения; создание условий для сохранения жизни и здоровья личного состава.

Определить приоритетные направления сосредоточения управленческих ресурсов руководителю призвана помочь аналитическая работа, заключающаяся в соответствующем сборе, обработке, систематизации, анализе и оценке информации о состоянии служебной дисциплины и законности, причинах и условиях совершения проступков личным составом.

По формам анализ состояния служебной дисциплины и законности делится на общий – характеризующий ее состояние в целом по территориальным органам МВД России и частный – по службам и подразделениям территориального органа МВД России, а также по линиям отдельных служб.

Итогом анализа является объективное определение на основе достоверных сведений и истинного положения дел на данном участке оперативно-служебной деятельности степени соответствия осуществляемой работы с личным составом предъявляемым современным требованиям, а также оценка роли каждого руководителя в воспитании своих подчиненных [3].

Порядок количественного и качественного учета совершаемых сотрудниками нарушений служебной дисциплины и законности в целом

определен в приложениях к приказу МВД России от 31 июля 2011 г. № 747 «Об утверждении форм статистической отчетности».

Основным содержанием анализа должно быть определение, в какой степени состояние служебной дисциплины и законности способствует выполнению основных оперативно-служебных задач ОВД.

Учитывая, что в соответствии с Указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» вектор развития современного российского общества определен как цифровой, возникает необходимость внедрения технологий больших данных как основного элемента эволюции системы государственного управления. Система ОВД не исключение, что влечет необходимость рассмотрения процессов социального взаимодействия (в том числе дисциплинарных отношений руководитель – подчиненный) через призму различных социально-экономических, процессуальных и иных показателей, сбор и обработка которых осуществляется всеми органами государственной власти на различных уровнях. Тем самым повышается точность прогнозирования процессов, происходящих в служебных коллективах, появляется возможность моделирования кризисных ситуаций с выработкой решений, повышающих эффективность системы ОВД в целом.

На сегодняшний день анализ данных о состоянии служебной дисциплины и законности в ОВД включает:

– систематизацию и классификацию данных о состоянии служебной дисциплины и законности в подразделениях за определенный период;

– выяснение количества и характера правонарушений, допущенных сотрудниками, изучение индивидуальных особенностей сотрудников, социально-психологической обстановки в коллективе, их взаимосвязи с причинами правонарушений;

– общую оценку состояния служебной дисциплины и законности среди личного состава в подразделении;

– общую оценку работы по профилактике нарушений служебной дисциплины и законности [4].

Однако система ОВД не замкнута сама в себе и подвержена влиянию многочисленных внешних и внутренних факторов. Изучение вопросов возникновения негативных тенденций в организации личным составом соблюдения служебной дисциплины и законности разумно рассмотреть с позиции межведомственного взаимодействия, а именно перекрестного сравнения ключевых показателей, таких как:

– численность населения – штатная численность органа – показатели, характеризующие условия функционирования, – уровень экономического развития региона;

– количество нарушений служебной дисциплины – укомплектованность/ сменяемость руководителей;

– стаж службы сотрудников – образовательный уровень сотрудников;

– допущенные нарушения законности – количество возвращенных прокурором дознавателям/следователям дел для производства дополнительного расследования [5].

Вышеуказанный список возможных вариаций перекрестного исследования статистических показателей далеко не полный, однако позволяет взглянуть на процессы организации соблюдения личным составом ОВД служебной дисциплины и законности с позиций диффузного взаимодействия различных аспектов жизни общества – экономического, демографического, процессуального и т. д.

Результаты подобных исследований больших данных позволят выйти на более высокий качественный уровень прогнозирования в деятельности ОВД, а также осуществлять перераспределение сил и средств таким образом, чтобы решать поставленные задачи максимально эффективно с привлечением оптимального количества ресурсов.

Подобное высокоорганизованное управление возможно исключительно при положительном состоянии служебной дисциплины, т. е. при форме организации служебной деятельности, где сотрудники профессионально подготовлены, инструктированы, способны к сотрудничеству и работе без непосредственного и постоянного руководства. В отношении отдельных из них дисциплинарные меры применяются не как механизм наказания, а как механизм исправления, например дополнительная подготовка или обучение.

Список литературы

1. Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации: приказ МВД России от 1 февраля 2018 г. № 50 // СТРАС «Юрист».
2. Основы работы по укреплению служебной дисциплины и законности в органах внутренних дел: учеб. пособие / под общ. ред. канд. пед. наук В. Л. Кубышко. М., 2008.
3. Основные формы и методы анализа состояния служебной дисциплины и законности в органах внутренних дел Российской Федерации: метод. рекомендации. М., 2015.
4. Воспитательная работа с личным составом органов внутренних дел: пособие / под ред. А. А. Прошина. М., 2000.
5. Математические методы в современных социальных науках: учеб. пособие / Г. В. Осипов, В. А. Лисичкин. М., 2017.

А. В. ШАПКИН,
начальник управления информационных технологий
(ДИТСиЗИ МВД России)

И. А. КУБАСОВ,
профессор кафедры информационных технологий,
доктор технических наук, доцент
(Академия управления МВД России)

В. В. КОНЮШЕВ,
главный специалист
(СТиС МВД России)

МВД России: дорога к искусственному интеллекту

Выполнение комплекса мероприятий, направленных на применение искусственного интеллекта, является одной из важнейших задач реализации в системе МВД России государственной политики в области развития информационного общества и цифровой экономики.

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы[37], утвержденной Указом Президента РФ [5], особо выделяются объекты критической информационной инфраструктуры, в частности информационные системы и информационно-телекоммуникационные сети государственных органов, что имеет непосредственное отношение к информационной инфраструктуре МВД России. Этот важнейший документ также дает определение понятию «обработка больших объемов данных», из которого следует, что большие данные – это структурированная и неструктурированная информация, поступающая из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации в объемах, которые невозможно обработать вручную за разумное время.

Искусственный интеллект и технологии искусственного интеллекта занимают особое место в совокупности подходов, инструментов и методов автоматической обработки больших данных, направленных на устранение противоречия между большим количеством данных и современными возможностями использования их в реальном времени, в том числе в оперативно-служебной деятельности ОВД.

Ключевое понятие «искусственный интеллект» на протяжении последних трех десятилетий неоднократно претерпевало существенные изменения. В государственных стандартах [9-11] оно определялось сначала

[37] Далее – Стратегия развития информационного общества.

как «способность вычислительной машины моделировать процесс мышления за счет выполнения функций, которые обычно связывают с человеческим интеллектом» [9], затем – как «моделируемая (искусственно воспроизводимая) интеллектуальная деятельность мышления человека» [10] и, наконец, – как «способность функционального блока выполнять функции, обычно ассоциирующиеся с интеллектом человека, такие, как, например, рассуждения и обучение» [11].

В настоящее время очевидно, что в ключевых определениях функциональные составляющие, независимо от степени сходства процессов искусственного и естественного интеллектов, обладают значительно большей репрезентативностью.

В Национальной стратегии развития искусственного интеллекта на период до 2030 года сделан следующий шаг: искусственный интеллект рассматривается как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека». То есть акцент сделан именно на результатах выполнения когнитивных функций, а не на самих функциях. При этом имитация когнитивных функций человека рассматривается в контексте решения конкретных задач, а не как цель создания искусственного интеллекта.

О такой тенденции в развитии понятия искусственного интеллекта в мировой практике свидетельствуют соответствующие исследования, нашедшие свое отражение в ряде работ [12, 13 и др.]. Все это указывает на необходимость уточнения терминологических дефиниций в данной области.

Производное понятие «технологии искусственного интеллекта» определено в Стратегии развития искусственного интеллекта как «технологии, основанные на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта» [8]. В свою очередь, о перспективных методах искусственного интеллекта говорится как о направленных «на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) искусственного интеллекта (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объемов данных, обработка информации на основе новых типов вычислительных систем, интерпретируемая обработка данных и другие методы)».

Приоритетные результаты, на достижение которых направлено развитие и использование технологий искусственного интеллекта,

спроецированные на сферу деятельности ОВД, представляются в следующем виде:

– повышение эффективности процессов планирования, прогнозирования и принятия управленческих решений;

– автоматизация рутинных (повторяющихся) операций, связанных с обработкой информации;

– использование автономного интеллектуального оборудования и робототехнических комплексов, интеллектуальных систем автоматизированного управления;

– повышение безопасности сотрудников при выполнении оперативно-служебных задач (включая прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья);

– повышение лояльности и удовлетворенности граждан в получении государственных услуг, предоставляемых МВД России;

– оптимизация процессов подбора и обучения кадров, составления оптимального графика работы сотрудников с учетом различных факторов.

Стратегия развития искусственного интеллекта [8] предусматривает два основных этапа организационного, технического и кадрового обеспечения решения задач в области искусственного интеллекта:

– первый этап (2010–2024 гг.): создание инфраструктуры поддержки отечественных организаций, осуществляющих деятельность в области искусственного интеллекта, включая создание высокопроизводительных центров обработки данных; разработка российских микропроцессоров, не уступающих мировым аналогам по скорости и энергоэффективности; существенное увеличение числа граждан, имеющих компетенции в области искусственного интеллекта и в смежных областях его использования, в том числе аспирантов и специалистов в области искусственного интеллекта, имеющих ученую степень; Российская Федерация должна стать привлекательной для трудоустройства квалифицированных специалистов в области искусственного интеллекта, в том числе в связи с высоким уровнем заработной платы и созданием благоприятных условий для работы;

– второй этап (2024–2030 гг.): широкое предоставление функционирующих образцов микропроцессоров с комплектом соответствующего программного обеспечения; открытие специализированных центров обработки данных на основе российских микропроцессоров; введение в обращение на соответствующем товарном рынке интеллектуальных устройств, в которых используются такие микропроцессоры; разработка принципиально новых типов архитектур вычислительных систем и регистрация интеллектуальных прав на них; реализация образовательных программ мирового уровня для подготовки высококвалифицированных специалистов и руководителей в области искусственного интеллекта; обеспечение выхода российских

образовательных организаций высшего образования на лидирующие позиции в мире по направлениям в области искусственного интеллекта.

Необходимыми для решения задач в области искусственного интеллекта направлениями являются: разработка и развитие программного обеспечения, повышение доступности и качества данных, повышение доступности аппаратного обеспечения. В настоящее время ряд внешних и внутренних факторов обуславливают необходимость дальнейшего развития ИСОД МВД России.

Основными внешними факторами выступают:

– рост технического, научного и финансового потенциала преступной среды, усиление угроз терроризма, незаконной миграции;

– вступление мирового сообщества в четвертую научно-техническую революцию, основным содержанием которой является глобальное развитие информационно-телекоммуникационных систем на основе перспективных информационно-коммуникационных технологий и цифровых средств связи;

– недостаточно эффективное планирование и использование результатов фундаментальных и прикладных исследований, научно-технологических разработок в области перспективных информационно-коммуникационных технологий, выполняемых за счет государственного бюджета;

– слабое развитие конкурентной среды в сфере проведения научно-исследовательских и опытно-конструкторских работ;

– недостаточное количество квалифицированных кадров по техническим специальностям в системе МВД России.

Основными внутренними факторами являются:

– построение большинства сервисов ИСОД МВД России с использованием разнородных технологических решений, зачастую излишне усложненных и дорогостоящих как при разработке, так и в процессе дальнейшей эксплуатации;

– использование практически всеми реализованными в настоящее время сервисами ИСОД МВД России локальных баз данных, содержащих рассогласованную и дублирующуюся информацию (одну и ту же справочную информацию, имеющую разную кодификацию, а также списки физических и юридических лиц, транспортных средств и других объектов учета, совместно используемых во многих подразделениях МВД России);

– отсутствие интеграции унаследованной инфраструктуры упраздненной ФМС России с инфраструктурой ИСОД МВД России, а также иных ведомственных информационных систем, разработанных и введенных (не введенных) в эксплуатацию;

– отсутствие единой аппаратно-программной платформы ИСОД МВД России, обеспечивающей возможность оперативного проведения поиска и комплексного анализа накопленной разнородной информации;

– нереализованность в полной мере мероприятий по переходу на российское и (или) свободно распространяемое с открытым исходным

кодом программное обеспечение, а также на использование российской микроэлектроники;

– отсутствие ведомственного документа, определяющего направления дальнейшего развития ИСОД МВД России.

В МВД России осуществляются мероприятия по развитию единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы, а также инициативные научно-исследовательские работы по темам «Исследование путей применения методов искусственного интеллекта для анализа больших данных и поддержки принятия решений при проведении оперативно-разыскной деятельности» и «Исследование путей применения робототехнических комплексов (систем) в правоохранительной деятельности на базе перспективных информационно-коммуникационных технологий». Кроме того, разрабатывается понятийный аппарат, необходимый для реализации единого научного подхода к применению перспективных информационных технологий в интересах МВД России.

Мероприятия по реализации дальнейшего развития ИСОД МВД России направлены на решение следующих задач: выработку единых подходов к формированию способов предоставления информации в ИСОД России, в том числе в виде единого информационного пространства и единой системы классификации и кодирования информации; создание в рамках ИСОД МВД России единого аналитического механизма, представляющего возможность проведения оперативного поиска и комплексного анализа накопленной разнородной информации; интеграцию разрозненных ведомственных информационных систем, баз данных и программно-технических комплексов; оптимизацию и реструктуризацию потоков информации, аккумулируемой в ОВД.

Реализация основных направлений дальнейшего развития ИСОД МВД России на 2020–2024 годы проходит поэтапно.

2020–2021 годы – создание базовых сервисов, а также сервисов аналитической обработки данных, внешнего взаимодействия и обеспечения контроля документов, планов и поручений МВД России; повышение доли использования отечественного и свободно распространяемого программного обеспечения; совершенствование системы защиты информации ИСОД МВД России; утверждение технических требований и проекта строительства центров обработки данных.

2022–2023 годы – создание конструктора учетов и сервиса обработки биометрических данных ИСОД МВД России; интеграция в ИСОД МВД России сервиса обработки геопространственных данных и ведомственных информационных систем, разработанных и введенных в эксплуатацию; повышение доли использования отечественного и свободного распространяемого программного обеспечения; организация создания центров обработки данных.

2024 год – создание единой аппаратно-программной платформы ИСОД МВД России; профессиональная подготовка и переподготовка специалистов по эксплуатации и сопровождению информационных и телекоммуникационных систем, а также средств и систем защиты информации; совершенствование правовых, нормативно-технических, организационно-методических и иных основ в сфере разработки, внедрения, эксплуатации и развития ИСОД МВД России и ее компонентов; миграция данных ведомственных информационных систем на единую аппаратно-программную платформу ИСОД МВД России; создание основного и резервного центров обработки данных.

Специфика применения технологий искусственного интеллекта в МВД России обусловлена многоплановостью и разнородностью правоохранительной деятельности. Принципиально разные цели ставятся в сфере экономики и в секторе обеспечения общественной безопасности. Бизнес-процессы направлены на достижение максимальной прибыли, соответственно, структура задач и проблемы в области совершенствования бизнес-процессов [14] существенно отличаются от задач и проблем правоохранительной, в частности оперативно-служебной, деятельности подразделений МВД России.

В докладе исследовательского центра британской полиции по вопросам использования больших данных делается акцент на том, что полицейские операции, как правило, «уникальны и этим отличаются от массового посещения магазинов» и других рыночных отношений. То есть прямой перенос технологий искусственного интеллекта, разрабатываемых и применяемых в настоящее время в экономике, в правоохранительный сегмент невозможен.

Кроме того, в исследованиях зарубежных ученых и специалистов отмечается: в ближайшие несколько лет можно ожидать, что малые группы или одиночки будут способны к совершению преступлений масштаба, затрагивающего не отдельных граждан, а целые графства и города страны. Это в корне меняет саму философию полиции. Полицейские обязаны не столько раскрыть преступление или разыскать преступника, сколько на основе достоверных данных спрогнозировать возможность совершения преступления и пресечь его еще на подготовительной стадии. Превентивные полицейские меры невозможны без больших данных, которые являются основой предиктивной аналитики, становящейся в центр практической полицейской деятельности [16].

Эффективный анализ собранных данных, а тем более предиктивная (прогнозная) аналитика на их основе требуют применения соответствующих технологий искусственного интеллекта. Зарубежные аналитики говорят о «гибридном» искусственном интеллекте, когда в синергии человека и компьютера осуществляются практические процессы применения знаний, извлекаемых из больших данных.

Использование полицейской робототехники, в свою очередь, требует применения технологий искусственного интеллекта различных уровней.

Применение результатов автоматизированной обработки больших данных, использование виртуальных роботов (ботов) и физической робототехники (роботов) в реальной деятельности влечет за собой ряд проблем этического и юридического характера.

Стивен Л. Моррис, заместитель директора ФБР, в своем докладе «Искусственный интеллект: ФБР и полиция против преступников» [16] отметил следующие три типа этических проблем, порождаемых применением искусственного интеллекта и неразрывно связанной с ним робототехники: этические вопросы программирования искусственного интеллекта (просчеты программистов и ошибки в составлении алгоритмов); этические вопросы результатов и выводов, полученных искусственным интеллектом (интерпретация результатов в условиях, когда затруднен или невозможен перевод на язык, понятный человеку, глубинных процессов аналитики); этические вопросы действий людей, принимающих решения на основе информации искусственного интеллекта.

В области правовых норм наиболее остро стоят вопросы, связанные с отсутствием возможности определить, кого винить в жертвах либо материальном ущербе, вызванных человеческими решениями, принятыми под воздействием искусственного интеллекта, либо понесенных в результате действий автономных роботизированных систем.

Выводы.

1. Дорога к применению искусственного интеллекта в МВД России лежит через поэтапное приведение технических, кадровых, юридических и организационных составляющих деятельности в соответствие с мировыми тенденциями применения искусственного интеллекта в правоохранительном сегменте информационной экосистемы.

2. Особенности правоохранительной деятельности определяют специфику применения технологий искусственного интеллекта в МВД России и обусловливают невозможность прямого переноса опыта использования искусственного интеллекта из сферы бизнеса.

3. Критическими вопросами развития и внедрения технологий искусственного интеллекта в МВД России являются вопросы профессиональной подготовки кадров и совершенствования аппаратно-программного обеспечения.

Список литературы

1. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // СПС «Гарант».
2. О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ // СПС «Гарант».
3. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (одобрена решением Президента РФ от 23 ноября 1995 г. № Пр-1694).

4. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).
5. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. № 203).
6. Программа «Цифровая экономика Российской Федерации» (утв. распоряжением Правительства РФ от 28 июля 2017 г. № 632-р).
7. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента РФ от 7 мая 2018 г. № 204 // СПС «Гарант».
8. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента РФ «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 г. № 490).
9. ГОСТ 5971-90. Государственный стандарт. Системы обработки информации. Термины и определения. М., 1991.
10. ГОСТ Р 43.0.5-2009. Национальный стандарт Российской Федерации. Информационное обеспечение техники и операторской деятельности. Процессы информационно-обменные в технической деятельности. Общие положения. М., 2010.
11. ГОСТ 33707-2016 (ISO/IEC 2382:2015). Межгосударственный стандарт. Информационные технологии (ИТ). Словарь. М., 2016.
12. *Буренок В. М., Дурнев Р. А., Крюков К. Ю.* Разумное вооружение: будущее искусственного интеллекта в военном деле // Известия Российской академии ракетных и артиллерийских наук. 2018. № 2 (102). С. 11–21.
13. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход. М., 2006.
14. *Зайнетдинов Э.* 30 бизнес-процессов, которые изменятся из-за искусственного интеллекта. URL: https://hype.ru/deecrypto-store-club/30-biznes-processov-kotorye-izmenyatsya-iz-za-iskusstvennogo-intellekta-dkvza585 (дата обращения: 27.11.2019).
15. *Трофимов В. В.* Искусственный интеллект в цифровой экономике // Известия СПбГЭУ. 2019. № 4 (118).
16. Обзор отдельных вопросов в области больших данных и искусственного интеллекта / под ред. В. С. Овчинского. М., 2019.

А. В. ШЕВЦОВ,
заместитель начальника кафедры управления деятельностью подразделений обеспечения охраны общественного порядка центра командно-штабных учений, кандидат юридических наук, доцент (Академия управления МВД России)

Применение в образовательной деятельности специализированных модулей сервиса охраны общественного порядка ИСОД МВД России

Чтоб стать, говорят, человеком –
Шагать нужно в ногу с Веком!

Ю. Энтин

Разрабатываемое методическое обеспечение образовательного процесса отражает грядущие изменения законодательства с учетом утвержденной 10 июня 2019 г. Концепции нового Кодекса РФ об административных правонарушениях (далее – КоАП) [4], одновременно определившей кратчайшие сроки разработки соответствующего кодифицированного акта. В науке исследованы риски, возникающие в ходе реформирования современного законодательства [2, с. 36-40]. Причем с точки зрения государственного (публичного) управления особый интерес представляет мнение ученых, доказывающих целесообразность уточнения административно-процессуальной компетенции ОВД [1, с. 27-32].

Это не только диктует объективную необходимость научного осмысления и анализа сложившейся практики применения ныне действующих административно-правовых норм [3, с. 141-163], но и требует активизации методического и практического взаимодействия профессорско-преподавательского состава образовательных организаций системы МВД России с должностными лицами, осуществляющими административную деятельность. Результатом такого взаимодействия должна стать, в частности, стабильность нового правового регулирования отношений в сфере реализации административной ответственности [5, с. 5-9].

Совершенствованию методики обучения слушателей может способствовать подключение виртуальных полигонов Академии управления к Сервису обеспечения охраны общественного порядка (далее – СООП), функционирующему на базе ИСОД МВД России. Это позволило бы на более высоком и качественном уровне разрабатывать практические занятия.

Концепция построения общесистемного сервиса предусматривает реализацию сервис-ориентированной архитектуры для автоматизации прикладных задач, реализуемых в сфере обеспечения правопорядка и безопасности. Принципиально новой является технология «облачных

вычислений», проявляющаяся в обеспечении повседневного и удобного сетевого доступа по требованию к общему пулу конфигурированных вычислительных ресурсов, оперирующих самым широким спектром информации об административной практике.

СООП ИСОД МВД России состоит из 5 профильных модулей: «Административная практика» (введен в эксплуатацию с 1 мая 2016 г.), «Административный надзор» (с 15 января 2017 г.), «Участковый» (с 1 апреля 2018 г.), «Изолятор» (с 20 июня 2010 г.), «Инспектор ПДН» (с 1 августа 2018 г.). Общее количество пользователей всех перечисленных модулей составляет более 85 тыс., включая более 300 пользователей подразделений центрального аппарата МВД России (ГУОООП, ГУТ, ГУОБДД, ГУУР, УОРИ, ГИАЦ).

В модуле «Административная практика» (16,6 тыс. пользователей) заведено порядка 78,3 млн (100 %) учетных записей о лицах, совершивших административные правонарушения (ежедневно вводится порядка 25 тыс. дел об административных правонарушениях).

В модуле «Административный надзор» (8,5 тыс. пользователей, или 100 %) внесены сведения в отношении 114,3 тыс. поднадзорных лиц, а также 157,9 тыс. лиц, формально подпадающих под административный надзор.

В модуле «Участковый» (37,7 тыс. пользователей, или 76,7 %) содержатся сведения о состоянии оперативно-служебной деятельности на 28,6 тыс. (59,6 %) административных участков, в том числе о лицах, состоящих на профилактических и списочных учетах.

В модуле «Инспектор ПДН» (10,8 тыс. пользователей, или 77 %) заведена информация, характеризующая состояние профилактики безнадзорности и правонарушений несовершеннолетних на 6,1 тыс. территорий обслуживания инспекторского состава подразделений по делам несовершеннолетних.

В отличие от действующих систем СООП ИСОД МВД России предусматривает построение централизованной системы инфраструктуры на базе центров обработки данных (ЦОД). Немаловажным является и то, что совокупность информационных взаимодействий операторов СООП ИСОД МВД России гарантирует не только полноту информационной поддержки деятельности сотрудников подразделений, обеспечивающих охрану общественного порядка, но и безусловное соблюдение требований по обеспечению информационной безопасности. В результате обеспечен централизованный учет административных правонарушений по всей стране, сведений о нарушителях общественного порядка на объектах спорта. Налажено электронное взаимодействие с Государственной информационной системой о государственных и муниципальных платежах в целях передачи сведений о наложенных административных штрафах и осуществления контроля за их оплатой.

Так, при повторном совершении административных правонарушений появилась возможность устанавливать наличие признаков преступлений с административной преюдицией [6].

Формируются и автоматически заполняются статистические отчеты (по ведомственной форме «1-АП», 4МВ-НОН).

Запущен электронный обмен информацией с ведомственными сервисами (Госавтоинспекции – «ФИС ГИБДД-М», дежурных частей – «СОДЧ», организационно-штатных подразделений – «СОШП», а также с системами учета оборота оружия «СЦУО» и банками данных подразделений по вопросам миграции в части получения паспортных и иных регистрационных сведений).

Совместно с заинтересованными подразделениями Министерства производится дальнейшая модернизация СООП, что будет способствовать улучшению профилактической работы ОВД в отношении правонарушений.

Таким образом, порядок использования СООП ИСОД МВД России в настоящее время определяется специальным методическим алгоритмом действий должностных лиц ОВД, проводящих проверки по заявлениям и сообщениям, содержащим признаки вышеуказанных противоправных деяний [6].

В этом смысле применение методических возможностей виртуальных полигонов образовательной организации позволит моделировать учебные задачи-ситуации, предусматривающие отработку навыков принятия управленческих решений, основанных на анализе сведений:

– о лицах, привлеченных к административной ответственности, в том числе при проведении массовых мероприятий;

– о повторном совершении административных правонарушений, в том числе с обозначением возможного наличия признаков составов преступлений с административной преюдицией.

Кроме того, интеграция соответствующего программного обеспечения даст возможность слушателям (адъюнктам, курсантам) освоить умения и навыки использования электронных бланков процессуальных документов, предусмотренных КоАП, а также составления ежеквартальных статистических отчетов по ведомственной форме 1-АП «Сведения об административной практике органов внутренних дел Российской Федерации».

Список литературы

1. *Дугенец А. С.* Административная деликтность в России: состояние, динамика и средства противодействия // Административное право и процесс. 2004. № 1.

2. *Конев А. Н.* Идеологические риски затянувшейся судебной реформы // Юридическая техника. 2019. № 13.

3. *Шевцов А. В. и др.* Совершенствование системы административных наказаний и порядка их назначения: учеб. пособие. М., 2019.
4. Концепция нового Кодекса Российской Федерации об административных правонарушениях. URL: http://static.government.ru (дата обращения: 10.06.2019).
5. *Милехин В. А., Семенистый А. В., Николаев А. Г., Шевцов А. В., Ускова А. С.* Административная юрисдикция органов внутренних дел: учеб.-метод. пособие. М., 2017.
6. Алгоритм порядка применения норм законодательства об ответственности за противоправные деяния, совершенные лицами, подвергнутыми административному наказанию (указание ГУОООП МВД России от 13 февраля 2017 г.).

М. В. ШЕКОВ,
референт по особым поручениям отдела обеспечения деятельности ведомственных интернет-ресурсов (Управление по взаимодействию с институтами гражданского общества и средствами массовой информации МВД России)

Б. А. ТОРОПОВ,
доцент кафедры информационных технологий, кандидат технических наук, доцент (Академия управления МВД России)

История создания, общественная потребность и перспективы развития официальных интернет-ресурсов МВД России

1. Введение

Министерством внутренних дел РФ уделяется пристальное внимание информационному обеспечению деятельности правоохранительной системы, основной целью которого является формирование позитивного образа стража закона, повышение уровня общественной поддержки.

Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» ориентировал систему МВД России на прямой диалог с общественностью и средствами массовой информации, открыл новые возможности для взаимодействия и сотрудничества. Так, в соответствии со ст. 8 Закона деятельность полиции «является открытой для общества в той мере, в какой это не противоречит требованиям законодательства Российской Федерации», т. е. открытость и публичность признаны основными принципами деятельности ОВД.

Публичность выражается в том, что функции, возложенные законодательством РФ на ОВД, осуществляются исключительно в интересах личности, общества и государства. Открытость предполагает широкий доступ граждан ко всем видам документированной информации, если это не противоречит требованиям законодательства. ОВД, в свою очередь, получают новые возможности для коммуникации (обратной связи) с населением.

Задачи коммуникации двояки:

– с одной стороны, поддержание положительного общественного мнения у граждан о проводимой государством политике и формирование позитивного имиджа органов государственной власти;

– с другой стороны, получение государственными органами информации о реальных нуждах и заботах граждан, необходимой для эффективного оказания им услуг со стороны государства.

Целью коммуникации государственных структур с гражданами является обеспечение адекватного реагирования населения в целом

и влиятельных социальных субъектов в частности на деятельность конкретного органа власти, а также реагирования органа власти на требования со стороны граждан.

Необходимо отметить, что органы государственной власти в процессе осуществления информационной политики являются как субъектами, так и объектами. Это обусловлено тем, что без активного информационного отклика общества на управленческие решения, без демонстрации согласия членов общества процесс однонаправленного воздействия государства на общество не может быть в полной мере эффективным.

Среди основных задач коммуникационной деятельности ОВД следует выделить:

– мониторинг публикаций, пропагандирующих преступную деятельность (экстремизм, детское насилие и пр.);

– реагирование на негативные ситуации, результатом которых могут стать репутационные потери Министерства;

– закрепление в массовом сознании образа полицейского как высокопрофессионального защитника прав и интересов граждан;

– освещение фактов мужества и героизма, проявленных сотрудниками ОВД при выполнении служебного долга.

Важнейшую роль в решении указанных задач играют подразделения информации и общественных связей территориальных органов МВД России (далее – ИиОС), осуществляющие работу по формированию положительного имиджа сотрудника полиции, освещению в СМИ и в Интернете результатов деятельности правоохранительной системы по пресечению преступлений и правонарушений.

До недавнего времени основное место в процессе коммуникации органов государственной власти с населением занимали традиционные СМИ – газеты, журналы, радио и телевидение. В конце XX в., с развитием Интернета, ситуация резко изменилась – появились и стали активно развиваться электронные СМИ, что повлияло и на способы коммуникации государственных структур с гражданами.

В условиях повсеместного проникновения интернет-технологий в жизнь человека сложно переоценить роль ведомственных интернет-ресурсов в информационном сопровождении деятельности МВД России.

Под интернет-ресурсами Министерства подразумеваются развернутый в глобальной сети аппаратно-программный комплекс «Официальный интернет-сайт МВД России», мобильное приложение «МВД России», а также официальные аккаунты в социальных сетях и на популярном видеохостинге YouTube.

2. Аппаратно-программный комплекс «Официальный интернет-сайт МВД России»

Основополагающим нормативным правовым актом, регламентирующим выход МВД России в сеть Интернет, является Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа

к информации о деятельности государственных органов и органов местного самоуправления».

Правовая база, определившая контент официальных интернет-сайтов подразделений МВД России, берет свое начало с 10 августа 2011 г. – со дня опубликования Указа Президента № 1060, в котором изложен Перечень информации, доступной к размещению Министерством внутренних дел Российской Федерации в сети Интернет.

В ноябре 2011 г. вышел ведомственный приказ о порядке размещения Министерством информации в сети Интернет, а в составе Управления общественных связей был создан отдел интернет-ресурсов, в задачи которого вошла реализация всех требований приказа, включая организацию данной работы в центральном аппарате и в территориальных органах МВД России.

На момент создания единого ведомственного интернет-ресурса в активе был интернет-сайт mvd.ru, который с 2003 г. велся в инициативном порядке Объединенной редакцией МВД России как дополнительный публикационный ресурс. Также в наличии имелись отдельные сайты у отдельных подразделений Министерства в ряде регионов России.

Учитывая масштаб поставленных задач, появилась идея создания не множества разрозненных сайтов, а комплекса унифицированных ведомственных сайтов, связанных между собой.

В результате проведенной работы 14 января 2013 г. был введен в промышленную эксплуатацию аппаратно-программный комплекс «Официальный интернет-сайт МВД России», объединивший на общей технической платформе интернет-сайты территориальных органов МВД России, подразделений центрального аппарата и управлений на транспорте, образовательных, медицинских организаций в системе МВД России, а также отделов полиции на районном уровне.

На момент запуска численность интернет-сайтов в АПК составляла 102. В целях оказания методической помощи, обучения сотрудников, допущенных к работе в АПК, а также координирования деятельности по реализации имиджевых акций МВД России в УОС МВД России была создана Группа администрирования АПК.

Вопросы хостинга и администрирования для сайтов в АПК были решены централизованно без привлечения бюджетных средств, что явилось немаловажным фактором в условиях ограниченного финансирования.

В настоящее время АПК, будучи размещенным в Интернете, администрируется посредством ИСОД МВД России. Головной сайт и кольцо сайтов АПК размещены в центре обработки данных (ЦОД).

Официальный интернет-сайт МВД России – это одновременно и комплекс интернет-ресурсов, и сервис ИСОД МВД России, предназначенный для обеспечения доступа граждан через сеть Интернет к информационным ресурсам Министерства посредством использования современных информационных технологий.

Отличительной особенностью интернет-сайтов в составе АПК является одновременная работа администраторов структурных компонентов АПК, вертикальное и встречное распространение новостного контента, наличие мультимедийных возможностей с опорой на специальное хранилище – Медиабанк, а также наличие широкого круга интерактивных возможностей, таких как онлайн-сервисы различных типов, федеральные и региональные опросы пользователей сайта, онлайн-голосования, прямые интернет-трансляции и, что крайне важно, – онлайн-обсуждения через форму обратной связи.

С помощью интернет-сайтов граждане получают доступ не только к новостной информации, но и к онлайн-сервисам МВД России по предоставлению государственных услуг, в том числе касающихся вопросов миграции, деятельности ГИБДД, работы участковых, дежурных частей территориальных отделов полиции.

Так, в 2018 г. к ведомственным интернет-ресурсам обратились более 3 млн граждан, из которых 1,2 млн – за информацией об оказываемых государственных услугах по линии ГИБДД, более 1 млн посетили страницы с информацией об услугах по вопросам миграции, более полумиллиона граждан обращались за информацией об участковых уполномоченных полиции.

Наибольшей популярностью у посетителей интернет-сайта МВД России в 2018 г. пользовались разделы по вопросам миграции, такие как: «Гражданство РФ» (317 тыс.), «Оформление загранпаспорта» (308 тыс.), «Выдача разрешения на временное проживание» (240 тыс.), «Выдача вида на жительство» (216 тыс.), «Осуществление миграционного учета» (168 тыс.), «Выдача паспорта гражданина РФ» (140 тыс.), «Оформление приглашения на въезд в РФ» (128 тыс.) и другие.

С вводом функции создания новых интернет-сайтов в домене мвд.рф по состоянию на 1 октября 2019 г. в АПК «Официальный интернет-сайт МВД России» входит более 950 сайтов.

В рамках проводимой работы по администрированию АПК на новостной ленте сайта в текущем году опубликовано около 8 тыс. материалов, количество посетителей составило 5,7 млн.

3. Социальные медиа МВД России

«Социальные медиа» – термин относительно новый, и единого подхода к его определению среди научной общественности к настоящему времени не сложилось. Тем не менее представляется возможным выделить основополагающий признак в понимании электронных социальных медиа – это двусторонний характер коммуникационного влияния.

Так, например, Б. Солис предлагает следующее определение: «…социальные медиа в самом общем виде – это способ, при помощи которого люди обнаруживают, читают и комментируют новости, информацию и содержание. Это слияние социальной составляющей

и высоких технологий, трансформирующих монолог (от одного ко многим) в диалог (многие ко многим)»[38].

С точки зрения коммуникационной составляющей АПК «Официальный интернет-сайт МВД России» существенно уступает по оперативности информационного воздействия и востребованности размещаемой информации социальным медиа, которые способны собирать аудиторию, сопоставимую по численности с аудиторией традиционных СМИ, а зачастую и превышающую таковую.

По результатам исследования, проведенного Институтом маркетинговых исследований gfk.com, проникновение Интернета (в части использования социальных сетей) среди молодежи и людей среднего возраста близко к 100 % от их количества (более 73 млн человек), сегодня рост аудитории Интернета происходит в основном за счет людей старшего возраста[39].

Данные Фонда общественного мнения свидетельствуют о том, что большинство интернет-пользователей отдают предпочтение поиску и распространению информации, а также непосредственному общению с людьми. Соответственно, та часть присутствующей в соцсетях аудитории (более 80 %), которая сама не создает новости (твиты, посты и пр.), читает чужие сообщения, переходит по рекомендованным ссылкам и вступает в инициированные дискуссии[40].

По данным Statista, активнее всего в нашей стране используют YouTube (63 % опрошенных), второе место занимает «ВКонтакте» – 61 %. Глобальный лидер Facebook лишь на четвертой строчке с показателем в 35 %[41].

Это, безусловно, необходимо учитывать при формировании концепции работы МВД России с медиаресурсами.

Интерес органов государственной власти к использованию социальных медиа, таких как Twitter, Facebook, «ВКонтакте», Instagram, YouTube, в работе по информированию граждан о своей деятельности обусловлен рядом обстоятельств:

– затраты при использовании социальных медиа включают лишь издержки по созданию и поддержке аккаунта;

– социальные медиа, ввиду своей популярности, позволяют производить мониторинг реакции пользователей на действия и решения органов государственной власти;

---

[38] Как стать компанией новой волны, создавая эмоции, привлекающие клиентов. URL: https://www.mann-ivanov-ferber.ru/books/makrotrendy_v_biznese/ (дата обращения: 12.07.2020).

[39] URL: https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/Press_Releases/2019/GfK_Rus_Internet_Audience_in_Russia_2018.pdf (дата обращения: 12.07.2020).

[40] URL: https://fom.ru/SMI-i-internet/13999 (дата обращения: 12.07.2020).

[41] Социальные сети в 2018 году: глобальное исследование. URL: https://www.webcanape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/ (дата обращения: 12.07.2020).

– упрощается процесс сбора предложений и определения инициатив, наиболее поддерживаемых обществом;

– появляется возможность повысить уровень доверия общества к работе органов государственной власти благодаря увеличению информационной открытости и развитию публичности их деятельности;

– наиболее востребованная информация благодаря возможностям социальных медиа распространяется с максимальной быстротой;

– социальные медиа обладают более высоким имиджевым потенциалом в сравнении с официальными сайтами органов государственной власти, появляется возможность посредством новых информационно-коммуникационных технологий организовать диалог с населением;

– социальные медиа стимулируют инновации в сфере предоставления государственных услуг и государственных операций.

Наметившаяся тенденция к подлинно демократическому диалогу власти и общества предполагает обмен точными, полными и проверяемыми сведениями. Для общественности социальные медиа иногда являются единственной возможностью быть услышанной и повлиять на общественно-политические процессы в стране. В то же время, безусловно, электронные социальные медиа несут в себе и некоторые риски, так как представляют собой свободное и демократическое, но нередко анархическое явление, с большим объемом политизированного компромата и фальсификаций. Каналы социальных медиа используются отдельными федеральными органами власти (включая МВД России) достаточно активно: количество подписчиков официальных сообществ и проектов насчитывает сотни тысяч человек.

Расширение присутствия МВД России в социальных медиа и налаживание контактов среди наиболее активной части российских интернет-пользователей привело к значительному увеличению числа подписчиков официальных аккаунтов Министерства. Так, по состоянию на 30 сентября 2019 г. количество подписчиков официальных аккаунтов МВД России распределилось следующим образом: Twitter – 137 148 чел., Facebook – 17 254 чел., «ВКонтакте» – 178 177 чел., «Одноклассники» – 191 467 чел., Instagram – 172 891 чел., YouTube – 34 000 чел.

Потенциал ресурсов социальных медиа обусловлен:

– масштабной аудиторией;

– разнообразием способов подачи информации;

– дифференциацией уровней доступа к информации;

– возможностью дискуссии с аудиторией интернет-пользователей (с потребителями информации);

– получением оценок и обратной связи от аудитории интернет-пользователей;

– наличием контроля за информационным потоком;

– сегментацией аудитории (проведением адресной коммуникации);

– возможностью оперативного информационного реагирования;

– финансовой доступностью ресурсов социальных медиа;

– наличием дополнительных PR-инструментов.

Документом, определяющим направления развития информационного общества (включая социальные медиа) в России, является Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, в которой отражено, что социальные сети, доступ к которым осуществляется с использованием сети Интернет, стали частью повседневной жизни россиян, а в качестве одного из приоритетных направлений развития названо «формирование информационного пространства с учетом потребностей в получении качественных и достоверных сведений».

Таким образом, в современной России органам государственной власти в целях успешной коммуникации с населением важно обеспечить свое полноценное присутствие в социальных сетях. Именно официальные интернет-сайты и социальные сети обладают наибольшим имиджевым потенциалом для государственных органов и становятся важными инструментами в реализации медийной и социальной коммуникации в интернет-пространстве.

4. Перспективы развития интернет-ресурсов МВД России

В связи с постоянным развитием АПК «Официальный интернет-сайт МВД России» подразделения МВД России, отвечающие за его функционирование (Департамент информационных технологий и защиты информации МВД России, ФКУ НПО «Специальная техника и связь МВД России» и, конечно, УОС МВД России), столкнулись с вполне ожидаемыми проблемами, решение которых не терпит отлагательств.

Основные блоки, которые значительно замедляют работу АПК, – это логирование (ведение журнала событий) и база данных новостей, которая ведется со всем прикрепленным мультимедийным контентом с самого появления сайта mvd.ru в 2009 г. Это связано с тем, что с каждым запросом пользователя огромная база индексируется (пересчитывается) и скорость работы сайта заметно падает.

Так, по данным администраторской части сайта, на конец 2017 г. – начало 2018 г. в базе данных новостей было 600 000 материалов, а на начало октября 2019 г. это число составило 2,5 млн.

Таким образом, основным вопросом является пересмотр алгоритма работы с новостным контентом, так как по мере разрастания АПК отправка ключевых новостей на нижестоящие сайты [42], так называемое «расшаривание»[43], породила создание дублирующей информации, которая молниеносно стала заполнять базу данных.

Внешний вид интернет-сайта Министерства обновлялся в 2013 и 2017 гг. в связи с предъявляемыми современными требованиями к уровню

[42] Технологически в АПК каждый интернет-сайт в домене мвд.рф может сделать свое кольцо сайтов уже в «собственном» домене на уровне выше.

[43] От англ. *share* – «распространять».

доступности и удобства в использовании. В настоящее время планируется новая модернизация в связи с проводимой Правительством РФ работой по унификации интернет-сайтов органов государственной власти.

В настоящее время для контроля и координации работы региональных подразделений ИиОС МВД России по линии работы с АПК используется устаревшая Методика [44], в основу которой заложена актуальность информации и корректность функционирования интернет-сайта без учета количества репостов и ретвитов при проведении имиджевых акций МВД России, а также количества «подхваченного» новостного видеоконтента в YouTube. Как сообщалось ранее, основополагающим концептуальным документом, в котором на высшем государственном уровне определена необходимость доведения до граждан значимой и достоверной информации, в том числе посредством социальных сетей, является Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, однако данный нормативный правовой акт не содержит положений о порядке использования социальных медиа в работе органов государственной власти.

Анализируя федеральное законодательство в рассматриваемой сфере деятельности, следует признать, что общего нормативного правового акта, регулирующего порядок работы органов государственной власти в социальных сетях, до сих пор нет. Понятие социальной сети либо порядок ее использования в нормативных правовых актах также не представлены.

На сегодняшний день в наличии имеются только правовые нормы о содержании и технологических требованиях, предъявляемых к официальным сайтам органов государственной власти. Однако в отношении правил ведения социальных сетей подобных норм нет, хотя общие принципы правового регулирования отношений, возникающих в сфере информации и информационных технологий, разработаны достаточно давно (в 2006 г.).

Таким образом, для четкого взаимодействия ведомственных модераторов социальных медиа необходимо разработать унифицированную инструкцию по работе в социальных сетях, изучив опыт правоохранительных структур других стран, которая в будущем может стать ведомственным нормативным правовым актом по ведению подразделениями МВД России аккаунтов в социальных сетях.

[44] Приложение № 1 к распоряжению МВД России от 26 декабря 2017 г. № 1/15716 «Об утверждении методик оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации по направлениям деятельности УОС МВД России».

Список литературы

1. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 9 февраля 2009 г. № 8-ФЗ // СПС «Гарант».
2. О средствах массовой информации: Закон РФ от 27 декабря 1991 г. № 2124-1 (в ред. от 6 июня 2019 г.) // СПС «Гарант».
3. Об утверждении перечня информации о деятельности МВД России, размещаемой в информационно-телекоммуникационной сети «Интернет»: Указ Президента РФ от 10 августа 2011 г. № 1060 // СПС «Гарант».
4. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // СПС «Гарант».
5. О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов: постановление Правительства РФ от 25 апреля 2012 г. № 394 // СПС «Гарант».
6. О приоритетных направлениях использования и развития информационно-коммуникационных технологий в федеральных органах исполнительной власти и органах управления государственными внебюджетными фондами и о внесении изменений в некоторые акты Правительства Российской Федерации: постановление Правительства РФ от 5 мая 2016 г. № 392 // СПС «Гарант».
7. О совершенствовании взаимодействия подразделений системы Министерства внутренних дел Российской Федерации со средствами массовой информации: приказ МВД России от 19 июня 2018 г. № 385 // СТРАС «Юрист».
8. О порядке подготовки и размещения информации о деятельности Министерства внутренних дел Российской Федерации в информационно-телекоммуникационной сети «Интернет»: приказ МВД России от 26 февраля 2018 г. № 109 // СТРАС «Юрист».
9. Об утверждении методик оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации по направлениям деятельности УОС МВД России: распоряжение МВД России от 26 декабря 2017 г. № 1/15716 // СТРАС «Юрист».
10. Вопросы организации информационно-правового обеспечения деятельности органов внутренних дел Российской Федерации: приказ МВД России от 25 августа 2017 г. № 680 // СТРАС «Юрист».

ШУКЮРОВ ШАХИН ТЕЙЮБ ОГЛЫ,
доктор философии по праву,
доцент кафедры административной деятельности в ОВД
(Академия полиции МВД Азербайджанской Республики)

Правовое обеспечение информационной безопасности, информации, информационных технологий и его значение в деятельности ОВД

Безопасность является необходимым условием существования человека, общества, государства. Заботясь о реализации жизненно важных потребностей, органы государственной власти вместе с тем обеспечивают безопасность прав и свобод личности, материальных и духовных ценностей общества, собственности, территориальной целостности, суверенитета и конституционного строя государства. Более того, национальная безопасность – это еще и способность сохранять определенные параметры нации: самосохранение и самосовершенствование. Как указала Н. В. Мясникова, самую непосредственную роль в этом направлении играют связи с общественностью, обеспечивающие в том числе и информационную безопасность в государстве [11, с. 1].

Информационная безопасность зависит от ряда факторов. Информационное пространство каждой страны, ее информационные ресурсы и технологии определяют уровень и динамику социально-экономического, научно-технического и культурного развития общества. Эффективность определяется объемом накопленной информации, скоростью ее обработки и использования [5, с. 232].

На современном этапе в каждом государстве формируются правовые основы информационной безопасности. В Концепции национальной безопасности Азербайджанской Республики в общей форме нашли свое отражение основные задачи информационной безопасности страны. В ней указывается, что одно из основных направлений национальной безопасности составляет политика информационной безопасности. По словам А. М. Гасанова, политика информационной безопасности Азербайджанской Республики состоит в осуществлении комплекса мер, направленных на охрану государственных, общественных и частных информационных ресурсов, а также на защиту национальных интересов в сфере информации [5, с. 248].

Право на информацию неразрывно связано с развитием гражданского общества, первоначально находя свое отражение в Декларации прав человека и гражданина периода Великой французской революции, Конституции США, Конституции Швеции, документах Лиги Наций. Конституция СССР 1936 г. предоставляла гражданам ряд информационных прав, включая свободу слова и печати, неприкосновенность тайны переписки граждан. Однако подлинный всплеск развитие информационных прав

и свобод получило после Второй мировой войны с принятием Организацией Объединенных Наций Всеобщей декларации прав человека 1948 г., в ст. 19 определившей «свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ». Дальнейшее закрепление данный принцип получил в ст. 19 Международного пакта о гражданских и политических правах.

Важнейшие преобразования в деятельности органов государственной власти в настоящее время связаны с реализацией мероприятий по упорядочению значительных массивов информации, необходимых для принятия эффективных управленческих решений и обеспечения взаимодействия органов публичной власти с гражданами и организациями. Публичные информационные ресурсы становятся важнейшими источниками получения юридически значимой информации о деятельности государственных органов.

Информационные технологии формируются из ряда структурных элементов, приоритетным из которых является сама «информация». Информация – это стратегический продукт, но с появлением современных средств вычислительной техники она стала выступать также одним из важнейших ресурсов научно-технического прогресса и преобразования общества. Самым приоритетным видом деятельности сегодня является формирование информационного общества – общества, в котором процессы сбора, обработки, анализа, передачи информации, т. е. информационные и коммуникационные технологии, занимают основное место в различных сферах человеческой деятельности. Особенно значимую роль информация играет в управленческой деятельности, к которой относится и юридическая деятельность [2, с. 11].

С помощью информации осуществляется взаимосвязь и взаимодействие всех элементов правовых механизмов, объединение их в правовую систему общества, связь правовых образований с внешней средой; во-вторых, информация является основой всех этапов правового воздействия. На основе полной и своевременной информации происходит движение в направлении поставленных целей, принимаются оптимальные решения [2, с. 13].

Информация является основным достоянием специализированной деятельности. В качестве основных составляющих деятельности юриста можно выделить следующие: 1) работа с социально-правовой информацией (ее поиск, оценка, отбор, систематизация, изучение, анализ, переработка и пр.); 2) уяснение задачи, оценка ситуации с учетом ее предполагаемых изменений и выдвижение гипотез; 3) определение оптимальных или рациональных способов и средств выполнения поставленной задачи; 4) осуществление межличностных контактов (бесед, допросов, обсуждений и т. д.); 5) анализ (логический, профессиональный) исходных данных и доказательств; 6) принятие решений; 7) подготовка документов

(протоколов, справок, решений и др.); 8) контроль исполнения и законности [2, с. 12–13].

Все стадии процесса правового воздействия осуществляются с помощью непрерывных информационных процессов – информационной связи с деятельностью учреждений, предприятий, организаций, граждан и т. д. На основе своевременно собранной, достаточной, проанализированной информации строится информационная модель преступления и принимаются необходимые решения. Информационные процессы в правовой системе – это процессы поиска, сбора, производства, получения, хранения, распространения, обработки, передачи и потребления информации, принятия на ее основе необходимых решений.

Деятельность правоохранительных органов связана с обработкой больших объемов различной информации, что в современных условиях требует использования информационных технологий. К настоящему времени уже разработано и внедрено большое количество разнообразных информационных систем. Они активно используются для сбора и обработки учетно-регистрационной и статистической информации, организации оперативно-следственных мероприятий, проведения криминалистических исследований, управления деятельностью правоохранительных органов и т. д. [13, с. 1].

Современные информационные технологии можно определить как систему операций по сбору, хранению, обработке и передаче информации, осуществляемых по каналам связи с использованием компьютерной техники. Основными принципами современной информационной технологии являются: интерактивный, «дружественный» интерфейс работы; интегрированность с другими программными продуктами; гибкость процесса изменения данных и постановки задач. Выделяют несколько видов информационных технологий: обработки данных; управления; автоматизации офиса; поддержки принятия решений; экспертных систем и т. д. В ОВД внедрение новых информационных технологий идет через построение на основе современных компьютеров локальных, региональных и общегосударственной отраслевых информационно-вычислительных сетей, которые будут способствовать дальнейшему совершенствованию информационного обеспечения ОВД [9].

Значение информационных технологий в юридической деятельности проявляется в том, что они позволяют: наиболее эффективно искать, обрабатывать и использовать накопленные ресурсы правовой и иной информации; автоматизировать информационные процессы в юридической сфере, в том числе связанные с принятием и реализацией правовых решений, определением направления действий в сложных ситуациях профессиональной деятельности; обеспечить информационно-телекоммуникационное взаимодействие различных субъектов при решении юридических задач; оптимизировать образовательный процесс, профессиональную подготовку юристов; обеспечить процесс получения

и накопления новых правовых знаний на основе теории искусственного интеллекта и методов информационного моделирования. При этом обеспечивающие информационные технологии представляют собой инструменты, которые могут быть использованы в различных предметных областях юриспруденции. К ним можно отнести технологии текстовой обработки информации, технологии баз данных и работы с ними, телекоммуникационные технологии, технологии мультимедиа, технологии защиты информации и другие. В свою очередь, функциональные информационные технологии реализуют типовые процедуры обработки информации в определенной предметной области юриспруденции и направлены на компьютеризацию решения задач конкретных специалистов, в том числе сотрудников правоохранительных органов [8].

Информация стала важнейшим стратегическим, управленческим ресурсом наряду с ресурсами – человеческим, финансовым, материальным. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы предполагает формирование в России цифровой экономики. В целях развития информационного общества государством создаются условия для формирования пространства знаний и предоставления доступа к нему, совершенствования механизмов распространения знаний, их применения на практике в интересах личности, общества и государства. Федеральный закон «О полиции» провозгласил использование достижений науки и техники, современных технологий и информационных систем основным принципом деятельности полиции, законодательно закрепив инновационные процессы в правоохранительной сфере, и стимулировал внедрение инновационных продуктов мира цифровых технологий в деятельность ОВД [16, с. 1].

Усиливается потребность в быстром и надежном получении сведений, необходимых для правоохранительной деятельности. В этой связи одним из эффективных путей укрепления правопорядка является своевременное, полное и объективное информационное обеспечение правоохранительных органов [14, с. 1].

Развитие компьютерных средств, информационно-телекоммуникационных систем, средств связи, возросшие возможности их применения и, как следствие, изменения в российском законодательстве привели к необходимости рассмотрения правовых, организационно-тактических и технических аспектов применения компьютерных технологий в деятельности по расследованию преступлений [10, с. 2].

На сегодняшний день эффективность борьбы с преступностью определяется уровнем организации профилактической, оперативной, следственной работы, проводимой ОВД. Результаты этой работы непосредственно зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации. Именно эти функции и призвана реализовать система

информационного обеспечения ОВД. Основополагающую роль в информационном обеспечении правоохранительных органов занимают учеты, используемые для регистрации первичной информации о преступлениях и лицах, их совершивших. Учеты предназначены для получения информации, которая помогает в предупреждении, раскрытии и расследовании преступлений, установлении личности неизвестных граждан и принадлежности изъятого имущества, розыске преступников [15, с. 1].

Современное общество характеризуется распространением информационных технологий, в том числе информационных корпоративных систем, позволяющих охватить большинство управленческих, оперативных и стратегических функций крупных организаций, предприятий и учреждений. Данная система должна быть направлена на обеспечение поддержки следующих функций: автоматизации приема звонков от населения и сообщений от организаций, обслуживающих население; получения информации для оценки статуса и приоритета применения сил реагирования, а также прогнозирования развития оперативной обстановки; мониторинга мобильных служб, размещенных на автомашинах оперативного реагирования; оценки действий дежурных и выработки рекомендаций по их дальнейшим шагам, контроля сроков реагирования и дисциплины исполнения; фиксации всех действий операторов, записи переговоров [12, с. 1].

Немаловажную роль оказывают информационные технологии в области полицейского образования. Формирование цифровой компетентности – это одно из основных требований современного образования полицейского. Появляются новые формы информационного обеспечения деятельности полиции, которые дают возможность раскрывать преступления, не выходя из стен служебного кабинета. Каждый современный полицейский должен: уметь пользоваться электронным документооборотом (с использованием цифровой подписи); пользоваться служебной почтой; использовать базы данных и информационные ресурсы ОВД и других государственных органов; использовать цифровые технологии в своей служебной деятельности в зависимости от специализации (например, эксперт); иметь навыки в области информационной безопасности и защиты информации.

Как отмечает Е. М. Шпагина, формирование цифровой компетентности современного полицейского должно охватывать, по крайней мере, три направления: цифровые навыки для обеспечения повседневной деятельности; навыки работы с информацией ограниченного доступа в цифровом виде (обеспечение информационной безопасности ОВД) и специальные навыки, позволяющие бороться с преступностью, используя информационные технологии [16, с. 2–3].

В заключение научной статьи хотелось бы сделать ряд выводов и выдвинуть некоторые предложения:

– информационная безопасность занимает одно из приоритетных и актуальных положений среди областей института безопасности,

так как существует самостоятельно и взаимодействует, оказывает непосредственное влияние на другие отрасли, в связи с чем необходимо создать условия для развития и совершенствования научных основ информационной безопасности, для разработки научных исследований в этой области;

– информационные технологии – это элементы и средства для качественной и улучшенной деятельности органов и лиц, необходимые для ежедневной практической работы; они нуждаются в распространении на всех уровнях и стадиях;

– необходимо и актуально совершенствование знаний и развитие навыков в области информационных технологий при подготовке специалистов в правоохранительных органах, особенно в ОВД.

Список литературы

1. *Акапьев В. Л., Гуржий А. А., Савотченко С. Е.* Система правового регулирования в области создания, использования и хранения баз данных // 300 лет на страже закона и правопорядка: материалы всероссийской научно-практической конференции. Хабаровск, 2018.
2. *Бурцева Е. В., Селезнёв А. В., Чернышов В. Н.* Информационные технологии в юриспруденции: учеб. пособие. Тамбов, 2012.
3. *Бочкарева Ю. Е., Курилова О. Л.* Информационные технологии в юридической деятельности. Лабораторный практикум: учеб.-метод. пособие. Ульяновск, 2011.
4. *Васильева Т. А.* Конституционные реформы в цифровую эпоху: опыт Исландии. URL: https://cyberleninka.ru/article/n/konstitutsionnye-reformy-v-tsifrovuyu-epohu-opyt-islandii (дата обращения: 19.11.2019).
5. *Гасанов А. М.* Политика национального развития и безопасности Азербайджанской Республики. Баку, 2014.
6. *Егоров В. А.* Организация правоохранительной деятельности с использованием информационных технологий: автореф. дис. … д-ра юрид. наук. Саратов, 2007.
7. *Елин В. М.* Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография / под ред. А. П. Баранова. М., 2016.
8. *Епифанов С. С.* Тенденции развития информационных технологий в юридической сфере (правоохранительный аспект). URL: https://novainfo.ru/article/3698 (дата обращения: 14.11.2019).
9. Информатика и математика для юристов: учебник / под ред. С. Я.Казанцева, Н. М. Дубининой. М., 2010.
10. *Куриленко Ю. А.* Компьютерные технологии как средство повышения эффективности организации правоохранительной деятельности: применительно к деятельности ОВД по расследованию преступлений. Саратов, 2008.

11. *Мясникова Н. В.* Связи с общественностью как инструмент поддержания национальной безопасности Приднестровского государства // Вестник Московского государственного областного университета. 2018. № 3.
12. *Орехов В. М.* Специфика использования информационных технологий управления в правоохранительной деятельности. URL: http://pravmisl.ru/index.php?option=com_content&task=view&id=2011&Itemid=76 (дата обращения: 17.11.2019).
13. *Попов А. Ю., Рак И. П.* Информационные технологии в деятельности правоохранительных органов. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-deyatelnosti-pravoohranitelnyh-organov (дата обращения: 24.11.2019).
14. *Попов В. И., Ледков Ю. В., Солоненко Д. Ю.* Некоторые аспекты подготовки подведомственных правовых актов по вопросам совершенствования информационного обеспечения органов внутренних дел. URL: http://zhenilo.narod.ru/main/ips/2003_common_problems.pdf (дата обращения: 22.11.2019).
15. *Худяков А. Н.* Информационные технологии в правоохранительной системе России: состояние и перспективы развития. URL: https://isfic.info/SPBU/konf43.htm (дата обращения: 29.11.2019).
16. *Шпагина Е. М.* Формирование цифровой компетентности у сотрудников полиции. URL: http://petrovka-38.com/arkhiv/item/formirovanie-tsifrovoj-kompetentnosti-u-sotrudnikov-politsii (дата обращения: 28.11.2019).

Е. П. ШУЛЬГИН,
адъюнкт 3-го факультета
(Академия управления МВД России)

Обновление цифровой среды правоохранительных органов посредством внедрения электронного досудебного расследования

Электронное правосудие в деятельности правоохранительных органов за последние годы существенно актуализировалось в связи с проводимой судебной реформой и интенсификацией процессов внедрения электронного правосудия в стадию досудебного расследования уголовных дел. Вместе с тем для законодателя должна быть первостепенной разработка общих теоретико-методологических основ и концептуальных механизмов расследования уголовных дел в электронном формате.

Цифровую среду правоохранительных органов необходимо напрямую связывать с правовым механизмом. Так, в частности, имеется указание на то, что правовой механизм следует расценивать не как просто набор тех или иных средств, а как слаженную, четко функционирующую цифровую среду. Формирование электронного правосудия является одной из наиболее актуальных задач развития государственного механизма. Решение данной задачи является ответом на вызовы современного информационного общества и неотъемлемым компонентом стратегии перспективного совершенствования законодательства и правоприменительной практики в сфере организации досудебного расследования. Вместе с тем формирование и реализация подобной стратегии вызывают необходимость в четком понимании методологических основ электронного правосудия в уголовно-процессуальном законодательстве. При этом без единообразного и однозначного их установления невозможно осуществление электронного правосудия.

Между тем такое единообразие крайне важно именно в сфере организации досудебного расследования в электронном формате, для соблюдения конституционного принципа равенства всех перед законом и судом. История становления электронного правосудия в мире неразрывно связана с информатизацией широких сфер общественной жизни и проникновением компьютера в повседневность граждан и организаций. Ведь право, как универсальный социальный регулятор, не только упорядочивает общественное восприятие, но также зачастую фиксирует его основные изменения и, уловив перспективные тенденции, актуализирует то или иное направление общественного развития.

Внедрение электронного правосудия можно рассматривать как одно из проявлений процессов глобализации, охвативших, в частности, и среду деятельности правоохранительных органов.

При этом иногда под правовым механизмом понимают не совокупность правовых предписаний, обеспечивающих тот или иной процесс, а комплекс управленческих отношений, в рамках которых применяются те или иные методы, правила [45]. Также имеет место определение понятия «правовой механизм» посредством его сопоставления с понятием «правовой режим» (учитывая тот факт, что их нередко отождествляют). В частности, указывается, что правовой механизм – это «инструментальная субстанция», которая может содержать и весьма обширный набор тех или иных правовых средств, но обеспечиваться правовой механизм может только посредством надлежащего правового режима [46]. В ряде случаев понятию «правовой механизм» придается совсем иное значение, преимущественно отражающее содержательный, социально-ценностный аспект соответствующей деятельности.

Так, в частности, А. Ф. Кучин, оценивая в своем диссертационном исследовании правовой механизм публичного уголовного преследования, указывает, что «главной деталью правового механизма уголовного преследования является обвинение, через которое он приводится в движение и сообщает тем самым энергию для развития уголовного судопроизводства в целом» [47]. Как указывает Ю. С. Жариков, понятие «правовой механизм» преимущественно связывается с «системой правовых средств, т. е. различных правовых явлений, задействованных в упорядочении общественных отношений и призванных обеспечить их нормальное функционирование»[48].

Таким образом, понятие «правовой механизм» должно позволять в каждом конкретном случае показывать, каким образом осуществляется или должно осуществляться правовое регулирование общественных отношений, возникающих по определенному поводу, позволять наметить пути развития законодательства и правоприменительной деятельности в любой исследуемой области[49].

В данном ключе следует признать, что в настоящее время более верным будет вести речь о формировании правового механизма деятельности должностных лиц органов досудебного расследования в рамках электронного формата судопроизводства, а не о его совершенствовании. Фактически к настоящему времени имеется лишь набор правовых предписаний, причем пока не находящихся в органическом единстве, а также начинающая

---

[45] *Селюков А. Д.* Финансово-правовые механизмы государственного управления // Финансовое право. 2010. № 7. С. 2.

[46] *Долгополов А. А.* Теоретические основы административно-правовых режимов в сфере оборота оружия и взрывчатых веществ // Российский следователь. 2005. № 8. С. 41.

[47] *Кучин А. Ф.* Правовой механизм публичного уголовного преследования: автореф. дис. … канд. юрид. наук. Н. Новгород, 2004. С. 9.

[48] *Жариков Ю. С.* Уголовно-правовое регулирование и механизм его реализации. М., 2009. С. 43.

[49] *Кузнецова С. А.* К вопросу об определении понятия «правовой механизм» // Вестник Санкт-Петербургского университета МВД России. 2013. № 1 (57). С. 10.

складываться правоприменительная практика по их реализации. Непосредственно в сфере реализации должностными лицами функций по досудебному расследованию вопросы определения понятия «правовой механизм» преимущественно затрагивают те или иные частные аспекты уголовно-процессуальной деятельности (механизм обеспечения прав участников процесса, механизм обеспечения принципов процесса и т. д.).

Помимо определения исключительно правового механизма (то есть совокупности значимых правовых предписаний, которые оформляют всю деятельность по реализации электронного формата досудебного расследования) следует признать и особый управленческий механизм в деятельности должностных лиц органов уголовного досудебного расследования.

Таким образом, следует признать, что современный правовой механизм деятельности должностных лиц органов досудебного расследования, осуществляющих производство в электронном формате, – это совокупность правовых предписаний (средств, инструментов), формирующих определенный порядок осуществления деятельности должностных лиц при производстве расследования в электронном формате, на основе которых могут приниматься соответствующие управленческие решения. Оценивая все вышеприведенные теоретические концепции относительно определения понятия «правовой механизм» в контексте предмета нашего исследования, заметим, что речь должна идти фактически о двух взаимодополняющих элементах: полнота (достаточность) правовых предписаний по вопросам обеспечения электронного документооборота в досудебной стадии (этот аспект преимущественно относится к собственно правовому инструментарию) и непротиворечивость имеющейся нормативно-правовой базы (т. е. согласованность, отсутствие коллизий как с другими нормативными правовыми актами, так и с иными значимыми основами деятельности в рамках досудебного производства).