Министерство внутренних дел Российской Федерации

Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Сборник научных статей

Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2024

Министерство внутренних дел Российской Федерации

Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Сборник научных статей

Орел
ОрЮИ МВД России имени В.В. Лукьянова
2024

УДК 004
ББК 32.97
И74

И74 **Информационные технологии в деятельности правоохранительных органов: современное состояние, проблемы и перспективы :** сборник научных статей / редколлегия: Л.Д. Матросова [и др.]. – Орел : ОрЮИ МВД России имени В.В. Лукьянова, 2024. – 93 с.
ISBN 978-5-88872-349-4

Сборник содержит статьи профессорско-преподавательского состава, курсантов и слушателей, посвященные проблемам применения технологий компьютерной обработки информации в деятельности ОВД и обеспечения информационной безопасности в деятельности ОВД.

Статьи представлены в авторской редакции.

УДК 004
ББК 32.97

ISBN 978-5-88872-349-4

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Формирование единого информационного пространства и развитие телекоммуникационных технологий занимает значительное место в современном обществе. Это связано с тем, что в вычислительных системах интегрируется информация о различных сторонах деятельности государства, населения, конкретных граждан и их личной жизни в политическом, экономическом, моральном и имущественном аспектах.

Широкое применение технологий компьютерной обработки информации в деятельности ОВД, значительно повысило эффективность ее повседневной деятельности. Применение автоматизированных рабочих мест и управляющих систем позволило снизить время реагирования на различные ситуации. Автоматизация деятельности региональных подразделений позволила сократить время на принятие управленческих решений и объединить в единую информационную систему все подразделения ОВД, находящиеся на территории региона. Используемые в настоящее время информационные системы позволяет автоматизировать все направления деятельности региональных подразделений ОВД, что обеспечивает оперативный обмен информацией и улучшенный доступ к информационным ресурсам.

СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, КЛАССИФИКАЦИЯ, ОСОБЕННОСТИ ПРИМЕНЕНИЯ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ

Матросова Л.Д.,
канд. юрид. наук, доцент,
начальник кафедры информационных
технологий в деятельности ОВД
ОрЮИ МВД России
имени В.В. Лукьянова

В нынешнее время нам предоставлено огромное количество информационных технологий, которые к слову никогда не стоят на месте и ежедневно модернизируются. Почти каждый день увеличивается количество необходимой для повседневной деятельности информации, причём в различных сферах жизнедеятельности, в связи с этим является логичным появление новейших средств и методов обработки информации. Прогрессивно новым технологиям и появлением новой информации, изменяются способы её защиты со стороны её обеспечения и хранения. Важнейшей составляющей жизнедеятельности человека в настоящее время, безусловно, будет образование. Образование, несомненно, учитывает современные технологии, то есть держит руку на пульсе современных обновлений и открытий информационных технологий, все это для того, чтобы образование соответствовало понятию качественного и продуктивного.

Одной из характеристик информатизации образования является процесс массового распространения и совершенствования информационно-коммуникационных технологий (ИКТ). Что же такое информационно-коммуникационные технологии? Обратимся к словарю Д.Н. Ушакова, который дает определение технологии в широком смысле: «Технология, (от греч. techne – искусство и logos – учение). Совокупность наук, сведений о способах переработки того или иного сырья в фабрикат, в готовое изделие».

Дать более конкретное понятие этого термина, можно обратившись к более узкоспециализированному Финансовому словарю Финам: «Технология – способ преобразования вещества, энергии, информации в процессе изготовления продукции, обработки и переработки материалов, сборки готовых изделий, контроля качества, управления. Технология включает в себе методы, приемы, режим работы, последовательность операций и процедур, она тесно связана с приме-

няемыми средствами, оборудованием, инструментами, используемыми материалами». Анализируя вышеуказанные понятия терминов, следует выделить способы обработки и преобразования информационного потока.

«Информационно-коммуникационные технологии – совокупность методов, процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации. ИКТ включают различные программно-аппаратные средства и устройства, функционирующие на базе компьютерной техники, а также современные средства и системы информационного обмена, обеспечивающие сбор, накопление, хранение, продуцирование и передачу информации». Исходя из данного определения, можно сделать вывод, что главным устройством ИКТ является какое-либо современное устройство, которое способно обработать информацию и на котором установлено соответствующее программное обеспечение. В качестве данного устройства может выступать компьютер, планшет, современный смартфон.

Рассмотрим, с каких точек зрения можно классифицировать информационные технологии.

Классификация по области решаемых задач:

– мультимедиа-технологии – компьютерные технологии, которые одновременно используют несколько информационных сред: графика, видео, текст, анимация, звук (презентации, фильмы, интерактивные тренажеры);

– телекоммуникационные технологии – технологии обеспечивающие передачу и хранение информации (компьютерная сеть);

– CASE-технологии (Computer Aided Software Engineering) – набор инструментов и методов программной инженерии для проектирования программного обеспечения (разработка приложений JAM, менеджер транзакций Tuxedo);

– технологии защиты информации;

– геоинформационные технологии;

– технологии искусственного интеллекта.

Классификация по предметной деятельности:

– технологии организационного управления (автоматизация функций управленческого персонала);

– технологии управления технологическими процессами (автоматизация функций производственного персонала);

– технологии автоматизированного проектирования (построение моделей, производство расчетов);

– образовательные технологии.

Классификация по типу обрабатываемой информации (является условной, так как многие информационные технологии многозадачны, например, в текстовом редакторе можно производить вычисления и обрабатывать графическую информацию):

– технологии обработки данных (табличные процессоры, СУБД);

– технологии обработки текста (текстовые процессоры);

– технологии обработки графики (графические процессоры);

– технологии обработки знаний (экспериментальные системы);

– технологии обработки объектов реального мира (средства мультимедиа).

Классификация по типу пользовательского интерфейса:

– командный интерфейс – выдача на экран системного приглашения для ввода команды;

– WIMP-интерфейс – выдача на экран окна, содержащего образы программ и меню действий, для выбора которых используется указатель мыши;

– SILK-интерфейс – выдача на экране информации по речевой команде. По смысловым связям происходит перемещение от одних поисковых образов к другим.

Информационные и коммуникативные технологии – это обобщающее понятие, описывающее различные устройства, механизмы, способы и алгоритмы обработки информации.

Важнейшими современными устройства ИКТ являются компьютер, снабженный соответствующим программным обеспечением, и средства телекоммуникации вместе с размещенной на них информацией.

В настоящее время классификация информационных и коммуникативных технологий проводится по следующим признакам:

- способу реализации в (автоматизированных) информационных системах (АИС);
- степени охвата задач управления;
- классам реализуемых технологических операции;
- типу пользовательского интерфейса;
- технологиям обработки информации;
- обслуживаемой предметной области.

Рассмотрим подробнее некоторые признаки.

1. По способу реализации информационные и коммуникативные технологии делятся на:

· традиционные;

· современные.

Традиционные существовали в условиях централизованной обработки данных, до периода массового использования персональной электронно-вычислительной машины (ПЭВМ). Они были ориентированы главным образом на снижение трудоемкости пользователя. Например, инженерные и научные расчеты, формирование регулярной отчетности на предприятиях и др.

Современные (новые) связаны в первую очередь с информационным обеспечением процесса управления в режиме реального времени.

2. По степени охвата информационными технологиями задач управления выделяют: электронную обработку данных, автоматизацию функций управления, поддержку принятия решения, электронный офис, экспертную поддержку.

В первом случае электронная обработка данных выполняется с использованием ЭВМ без пересмотра методологии и организации процессов управления при решении локальных математических и экономических задач.

Во втором случае при автоматизации управленческой деятельности вычислительные средства используются для комплексного решения функциональных задач, формирование регулярной отчетности и работы в информационно-справочном режиме, для подготовки управленческих решений. К этой же группе относятся информационные технологии поддержки принятия решений, которые предусматривают широкое использование экономико-математических методов и моделей, пакеты прикладных программ (ППП) для аналитической работы и формирование прогнозов, составления бизнес-планов, обоснованных оценок и выводов по процессам и явлениям производственно-хозяйственной деятельности.

К названной группе относятся и широко внедряемые в настоящее время информационные технологии, получившие название электронного офиса и экспертной поддержки принятия решений. Электронный офис предусматривает наличие интегрированных ППП, которые обеспечивают комплексную реализацию задач предметной области. В настоящее время все большое распространение приобретают электронные офисы, сотрудники и оборудование которых могут находиться в разных помещениях. Необходимость работы с документами, материалами и базами данных конкретного предприятия или учреждения привела к появлению электронных офисов, включенных в соответствующие сети ЭВМ.

3. В зависимости от вида обрабатываемой информации, информационные и коммуникативные технологии могут быть ориентированы на:

1) Обработку данных (например, электронные таблицы, алгоритмические языки, системы программирования и т.д.);

2) Обработку тестовой информации (например, тестовые процессоры, гипертекстовые системы и т.д.);

3) Обработку графики (например, средства для работы с графикой, средства для работы с векторной графикой);

4) Обработку анимации, видеоизображения, звука (инструментарий для создания мультимедийных приложений);

5) Обработку знаний (экспертные системы).

Распределение достаточно условное, т.к. большинство информационных технологий позволяет поддерживать и другие виды информации.

4. Технология обработки информации на компьютере может заключаться в заранее определенной последовательности операций и исключать возможность пользователя влиять на обработку информации, пока она проводится в автоматическом режиме. Стоит отметить, что внедрение специальных систем обмена и хранения информации при использовании искусственного интеллекта стало крайне распространенным в западной практике. Это позволяет расширять границы использования информации, более активно и оперативно реагировать на происходящее и пресекать некоторые угрозы основам национальной безопасности на стадии их потенциального зарождения [1].

5. По обслуживаемым предметным областям информационные технологии подразделяются разнообразно. Например, в экономике можно выделить: бухгалтерский учет, банковская, налоговая и страховая деятельность и др. Также информационные и коммуникативные технологии широко применяются в науке, образовании, культуре, производстве, военном деле и т.д. Кроме того, использование информационно-коммуникационных технологий получило широкое распространение в противоправных целях.

В рамках данной работы, рассмотреть возможность применения всех информационно-коммуникационных технологий не представляется возможным, поэтому хочу ограничиться наиболее интересным и актуальным на сегодняшний день направлением – а именно сеть Интернет.

Информационно-коммуникационные технологии – это расширенный термин для информационных технологий. Это подчеркивает роль единой связи и интеграции телекоммуникаций и компьютеров, а

также корпоративного программного обеспечения, промежуточного программного обеспечения, систем хранения и аудиовизуальных средств, которые позволяют пользователям получать доступ, хранить, передавать и манипулировать информацией. Термин «ИКТ» используется для обозначения конвергенции аудиовизуальных и телефонных сетей с компьютерными сетями с помощью единой кабельной или линк-системы.

Сеть Интернет в противоправных целях может быть использована так:

1. Незаконное использование чужого товарного знака, как путем размещения его на Интернет-ресурсе, так и в качестве доменного имени.

Особенностью нарушения является то, что теоретически «пострадать» может лицо, де-факто не совершившее противоправных деяний. К примеру, предприниматель в коммерческих целях использует доменное имя. Спустя некоторое время другой предприниматель регистрирует похожий на него товарный знак. А после регистрации предъявляет иск к владельцу (администратору и т.д.) доменного имени. Поскольку доменное имя не является объектом охраняемых авторских прав, победа в суде достанется истцу (постановление Суда по интеллектуальным правам от 25.12.2015 по делу № А41-11219/2015).

Чтобы не понести убытки, связанные с лишением права использования доменного имени, целесообразно в установленном законом порядке зарегистрировать права на соответствующее обозначение. Обнародование в сети объектов авторских прав, принадлежащих других лицам (фотографий, литературных, музыкальных произведений и проч.). Иски предъявляются к лицам, разместившим соответствующий контент в сети, а, если таковых установить не представляется возможным, то к хостинг-провайдеру (решение Московского городского суда от 03.12.2015 по делу № 3-713/2015). Если для защиты прав на товарный знак, таковой должен быть зарегистрирован в установленном порядке, то права на произведения подтверждаются иным образом, поскольку обязательной регистрации не подлежат. В частности, право на обладание исключительной лицензией может быть подтверждено лицензионным договором или договором об отчуждении исключительных прав (решение Московского городского суда от 17.03.2016 по делу № 3-375/2016). Автор произведения может подтвердить свое право на него, разместив на своем сайте или в блоге, а также опубликовав на стороннем ресурсе с указанием своего авторства. Если нарушитель не сможет в суде доказать, что права на произведение принадлежат другому лицу, требования автора будут удовлетворены (апелляционное

определение Омского областного суда от 07.05.2015 по делу № 33-2784/2015).

2. Опубликование сведений, порочащих честь, достоинство и деловую репутацию.

Закон четко определяет роли сторон при доказывании своей позиции в суде. Пострадавший подтверждает факт размещения информации и ее порочащий характер. Лицо, разместившее информацию, должно доказать, что информация соответствует действительности. Интернет-пространство – штука коварная. Мало того, что информация имеет свойство неожиданно появляться и исчезать. Так, еще и установить личность автора заметки не всегда представляется возможным. Это не помеха, если целью заявителя является удаление несоответствующей действительности информации. К этому можно обязать владельца ресурса или провайдера. Для возмещения ущерба потребуется отыскать самого автора (апелляционное определение Московского городского суда от 02.06.2015 по делу № 33-14207).

3. Незаконное списание денежных средств с банковских счетов.

Все чаще владельцы банковских счетов лишаются своих средств с помощью интернета. Мошенники используют различные технические средства, включая перехват данных доступа, не оставляя потерпевшим никаких шансов на возвращение денег на счет.

Привлечь к ответственности мошенников редко удается, равно, как и признать соответствующий банк неисполнившим обязательства по сохранности вкладов. Дело в том, что, зачастую по условиям договора с банком вкладчик (владелец счета) берет на себя все риски, связанные с использованием услуги интернет-банка, в том числе, в случае взлома канала связи (апелляционное определение Верховного Суда Республики Саха (Якутия) от 18.01.2016 № 33-206/2016).

Другими словами, получить свои деньги обратно можно, если удастся доказать, что хищение средств произошло по вине банка (была взломана именно система банка, например), а не путем нарушения конфиденциальности в зоне ответственности клиента (вирус в компьютере, подключение к сети через провайдера клиента и т.д.).

Кроме того, в противоправных целях используются и такое явление как социальные сети. В частности, незаконное получение, обработка, использование изображения человека, а также его личной информации. Примером таких действий служит громкое дело «В Контакте» против стартапа «Дабл». Пресс-служба «В Контакте» заявила, что Double Data бесконтрольно собирала данные пользователей, в том числе фамилии, имена, даты рождения и другую открытую информацию. Они использовались в коммерческих целях, в том числе для

оценки кредитоспособности заемщиков. При этом, как подчеркивает соцсеть, ни пользователи, ни сама «ВКонтакте» не давали на это разрешения.

В 2017 году «В Контакте» подала в суд на Double Data и Национальное бюро кредитных историй. Ответчики тогда назвали иск проявлением конкурентной борьбы и заявили, что соцсеть хочет сама заработать на этой информации. В Double Data сообщили, что информация собиралась при помощи программного обеспечения собственной разработки, а просились лишь те данные, которые находятся в открытом доступе. Тогда суд постановил, что социальная сеть не смогла доказать затраты исключительно на создание, сбор или обработку материалов, которые составляют базу данных.

В 2018 году Девятый арбитражный апелляционный суд частично удовлетворил иск «Вконтакте». Он запретил третьим лицам использовать данные пользователей ресурса в коммерческих целях.

В марте 2021 года Арбитражный суд отказал соцсети в иске, не признав факт нарушения исключительного смежного права на базу данных пользователей.

В 2020 году СМИ подробно писали о конфликте между Double Data и «В контакте». Дело в том, что первая компания продает технологию анализа открытых данных пользователей соцсетей. При этом Mail.ru, которая владеет «В контакте», в 2016 году запустила конкурирующий бизнес в сфере big data. Одновременно сотрудник Mail.ru написал на Double Data заявление по статье 272 УК РФ. В Mail.ru тогда пояснили, что их сотрудник действовал «в частном порядке», так как «Double Data хранит у себя историю публичных действий людей, лишая их возможности самостоятельно управлять информацией о себе и доступом к ней». Аргумент о том, что компания собирает только открытые данные, в том числе по соцсетям, в Mail.ru не принимают: «Мы категорически не согласны с мнением Double Data о том, что кто угодно может хранить и обрабатывать любые доступные в сети личные данные. Double Data занимается не предпринимательством и не бизнесом, а неправомерным сбором и перепродажей данных людей».

Как отмечает Е.С. Лысенко, результаты компьютерно-технических экспертиз нужны для успешного расследования преступлений в данной сфере, однако низкий уровень знаний в области информационных технологий приводит к тому, что следователи (дознаватели), ведущие дела, не могут правильно сформулировать и поставить перед экспертами вопросы, что в результате отрицательно сказывается на качестве проводимых экспертиз, а многие факты просто не попадают в поле зрения при соответствующих исследованиях [2].

Так, информационно-коммуникационные технологии стали распространенным средством, которое используется как во благо, так и в противоправных целях. В частности, сеть Интернет, по мнению некоторых ученых может быть рассмотрен как место совершение преступления, также как средство. Далее рассмотрим вопросы использования информационно-телекоммуникационной сети Интернет для совершения преступлений.

---

1. Семенов Е.Ю. Основные проблемы внедрения автоматизированных информационных систем в деятельность органов внутренних дел // Научный портал МВД России. 2022. № 1(57). С. 36–40. EDN WMLLZJ.
2. Лысенко Е.С., Семенов Е.Ю. Борьба с преступностью в условиях развития информационного общества // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4 (93). С. 57–64. EDN OLDPDP.

СПЕЦИФИКА РАЗРАБОТКИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ (АИС) В ОВД

Семенов Е.Ю.,
канд. юрид. наук, доцент,
профессор кафедры информационных
технологий в деятельности ОВД
ОрЮИ МВД России
имени В.В. Лукьянова

В настоящее время информационные технологии активно внедряются в различные сферы деятельности, включая правоохранительную систему. Применение программного обеспечения в органах внутренних дел позволяет автоматизировать множество процессов, увеличить скорость обработки данных и принятия решений, а также улучшить качество оказываемых услуг. Значительная часть информации, обрабатываемой органами внутренних дел, хранится в виде большого объема неструктурированных и слабоструктурированных данных, включая текст, изображения, видео и т.д. В этом отношении ключевое и реальное различие между аналитической обработкой данных и расширенным анализом больших данных заключается в том, что традиционный анализ отличается от расширенного анализа и не может об-

рабатывать многоформатные данные, включая неструктурированные. По мнению А.Ф. Острякова и И.С. Митряева, фундаментальное различие между большими данными и достоверными данными заключается в их разнообразии, неточности и неубедительности [1]. В.П. Шумилин отмечает, что залог успеха любых подразделений правоохранительной системы деятельности в большинстве своем зависит от степени систематизированности информации [2].

В качестве основных этапов разработки программного обеспечения для ОВД можно выделить:

1. Анализ требований. На этом этапе проводится детальный анализ потребностей и требований пользователей, а также существующих процессов и систем. Важно учитывать специфику работы ОВД и особенности их информационных потоков.

2. Проектирование системы. Разрабатывается архитектура системы, включающая программные и аппаратные компоненты, способы защиты данных, методы резервирования и восстановления информации. Особое внимание уделяется вопросам безопасности и интеграции с другими системами.

3. Написание программного кода. Создается программное обеспечение, отвечающее всем требованиям, разработанным на предыдущих этапах. Включает разработку интерфейсов, модулей для обработки данных, механизмов защиты и контроля доступа.

4. Тестирование. Проводится комплексное тестирование системы, включающее функциональное тестирование, нагрузочное тестирование, тестирование безопасности и другие виды испытаний. Цель – выявить и устранить возможные ошибки и проблемы до начала эксплуатации.

5. Внедрение и обучение персонала. После успешного тестирования система внедряется в работу ОВД. Проводится обучение сотрудников, которые будут работать с новой системой, включая администраторов и конечных пользователей.

6. Сопровождение и поддержка. После внедрения системы важно обеспечить ее сопровождение и техническую поддержку, включая мониторинг работы системы, устранение возникающих проблем и обновление программного обеспечения.

В ОрЮИ МВД России имени В.В. Лукьянова осуществлялась разработка программного модуля «Строевая записка». Для реализации проекта были сформулированы следующие задачи и требования к информационной системе:

1. Обеспечение сбора и хранения данных о наличии постоянного и переменного л/с.

2. Автоматическое формирование ежедневных бумажных отчетов.

3. Интеграция с имеющейся системой автоматизации учебного процесса Апекс-ВУЗ.

4. Формирование аналитических данных.

Разработка и внедрение программы осуществлялась в несколько этапов:

1. Создание подсистемы сбора информации, которая используется для внесения сведений с бумажных носителей (рис. 1).

Рис. 1 – Подсистема сбора информации

2. Доступ пользователей к системе. Предоставляется возможность плавного перехода на электронный ввод данных (решение проблем, связанных с техническими возможностями отдельных подразделений).

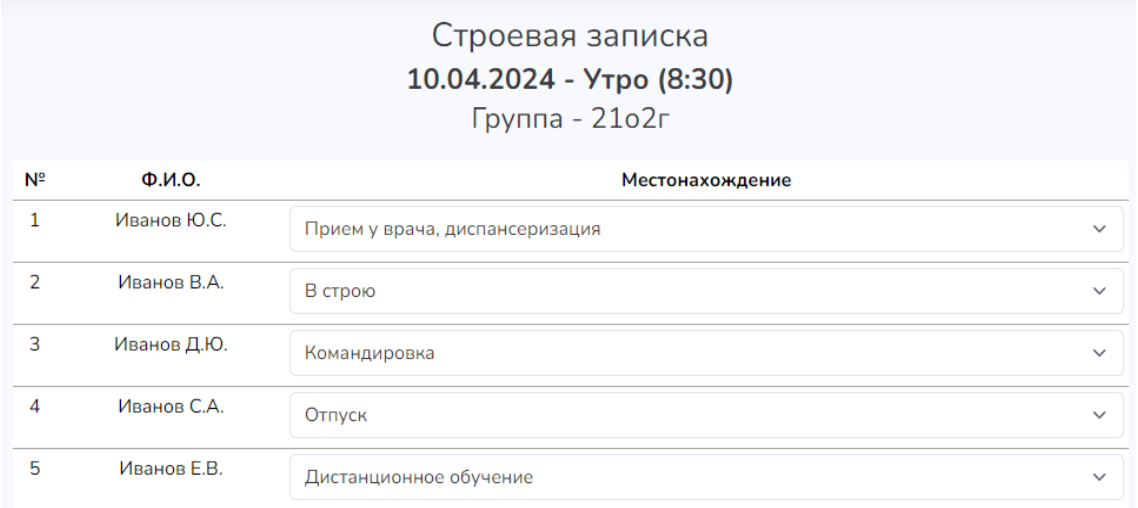

Рис. 2 – Окно ввода информации по подразделению

3. Доработка функциональных возможностей с учетом пользовательского опыта, итоговое внедрение.

Главное окно программы представлено на рисунке 1.

Рис. 3 – Главное окно программы

В качестве особенностей разработки и внедрения программы можно выделить следующее:

1. Автоматизация уже имеющейся деятельности. Поэтапно добавляются функции, и происходит плавное изменение алгоритмов действий сотрудников. Не требуется переобучение, можно внедрять в процессе повседневной работы. Отсутствие препятствия в виде сопротивления изменениям со стороны сотрудников.

2. Реализация плана действий на случай возникновения внештатных ситуаций.

3. Отсутствие персональных данных. В базе данных хранится только фамилия и инициалы, которые не позволяют однозначно идентифицировать субъекта, а значит, не требуют специальных мер по хранению и защите.

Положительные результаты выполненной работы:

1. Значительное сокращение времени на подачу сведений о наличии л/с. До этого приходилось приходить в дежурную часть.

2. Руководство института имеет необходимую информацию об отсутствующих до формирования итоговой строевой записки.

3. Доступ к данным и базовой аналитике способствует более качественной подготовке документов и устраняет ошибки, связанные с включением людей в списки и протоколы совещаний и советов в период их отсутствия.

4. Снижения количества ошибок, связанных с штатными изменениями. Заполняются только сведения об отсутствующих, а остальные данные заполняются автоматически.

5. Интеграция с Апекс-ВУЗ заключается в использовании общего справочника для личного состава. Кадровые изменения в Апекс-ВУЗ сразу отражаются в системе. Автоматическое выставление информации об отсутствующих в электронный журнал. Фактически курсовой офицер, заполняя данные об отсутствующих, сразу передает их преподавателю на учебные занятия.

Таким образом, разрабатывать качественное программное обеспечение для ОВД можно, но проектированием и проработкой деталей должны заниматься наиболее опытные сотрудники, имеющие полное представление о предметной области, совместно со специалистами в области информационных технологий. Необходимо планировать не только ввод в эксплуатацию, но и жизненный цикл программного продукта, его обновление и вывод из эксплуатации. При создании информационных систем необходимо обеспечить получение прав программный код и обеспечить его правильное хранение с использованием систем контроля версий Git.

Правовое регулирование создаваемых программных средств. Есть механизмы, касающиеся использования АИС, но не все про-

граммное обеспечение относится к данному понятию, а недостаточное регулирование ведет к опасениям сотрудников к использованию таких средств из-за возможных проверок и неоднозначного трактования.

В заключение следует отметить, что создание качественного программного обеспечения для ОВД требует участия опытных сотрудников, знакомых с предметной областью, и специалистов в области информационных технологий. Важно планировать весь жизненный цикл продукта, включая его обновление и вывод из эксплуатации.

---

1. Острякова А.Ф., Митряев И.С. Использование современных технологий в правоохранительных органах // Аграрное и земельное право. 2023. № 7 (223). С. 60–62. DOI 10.47643/1815-1329_2023_7_60. EDN HNRERD.
2. Шумилин В.П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4 (77). С. 173–176. EDN YPOGHB.

ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ТРАНСПОРТА

Капустина Е. Г.,
канд. пед. наук, доцент,
доцент кафедры административного
права и административной
деятельности ОВД
ОрЮИ МВД России
имени В.В. Лукьянова

Железнодорожный транспорт во все времена был наиболее востребованным у населения, в связи с доступностью и комфортностью. Стратегическое управление этой отраслью позволяет искать инновационные формы обеспечения транспортной безопасности, посредством совершенствования внедрения специальных технических средств.

К таким средствам на современном этапе развития железнодорожного транспорта относятся различные группы систем наблюдения и отслеживания движения поездов, такие как ГЛОНАСС, спутниковая навигация, а также встроенные в железнодорожное полотно путевые

датчики. Кроме того, в настоящее время используются автоматизированные средства сбора актуальной информации об обстановке на маршрутах следования поездов и прочих объектах железнодорожной среды.

К примеру, путевые датчики и связанные с ними управляющие системы предназначены для предотвращения столкновения поездов друг с другом и прочими средствами транспорта, людьми и иными объектами, а также схода поездов с рельс в случаях возникновения внештатных ситуаций на маршруте следования.

Путевые датчики представляют собой устройства, подключенные к железнодорожным светофорам, шлагбаумам, стрелкам и другим техническим устройствам. Они фиксируют движение поездов по железнодорожным путям в зоне действия. При получении данных о движении поезда в зоне обнаружения такой датчик посылает сигнал к пульту или системе управления. В результате обработки указанного сигнала автоматизированная система или правомочный сотрудник, управляющий пультом доступа принимает решение в связи с оперативной обстановкой на пути следования данного поезда.

Например, в случае если по пути движения поезда, образовалась аварийная ситуация, препятствующая его дальнейшему движению по заданному маршруту, путевой датчик подаст соответствующий сигнал в пункт управления. В пункте управления будет принято решение или об остановке данного поезда, или о смене маршрута его движения. В первом случае машинист получит информацию о необходимости прекращения движения, а на железнодорожных путях светофоры будут сигнализировать о запрещении движения, также сработает система автоблокировки движения данного поезда. Во втором случае, при наличии нескольких путей возможным будет решение о переключении стрелки и смены пути движения данного поезда при аварийных ситуациях и в иных экстренных случаях.

Кроме того, данная система направлена на увеличение пропускной способности железных дорог, так как машинисты поездов получают информацию о приближении или об удалении от станций на обеспечивающее безопасность расстояние других поездов, идущих по тем же железнодорожным путям.

Кроме того, светофоры, информационные таблички, системы экстренного оповещения и стрелки являются отдельными средствами организации безопасного движения поездов, способными работать как в автоматическом режиме, так и под ручным управлением.

Также следует обратить внимание на то, что особое место занимают системы быстрой связи машинистов поезда не только с пасса-

жирами и сотрудниками ближайших станций, но и специальными службами и подвижными наземными объектами железнодорожных служб. Так как скорость передачи наиболее важной информации способствует скорейшему реагированию и принятию необходимых мер, направленных на сохранение или восстановление безопасности на объектах железнодорожного транспорта и транспортной инфраструктуры.

Спутниковые системы навигации при движении поездов позволяют не только осуществлять мониторинг движения, но и вовремя реагировать на изменения в обстановке, складывающейся в пределах территорий объектов железнодорожного транспорта и инфраструктуры, принимать необходимые меры по срочному выезду к локализации аварий и прочих происшествий.

Перспективность использования спутниковой связи определяется несколькими показателями, такими как: неограниченная дальность связи, возможность обеспечения связи бесперебойно из любой точки маршрута следования поезда, относительная дешевизна использования, простота и удобство, высокая скорость передачи информации и связи.

В настоящее время на железных дорогах России большое распространение получила система «Сирена», разработка научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте – дочернего общества ОАО «РЖД». Система «Сирена» имеет различное исполнение: «Сирена-Р» – автоматическое речевое оповещение о приближении поездов к месту работ на стрелочных переводах малых станций; «Сирена-СР» – автоматическое речевое оповещение о приближении поездов к месту работ на стрелочных переводах станций с числом зон до 20; «Сирена-Ш» – оповещение о приближении поездов к месту работ на удаленных стрелках станций, а так же малых станций, с использованием шунта; «Сирена-РЦ» – автоматическое оповещение о приближении поездов к месту работ на перегоне, оборудованном кодовой автоблокировкой. Система «Сирена» построена на речевом и звуковом оповещении работников пути и других служб и дирекций, производящих работы на перегоне, стрелочных переводах станций, оборудованных электрической централизацией, о движении поездов по данной стрелке или группе стрелок, входящих в зону оповещения. Система по средствам радиосвязи сообщает работникам, находящимся в районе стрелочного перевода: об отсутствии поездов на участках приближения и возможности производства работ на данном участке перегона, стрелке; о приближении поезда к месту работ

на перегоне, стрелке (группе стрелок) и необходимости немедленно уйти на безопасное расстояние. Сигналы оповещения составляются при проектировании и записываются в ПЗУ [1].

Кроме названных технических средств, направленных на повышение уровня безопасной работы объектов железнодорожного транспорта, в частности от преступных действий пользователей данных объектов выступают средства видеонаблюдения, а также различные приборы досмотра. Видеокамеры позволяют не только контролировать состояние объектов охраны и прочих объектов железнодорожной инфраструктуры, но и способствовать предупреждению или оперативному реагированию на происшествия и аварии в работе вокзала и его элементов.

Помимо вышеуказанного, записи с данных видеокамер успешно используются сотрудниками полиции на транспорте при раскрытии преступлений и правонарушений, установлении личности.

В настоящее время практически все железнодорожные вокзалы и станции на территории РФ оборудованы специальными зонами для производства досмотра лиц, посещающих вокзал и иные объекты железнодорожной среды. Кроме того, как уже было отмечено ранее, вокзалы в таких зонах оснащены металлодетекторами и другими схожими техническими средствами обнаружения запрещенных и опасных предметов и вещей.

Так, Т.А. Березина отмечает, что на крупных вокзалах досмотровое оборудование в себя включает: аппаратуру радиационного контроля с функцией видеонаблюдения; стационарный многозонный металлообнаружитель; портативный обнаружитель паров взрывчатых веществ; портативную рентгено-телевизионную установку; стационарную сканирующую установку для досмотра багажа конвейерного типа; ручной металлоискатель [2].

Все эти средства техники применяются в отношении граждан, прибывающих на территории железнодорожных вокзалов и станций сотрудниками полиции на транспорте или ведомственной охраны, соответственно положениям федерального законодательства Российской Федерации, в целях обнаружения запрещенных к проносу вещей и предметов.

Использование технических средств обеспечения транспортной безопасности при проведении досмотра, дополнительного досмотра, повторного досмотра, регламентированного приказом Минтранса России от 23.07.2015 № 227 [3].

Кроме того, следует отметить, что законодателем в постановлении Правительства РФ от 26.09.2016 № 969 закреплены требования к

функциональным свойствам технических систем и средств досмотра, взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet [4]. Также следует отметить, что указанные средства должны быть подвергнуты поверке и сертифицированы в установленном законодательством РФ порядке.

Делая вывод, необходимо отметить, что для обеспечения безопасного состояния работы железнодорожных вокзалов, поездов и прочих объектов транспортной среды используется огромное количество специализированных средств техники, призванных повысить эффективность работы не только объектов транспорта, но и сотрудников правоохранительных органов при решении ими служебных и оперативных задач по охране общественного порядка и обеспечению транспортной безопасности. Рассмотренные приборы и устройства предназначены не только для контроля и мониторинга состояния подвижных составов поездов на маршрутах следования, но и состояния железнодорожного полотна и путей, а также платформ для пассажиров и станций в целях недопущения происшествий, влекущих не только материальный ущерб, но и угрозу безопасности людей, пользующихся объектами железнодорожного транспорта.

---

1. Щелконогов С.В. Анализ современных и перспективных систем предупреждения путевых работников о приближении подвижного состава [Электронный ресурс] // Молодой ученый. 2019. № 6 (41). С. 61–63. URL: https://moluch.ru/archive/41/4977.
2. Березина Т.А. Проведение досмотровых мероприятий на объектах железнодорожной инфраструктуры как мера предупреждения террористических актов [Электронный ресурс] // Молодой ученый. 2020. № 49 (339). С. 177–180. URL: https://moluch.ru/archive/339/75970.
3. Об утверждении Правил проведения досмотра, дополнительного досмотра, повторного досмотра в целях обеспечения транспортной безопасности [Электронный ресурс]: приказ Минтранса России от 23.07.2015 № 227 (ред. от 07.09.2020). Доступ из справ.-правовой системы «КонсультантПлюс».
4. Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности [Электронный ресурс]: постановление Правительства Рос. Федерации от 26.09.2016 № 969 (ред. от 17.04.2021). Доступ из справ.-правовой системы «КонсультантПлюс».

ВНЕДРЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ДОРОЖНОГО ДВИЖЕНИЯ

Жбанова С.А.,
канд. экон. наук,
заместитель начальника кафедры
кафедры организации деятельности
ГИБДД ОрЮИ МВД России
имени В.В. Лукьянова

Научно-технический прогресс предполагает применение передовых технологий, оказывающих существенное воздействие на различные области социальной жизни. Современные государства самостоятельно определяют и осуществляют свою национальную стратегию, направленную на внедрение современных, в том числе цифровых технологий, особое внимание уделяется инновациям, которые внедряются в различные общественные сферы.

Цифровизация транспортной индустрии – одна из важных составляющих стратегии развития Российской Федерации. И хотя это длительный многокомпонентный процесс, рассчитанный на годы, уже сегодня в стране удалось добиться ощутимых результатов.

Повсеместное применение информационных и автоматизированных систем в сфере транспорта и экономике в целом уже стало реальностью. Сейчас цифровое пространство преобразовывает работу всей транспортной отрасли. Показательный пример – изменение транспортно-логистических систем, причем как на уровне государственного контроля и управления, так и на уровне отдельных компаний.

Безусловно, серьезные изменения затронули и дорожную отрасль. Уже накоплен большой опыт использования цифровых технологий для решения практических задач. Речь идет о создании систем мониторинга транспортно-эксплуатационного состояния автомобильных дорог, в том числе с использованием интеллектуальных транспортных систем (ИТС), о создании цифровых двойников автомобильных дорог, о массовом внедрении технологий машинного обучения.

Главная федеральная программа в дорожной отрасли сегодня – национальный проект «Безопасные качественные дороги», рассчитанный до 2030 года. Среди основных целей – повысить качество жизни, привести дороги в соответствие с нормативами и снизить уровень аварийности и ДТП. Переход на этот этап развития отрасли

невозможен без внедрения и совершенствования цифровых технологий.

Проекты внедрения цифровых технологий организации дорожного движения наиболее полно находят воплощение в автоматическом управлении транспортными потоками, развитии интеллектуальных транспортных систем, взимании платы за проезд на отдельных участках автодорог, мониторинге дорожного движения и контроле режима движения в соответствии с Правилами дорожного движения. Указанные направления в полной мере коррелируют с положениями национального проекта Безопасные качественные дороги [1, с. 2]. Цифровизация занимает значительную часть плана мероприятий нацпроекта Безопасные качественные дороги. Она охватывает все жизненные циклы дорог – от строительства до эксплуатации. Вот некоторые примеры применения цифровых технологий в рамках нацпроекта:

1. Камеры контроля дорожного движения. Они фиксируют нарушения правил.

2. Автоматизированные системы весогабаритного контроля. Они позволяют следить за соответствием транспортных средств допустимым параметрам без остановки и дополнительного взвешивания.

3. Интеллектуальные транспортные системы. Они позволяют собирать, обрабатывать и распространять информацию о дорожном движении в реальном времени.

4. Беспилотные транспортные технологии. Они используются для мониторинга состояния дорожного полотна и инфраструктуры.

Кроме того, ведется работа по публикации части обрабатываемых данных в открытом виде. Создание подобных систем позволяет значительно повысить скорость получения данных заинтересованными лицами и снизить нагрузку, создаваемую запросами о предоставлении сведений [2, с. 126].

Цифровизация повышает безопасность и эффективность дорожного движения. Национальный проект Безопасные качественные дороги рассчитан до 2030 года, и среди основных его целей – повышение качества и доступности автодорог, улучшение дорожно-транспортной инфраструктуры и снижение уровня аварийности.

Сегодня дорожно-строительная отрасль постепенно переходит от бумажной документации к системному управлению жизненным циклом объектов на основе данных и цифровых моделей. Пока используемые в отрасли разрозненные системы плохо интегрированы между собой, на каждой стадии данные передаются в разных форматах – от 2D- и 3D-моделей до файлов Excel и PDF или документов в

бумажном виде. Уход за счет автоматизации от бумажных документов обеспечит бесшовную передачу данных и минимизирует ошибки, связанные с человеческим фактором. Единый источник информации позволит исключить потерю информации и повысить эффективность принятия решения.

Развитию строительства дорог в России помогут технологии цифрового моделирования BIM (Building Information Models). Цифровая модель зданий, сооружений и объектов инфраструктуры (инженерные сети, дороги, мосты, тоннели и др.) – это виртуальное представление характеристик объекта, формируемых на протяжении всего жизненного цикла строительства. Цифровое моделирование позволяет спроектировать полную модель дороги, включая местность, сооружения, инженерные коммуникации и сети. Единая цифровая платформа обеспечит всем участникам строительства доступ к полному спектру информации по объекту в режиме онлайн, чтобы оперативно учитывать риски и корректировать задачи. При внесении изменений в проект они отображаются на всех уровнях и для всех участников автоматически. Современные вызовы крупных городов диктуют необходимость использования инноваций, связанных с IT-решениями в дорожной отрасли.

Реализация таких работ помогает жителям безопасно и с большим комфортом передвигаться в городской среде, а городским службам – эффективнее и оперативнее справляться со своей работой. Благодаря поддержке нацпроекта по использованию «умных» систем регионы стали активнее включать новые технологии в процесс управления транспортом.

В качестве примера хотелось бы привести активное внедрение интеллектуальной транспортной системы в городе Курске. С помощью нацпроекта было установлено 15 «умных» светофоров. Кроме того, был осуществлен запуск системы приоритетного проезда общественного транспорта. Для обеспечения преимущественного проезда общественного транспорта на перекрестках были внедрены изменения в работу светофоров, которые переключаются адаптивно при задержке транспортных средств. Для удобства водителей установлены три динамические информационные табло, отображающие данные о скорости движения, погоде и других параметрах. Также установлено 80 датчиков, передающих информацию о транспортном потоке, скорости движения и загруженности дороги. Системы мониторинга и распознавания автомобильных номеров, видеоаналитика для выявления нарушений правил дорожного движения, умные светофоры и дру-

гие инструменты помогают контролировать ситуацию на дорогах и оперативно реагировать на возможные проблемы.

Актуальность и востребованность в современном мире беспилотных транспортных технологий бесспорна, данный факт подтверждается новыми возможностями для безопасного, эффективного и удобного передвижения как для грузовых, так и для пассажирских перевозок. Реализация цифровых технологий в систему обеспечения БДД сопряжено с рядом проблем, так на сегодняшний день, не проработано и регулирование ответственности при эксплуатации автомобилей в беспилотном режиме на дорогах: нормы, регламенты, процедуры, инструменты, кадры. И не только при ДТП автобеспилотников, но и в любых нештатных ситуациях, которые могут привести к срыву заказа на перевозку и убыткам для клиента.

Таким образом, внедрение цифровых технологий в управление организацией дорожного движения играет важную роль в современной транспортной инфраструктуре. Эти инновации способствуют повышению безопасности, эффективности и комфорта на дорогах, что делает их неотъемлемой частью развития городской среды и общественного транспорта. Кроме того, для успешного внедрения и использования ИТС требуется комплексный подход, включающий технологии, оборудование, компетентных специалистов для анализа полученной информации, а также взаимодействие между государственными органами, владельцами дорог и участниками дорожного движения.

---

1. Паспорт национального проекта «Безопасные качественные дороги» [Электронный ресурс]: утв. Президиумом Совета при Президенте Рос. Федерации по стратегическому развитию и национальным проектам. Протокол от 24.12.2018 № 15. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Семенов Е.Ю., Кобзина П.В. Возможности использования открытых данных в деятельности ГИБДД // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 1 (74). С. 125–127. EDN YSLHQQ.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

Белевский Р.А.,
канд. юрид. наук,
старший преподаватель кафедры
информационных технологий
в деятельности ОВД
ОрЮИ МВД России
имени В.В. Лукьянова

Интернет в наше время занимает очень важное и практически главенствующее место: в интернете люди зарабатывают деньги при помощи коммуникаций, при помощи социальных сетей люди всего мира могут общаться друг с другом на самых различных расстояниях, в интернете также происходят знакомства, любые услуги и покупки можно сделать и совершить при помощи этой уникальной сети, а главное – все это происходит с очень высокой скоростью. Перечислять плюсы интернета можно безгранично.

Несмотря на все его достоинства и качество, интернет был и продолжает с каждым разом становиться все более опасным местом. Это чистое поле для любых мошеннических действий и операций. В интернете хранится большой пласт информации практически о каждом человеке в мире: начиная от его простой фотографии, заканчивая паспортными данными.

В связи с этим мошеннические преступления вышли на новый и более опасный уровень. Люди совершают преступления, не выходя из дома, при помощи лишь интернета, любого гаджета и небольших программ, которые помогают им получить доступ к любой базе данных, в которой как раз и хранятся сведения о лицах.

Е.Ю. Семенов отмечает, что решение данной проблемы из-за развития информационно-телекоммуникационных технологий выходит за рамки возможностей одного государства и носит глобальный масштаб. Необходимы новые подходы как для организации законной деятельности в данной области, так и для предотвращения возможных угроз и обеспечения безопасности субъектов персональных данных [1].

Используя персональные данные, мошенники совершают операции с крупными суммами денег. Современные преступники со своими технологиями и изобретательными программами ухитряются похитить денежные средства с карты любого клиента, либо взять большую сумму на человека в кредит.

Данный вид преступления – самый опасный. Это обуславливается тем, что современные органы внутренних дел еще недостаточно продвинулись и усовершенствовались для раскрытия преступлений, связанных с интернетом.

Помимо всего прочего, несмотря на то, что интернет продолжает занимать лидирующее место в жизни человека, законодательство Российской Федерации в этом плане совсем не продвинулось. Более того, нет ни одного нормативно-правового акта, который бы регулировал вопрос защиты персональных данных в сети Интернет.

Расскажем более подробно о видах интернет-мошенничества.

Фишинг – это вид интернет-мошенничества, цель которого – это получение личных данных и сообщений пользователей, а также паролей и логинов [2].

Данное мошенничество реализуется при помощи проведения массовых рассылок электронных писем от каких-либо известных отправителей. Также такие рассылки случаются и среди личных СМС пользователей внутри социальных сетей, либо сервисов, таких как «Сбербанк» и т.д.

В таких сообщениях, как правило, содержатся ссылки на фальшивые сайты, которые внешне совсем неотличимы от подлинного, или ссылка на сайты с редиктором.

Сразу после того, как пользователь переходит на такую страницу, интернет-мошенники всевозможными психологическими приёмами пытаются воздействовать на него для получения пароля или логина. Если пользователь ввёл данные, используемые в доступе к личным данным на других сайтах, то мошенники могут очень просто получить доступ к аккаунтам на других сайтах и даже банковским счетам.

Такой вид интернет-инженерии, как фишинг, основан, прежде всего, на незнании пользователем главных основных способов безопасности в сети. Многие просто не знаю того, что сервисы не рассылают писем с просьбами сообщить свои логины, пароли либо другие учётные данные.

Для того чтобы можно было защититься от фишинга, многие производители основных интернет-браузеров, например, Яндекс, создали одинаковые способы предупреждения пользователей о том, что они зашли на фишинговый либо подозрительный сайт, который может быть создан мошенниками. Такая система оповещения пользователей называется антифишингом.

Один из методов борьбы с фишингом – это обучение пользователей различать поддельные страницы, а также бороться с ними. Каж-

дый может снизить и даже устранить угрозу мошенничества, стоит лишь изменить своё поведение и быть немного внимательнее.

Иногда самым верным способом защититься от фишеров – это всего лишь проверка ссылки, на которую вы собираетесь перейти, на подлинность. Чтобы это сделать, нужно просто ввести настоящую ссылку компании или сайта в поисковую строку Браузера. Интернет сам переведёт вас на неподдельный сайт, останется лишь сравнить две ссылки.

Следует запомнить, что все сообщения от подлинных отправителей включают в себя информацию, недоступную для интернет-мошенников.

Фарминг – это вид кибер-атаки, который предназначен для перенаправления трафика веб-сайта на другой, поддельный сайт.

В основном фарминг является угрозой для крупных фирм и предприятий, которые занимаются интернет-банкингом или моделированием сайтов электронной коммерции.

Для борьбы с фармингом были придуманы непростые методы, так называемые, анти-фарминги, но многие из них оказываются неэффективными для борьбы с этой угрозой [3].

Сейчас создано новое антивирусное программное обеспечение и специальное программное обеспечение для распознавания и удаление программ-шпионов. Данные программы довольно сильные, могут защитить от фишинга, но даже от фарминга они не могут огородиться.

Существует два вида фарминга.

Одна из них заключается в установке хакерами вредоносного программного обеспечения на компьютеры и ПК пользователей. Затем вредоносный вирус, внедрённый на компьютер, перенаправляет пользователя с первоначального подлинного сайта (онлайн-банка или маркета) на поддельную страницу, которую пользователь хотел посетить изначально. Поддельные страницы практически невозможно отличить, т.к. визуально они ничем не отличаются от оригинальной [4].

Еще один вид фарминга заключается в инфицировании всего сервера DNS, из-за чего потом каждый посетитель автоматически перенаправляется на мошеннический сайт. Этот вид фарминга считается самым разрушительным и вредоностным [5].

Эффективным и почти единственным способом защиты от данного вида интернет-мошенничества является использование надёжной антивирусной программы, позволяющей при выходе в интернет надёжно защитить DNS сервер и обеспечить защищённое соединение с сайтом. Такие антивирусные программы защищают от сетевой активности, обеспечивают надёжную защиту аккаунтов, а также способны проверять сайты на уровень угрозы.

Существуют и другие виды интернет-мошенничества, к примеру:

- кликджекинг;
- вишинг;
- смишинг.

Многие современные антивирусные программы и интернет Браузеры предусматривают защиту от хакерских и фишинговых атак [6]. Они обустроены специальными программами, которые могут закрывать фарминговые сайты, блокировать подозрительные письма от неизвестных адресатов. Во многих из них предусмотрена защита конфиденциальных данных пользователя – это означает, что запросе о получении информации о данных пользователя, интернет будет просить о вводе информации, которую могут знать только пользователь или сама социальная сеть.

Таким образом, можно заметить, что официальные сайты и компании всегда стараются защитить своего пользователя от подобных фишинговых атак. Но решение всегда принимает сам человек – будет ли он настороже и внимателен или самостоятельно отдаст свои персональные данные злоумышленникам при первой же хакерской атаке.

---

1. Семенов Е.Ю., Лысенко Е.С. Проблемы правового регулирования автоматизированной обработки общедоступных персональных данных // Вестник Уфимского юридического института МВД России. 2021. № 4 (94). С. 44–48. EDN ISQUQG.
2. Мазуров В.А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции [Электронный ресурс] // Вестн. Том. гос. ун-та. 2018. № 300-1 URL: https://cyberleninka.ru/article/n/prestupnost-v-sfere-vysokih-tehnologiy-ponyatie-obschaya-harakteristika-tendentsii (дата обращения: 31.03.2024).
3. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение [Электронный ресурс] // Власть. 2017. № 8. URL: https://cyberleninka.ru/article/n/kiberprestupnost-globalnaya-problema-i-ee-reshenie (дата обращения: 30.04.2024).
4. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц [Электронный ресурс] // Российское право: Образование. Практика. Наука. 2020. № 3 (93). URL: https://cyberleninka.ru/article/n/o-nekotoryh-sovremennyh-sposobah-soversheniya-moshennichestva-v-otnoshenii-imuschestva-fizicheskih-lits (дата обращения: 31.03.2024).
5. Никитина И.А. Финансовое мошенничество в сети Интернет [Электронный ресурс] // Вестн. Том. гос. ун-та. 2020. № 337. URL:

https://cyberleninka.ru/article/n/finansovoe-moshennichestvo-v-seti-internet (дата обращения: 10.04.2024).
6. Шумилин В.П. Проблемы законодательства о киберпреступности // Аграрное и земельное право. 2022. № 5 (209). С. 137–140.

ЗНАЧЕНИЕ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕСС ОБУЧЕНИЯ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Недоступенко Т.А.,
старший преподаватель кафедры
уголовно-правовых дисциплин
БЮИ МВД РФ имени И.Д. Путилина
Коюда М.В.,
курсант БЮИ МВД РФ
имени И.Д. Путилина

В современном мире важно знать основы работы с информационными технологиями. Каждому человеку подобная база знаний станет полезной для эффективного процесса жизнедеятельности, ведь практически все сферы в настоящее время связаны с Интернетом и техникой. Приобретение навыков использования информационных технологий в своей повседневной деятельности сотрудниками органов внутренних дел Российской Федерации (далее – ОВД РФ) является в настоящее время обязательной составляющей. Это связано с тем, что преступная среда постоянно прогрессирует и многие противоправные деяния совершаются как в сети Интернет, так и с использованием технологических ресурсов. Правонарушители изучают различные основы информационных технологий, информатики и программирования, а также разбираются в особенностях современных социальных сетей и мессенджеров, что позволяет им осуществлять свою деятельность и достигать поставленных целей с большей вероятностью успеха.

Так, согласно отчету, представленному официальным представителем МВД России И.В. Волк число ИТ-преступлений в России за 2023 год выросло на 29,7 % в сравнении с 2022-м. Обращено внимание на то, что каждое третье преступление в России по итогам 2023 года совершено с использованием информационно-телекоммуникационных технологий. Раскрываемость таких уголовно наказуемых деяний в 2023 году увеличилась на 21 % [1].

Представленная статистика свидетельствует не только о распространенности преступлений в сети Интернет, но и на то, что суще-

ствует положительная динамика в освоении и использовании информационных ресурсов сотрудниками ОВД.

Внедрение информационных технологий в процесс обучения сотрудников органов внутренних дел Российской Федерации выступает отправным шагом к повышению уровня раскрываемости, ведь сотрудники полиции не всегда своевременно ознакомляются со всеми изменениями, происходящими в информационной среде, и тем самым упускают возможность эффективной борьбы с преступностью. Именно поэтому во время прохождения курсов по повышению квалификации необходимо получить знания относительно развивающихся современных технологий и способов их использования.

Прежде чем вести речь о приобретении навыка использования существующих технологических ресурсов, а это могут быть не только технико-технологические ресурсы, но и информационные (программы, приложения и др.) следует обратить внимание на отдельные вопросы, затрагивающие процесс их обучения.

Современные реалии таковы, что в системе МВД при обучении сотрудников ОВД широкое распространение получил формат дистанционного обучения. В свете этого, вопрос применения информационных технологий в процесс обучения приобретает большую актуальность.

Использование подобной модели обучения предоставляет ряд очевидных преимуществ, на которые следует указать.

Так, большее число сотрудников ОВД получают возможность прохождения курсов повышения квалификации, в том числе, при нахождении в отдаленных участках местности. Отсутствие необходимости в командировке влечет снижение финансовых издержек. Увеличивается возможность принятия участия в большем количестве курсов. Сотрудник ОВД имеет возможность получать знания и формировать навыки без длительного отрыва от трудовой деятельности. Своевременно и в кратчайшие сроки информируется об использовании новых способов ведения преступной деятельности и о разработанных соответствующих мерах предупреждения. Все это позволяет увеличить общий объем знаний о мире, в том числе, повышает эффективность жизнедеятельности в целом.

При игнорировании данного вопроса могут наступить негативные последствия. Например, к таковым относится снижение компетентности сотрудников, что, ведет к общему снижению результативности деятельности всего коллектива, что отражается на статистических данных относительно прогрессивности работы ОВД РФ.

Еще в тот период, когда компьютеры стали использоваться повсеместно в образовании, появилось соответствующее понятие «новая

информационная технология обучения» [2]. Так и в настоящий момент без компьютера довольно затруднительно представить процесс работы или обучения. Практически все педагоги и многие другие профессионалы в своей деятельности применяют такое средство как способ методической работы. При этом на занятиях по повышению квалификации сотрудников ОВД РФ преподаватель решает самостоятельно какие программы и в каком количестве часов будут изучаться [3].

Кроме того, стоит отметить, что в процессе обучения использованию информационных технологий сотрудниками необходимо придерживаться тем основам образования, которые разработаны и существуют на сегодняшний день. Так, например, лекции являются не самым актуальным способом, а как раз практическая деятельность выступает в качестве ключевых, что объясняет важность работы на компьютере.

Всемирно известный исследователь в области использования аудиовизуальных материалов в обучении Эдгар Дейл, являясь профессором Государственного университета штата Огайо, выявлял и анализировал способность обучаемых воспроизводить полученную информацию. Результаты эго исследований были оформлены в виде «Dale's cone of experience» (известном как конусе Дейла) [4] и представлена на рис. 1.

Рис. 1 – Пирамида усвоения информации в процессе обучения

Изучив представленную информацию, связанную с построением алгоритма обучения, необходимо определить, какие же задачи перед собой ставит процесс внедрения информационных технологий в постоянную деятельность и работу сотрудников ОВД РФ.

Так, например, в качестве первой выделяется обеспечение возможности использования программно-телекоммуникационного обеспечения. Сотрудникам необходимо понимать различие между тремя типам программного обеспечения: прикладное, системное и инструментальное. Второй задачей выделяется развитие познавательной деятельности у сотрудников с возможностью использования компьютерной техники, программ и информационных технологий в процессе несения службы.

Конкретно же в среде образовательной деятельности в качестве задач ставятся следующие: создание автоматизированных мест для обучения методам и способом использования техники и технологий сотрудниками, подготовка и формирование условий для эффективного взаимодействия субъектов, то есть преподавателей и обучающихся в лице сотрудников ОВД РФ, с объектами, представленными в виде конкретных знаний в сфере информационной деятельности. Кроме того, также обозначается необходимость изменения предметной среды через широкое внедрение в обучение в процессе повышения квалификации компьютеров и иных технологий и техники [5].

Для решения поставленных задач высоко результативным выступает указанный ранее формат дистанционного обучения, при котором сотрудник напрямую самостоятельно сможет пользоваться технологиями в процессе образовательной деятельности. При этом подобный формат обладает собственными содержательными составляющими, включающими различные аспекты, что представлено на рис. 2.

Рис. 2 – Составляющие дистанционного обучения
в процессе изучения информационных технологий

Однако также следует указать, что подобный формат эффективен для сотрудников за счет большого количества ресурсов. Во-первых, к таковым относятся источники, представленные непосредственно в сети Интернет. Во-вторых, контроль знаний с помощью тестирования на компьютере. В-третьих, компьютерные программы и различные веб-квесты, позволяющие углубиться в интересующие области знаний. В-четвертых, также способность общаться с преподавателем и другими обучающимися в лице сотрудников с помощью видео- и аудиозаписей. Кроме того, возможен формат чатов, который позволяет реагировать на поступающие сообщения и вопросы по мере возможности и имеющегося времени, что действительно актуально при загруженности деятельности сотрудников ОВД РФ в настоящее время.

Также важным аспектом будет выделение трех форм дистанционного обучения. К ним относятся следующие: синхронная, асинхронная и смешанная соответственно. Третий тип заключается в объединении признаков первого и второго, что и определяется его названием. Однако синхронный и асинхронный нуждаются в более подробном пояснении (рисунок 3).

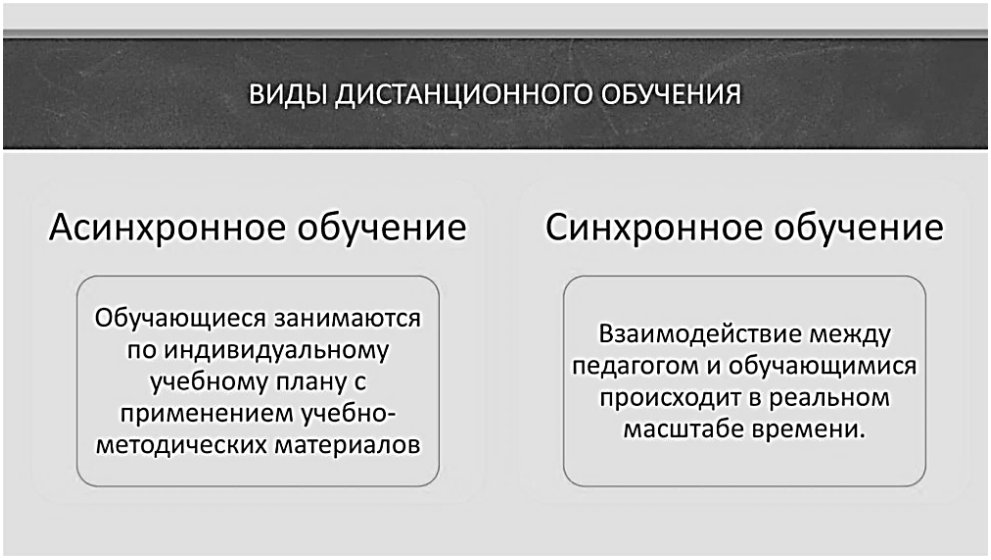

Рис. 3 – Синхронное и асинхронное дистанционное обучение

Так, например, синхронное дистанционное обучение — это возможность поддержания постоянного и тесного контакта, обучающего и обучаемого. Представленный формат включает в себя проведение онлайн-занятий в процессе изучения курса по овладению навыками использования информационных технологий в процессе служебной

деятельности. Все задания выполняются согласно составленному расписанию [5].

В свою очередь, при асинхронном обучении приоритет ставится на самостоятельность сотрудников. Им необходимо в свободной форме, в любое удобное время проходить тесты, слушать лекции и выполнять различного рода задания для прохождения курса по овладению навыками использования информационных технологий в процессе служебной деятельности соответственно. При данном формате преподаватели мало взаимодействуют с обучающимися и не поддерживают постоянный контакт.

Выбор формата обучения зависит от конкретного института, в котором сотрудники ОВД РФ будут проходить курсы по повышению квалификации. Кроме того, можно даже ввести возможность каждому сотруднику, то есть обучающемуся, определять наиболее приоритетный для него формат. Это все позволит углубиться в информационные технологии, основы информатики и программирования.

Таким образом, внедрение информационных технологий в процесс обучения сотрудников органов внутренних дел Российской Федерации видится шагом значительным и эффективным. Применение современных информационно-коммуникационных средств в процессе служебной деятельности требует использования современной техники обучения, которую необходимо активно внедрять в курсы повышения квалификации. Важно обучать сотрудников всем основам информационных технологий, так как в современных условиях развития общества практически все сферы становятся охвачены информатизацией и компьютеризацией, в том числе и преступная среда. Поэтому для эффективной борьбы с преступностью необходимо все чаще использовать информационные технологии в обучения сотрудников, включая формат дистанционного получения образования.

---

1. Киберпреступность и киберконфликты: Россия [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (дата обращения: 06.03.2024).
2. Бадраа С. Организация использования информационных технологий для обучения сотрудников и работников ОВД РФ // World science: problems and innovations. 2023. С. 134–139.
3. Кецко К.В. Преступность в сфере электронной коммерции // Российский следователь. 2021. № 9. С. 58–63.
4. Пирамида обучения [Электронный ресурс]. URL: https://viva-school.blogspot.com/2016/06/blog-post.html (дата обращения: 06.03.2024).

5. Смирнова А.Н. Исследование социально-экономических предпосылок реформирования государственной службы. М.: Литера, 2021. С. 198.
6. Яковцов С.А. Дистанционные образовательные технологии в системе профессиональной подготовки сотрудников ОВД России // KANT. 2022. № 3 (44). С. 303–307.

ЦИФРОВАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ СОТРУДНИКОВ ПОЛИЦИИ ПРИ ВЕРИФИКАЦИИ ВИДЕОИНФОРМАЦИИ

Толстых М.Ю.,
доцент кафедры СИТ УНК ИТ
МосУ МВД России имени В.Я. Кикотя

На расширенном заседании коллегии МВД России минувшего года Президентом Российской Федерации было отмечено, что одним из безапелляционных приоритетов работы министерства выступает борьба с преступлениями, которые совершаются благодаря использованию инфокоммуникационных технологий [1]. По результатам 2023 года количество уголовно наказуемых деяний данного вида составило более полмиллиона – четверть от всех преступлений. Независимо от того, что отмечается активное внедрение новаций в методологии обеспечения безопасности и противостояния дистанционным действиям преступников, обнаруживаются и блокируются уголовно наказуемые манипуляции в цифровом пространстве, крайне важно регулярно информировать общество о современных разновидностях указанных преступлений, объяснять, как защитить себя от них, в целом повышать цифровую грамотность и кибергигиену граждан.

В современных реалиях проблема дезинформации воспринимается губительней и значимей, чем, например, явление эпидемий, поскольку первая распространяется со скоростью света по всему земному шару и может оказаться смертельно опасной, когда усиливает неуместное личное предубеждение против всех заслуживающих доверия доказательств. Популярной вариацией представления сфальсифицированного контента выступают дипфейки. Угроза, которую они представляют, заключается в их способности распространять ложную информацию, которая в понимании реципиентов исходит из надежных источников.

Обозначенные угрозы справедливы и в отношении силовых структур, государственных учреждений и организаций, личному составу которых в силу их должностных обязанностей требуется оперативно детектировать и блокировать деструктивное влияние сфабрикованного контента новостного характера, либо видеоматериалы и аудиозаписи, стремительное распространение и увеличение которых имеет все шансы трансформироваться в очевидную преступную деятельность, направленную против государственной власти (экстремизм, терроризм, диверсии и пр.).

Таким образом, востребованы определение способов и разработка средств противостояния указанной угрозе безопасности, которые могут быть внедрены в деятельность подразделений органов внутренних дел Российской Федерации.

Под дипфейками, как правило, понимаются обработанные видео или другие цифровые изображения, созданные сложным искусственным интеллектом, которые создают сфабрикованные изображения и звуки, которые кажутся реальными. Это также могут быть и тексты, сгенерированные искусственным интеллектом. Система глубокого обучения может создать убедительную подделку, изучая фотографии и видео целевого человека с разных сторон, а затем имитируя его поведение и речевые модели. Наиболее популярные технологии создания дипфейков приведены на рисунке 1.

Рисунок 1 – Технологии создания фейкового визуального контента

Для противостояния множествам видов дезинформации принципиально важно определить основы, составить архитектуру и выработать протоколы (рекомендации) по созданию в государстве комплексной оппозиционной системы, противостоящей стремительному распространению фейков и нивелированию их воздействия на общество, а также ограничению каналов их распространения. Система, инкапсулирующая эффективные и проверенные формы, методы и технологии как активной, так и пассивной защиты, должна поддерживать прочные связи правительственных учреждений и вне властно-государственных структур на базе неполитических отношений, обеспечить информационную безопасность, кибергигиену и цифровую культуру.

На сегодняшний день некоторые подразделения МВД России реализуют комплекс мер по противодействию распространению недостоверной информации. В частности, специальные структуры министерства выполняют мониторинг и пресечение противоправных действий в глобальной сети, поиск потенциальных экстремистов или террористов, мошенников. В штат наравне с оперативными работниками входят аналитики и специалисты в компьютерной сфере, в области обеспечения кибербезопасности и защиты от компьютерных атак.

Наиболее результативным из неавтоматизированных способов проверки информации и доступным с точки зрения вовлекаемых ресурсов и средств является так называемый фактчекинг [2]. Понятие семантически отнесено к традиционной журналистике, базовому принципу существования и работы редакции – фильтрации, что коррелирует с аксиологическими основами: объективность и беспристрастность в создании контента, что обуславливает доверие аудитории.

На наш взгляд, целесообразно применять традиционные методы и средства фактчекинга и продвинутые технологические ресурсы и сервисы совместно: контроль и оценка медиапространства результативны для обнаружения требуемого контента по маркерам, метками или дескрипторам (тегам), ключевым формулировкам и определению точного географического местоположения устройства в разных средах распространения. Очевидно, что человеческий ресурс не является в данном процессе заменой автоматизированным технологиям. Одновременно признается, что компьютерные системы и современные цифровые ресурсы несовершенны, в этой связи ключевые решения должны исходить от специалистов и экспертов, но применение современных технологий способно максимально оптимизировать требующую концентрации внимания или рутинную работу, предлагая собой системы поддержки принятия решений (СППР).

Предлагается создание программного приложения, которое можно отожествить с СППР, основанной на обучении нейронных сетей. Приложение возможно эксплуатировать процессе деятельности сотрудников полиции с целью верификации подозрительного графического контента. Основные концептуальные положения, характеристики и параметры эффективности системы, основанной на обучении искусственных нейронных сетей, представлены в табличной форме (таблицы 1, 2).

Таблица 1

Характеристика СППР (с точки зрения построения и работы)

Критерий	**Значение**
Тип задачи машинного обучения	Задача бинарной классификации (ЗБК)
Датасет	1000 исходных видео с докладчиками
Дипфейк технология	Deepfakes, Deepfakes, Face2Face, FaceSwap, NeuralTextures
Выделение лица	Функционал «insightface» с доработкой в виде фреймофрков от Github
Конвейер обучения модели	Выделение участка изображения с лицом; сумма по трем изображениям по каналам; решение ЗБК с помощью сети ResNet50
Решение проблемы деградации	Внедрение глубокой остаточной структуры сети

Таблица 2

Метрики качества на тестовых данных спроектированной модели

	F1-score	**Precision**	**Recall**
Accuracy	0,62		
Macro avg	0,61	0,66	0,62
Weighted avg	0,61	0,66	0,62
0 – ложь (фейк)	0,69	0,59	0,85
1 – истина (оригинал)	0,52	0,73	0,40

В классификации положений Инструкции по формированию и ведению фонда алгоритмов и программ МВД России, утвержденной приказом [3], указанное специализированное программное обеспечение может быть охарактеризовано следующими параметрами (таблица 3).

Таблица 3

Возможная характеристика СППР
как объекта учета в фонде алгоритмов и программ

<table>
<tr><th>Тематический классификатор</th><th colspan="2">Техническое и информационное обеспечение</th></tr>
<tr><td rowspan="3">Вид</td><td colspan="2">специализированные клиентские приложения в комплекте, программное обеспечение типовой внутренней деятельности органов государственной власти, включающей:</td></tr>
<tr><td>справочно-информационное обеспечение</td><td>системы обработки и анализа данных</td></tr>
<tr><td colspan="2">универсальные программы для обработки и анализа массивов данных, в том числе статистической, экономической, социологической информации</td></tr>
</table>

В данной работе было рассмотрено явление графической фейковой информации как актуальной угрозы информационной безопасности, предложена техническая разработка, которую возможно интегрировать в работу структур силового блока, обеспечивающего безопасность общества и государства.

Предлагаемая концепция СППР в части верификации подозрительной информации на предмет дипфейка реализована в программном виде, инкапсулирующем технологии работы с нейронными сетями. Очередным этапом работ по модификации решения может быть создание дружественного пользовательского интерфейса для обеспечения удобства работы с имеющейся моделью.

Разработанное решение представляется применимым для обеспечения подразделений системы МВД России специализированным программным обеспечением, предусматривающим расширение области своего применения (масштабируемость, т.е. установку клиентской части на автоматизированные рабочие места большинства сотрудников, интегрирование потоков данных, их агрегацию и дообучение модели в серверной части). Программа сможет также способствовать созданию эффективного механизма для получения актуальной и достоверной информации сотрудниками органов внутренних дел Российской Федерации.

---

1. Сайт Администрации Президента России: Событие «Расширенное заседание коллегии МВД» 20 марта 2023 года, Москва [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/70744.

2. Фактчекинг как инструмент развития медиа и современного медиаобразования: материалы Всероссийской научно-практической конференции с международным участием (Новосибирск, 1–2 октября 2020 г.) / Министерство просвещения Российской Федерации, Новосибирский государственный педагогический университет, Институт филологии, массовой информации и психологии. Новосибирск: НГПУ, 2021. 165 с.
3. Об утверждении Инструкции по формированию и ведению фонда алгоритмов и программ МВД России: приказ МВД России от 20.04.2017 № 271 (в ред. приказа ФКУ НПО «СТиС» МВД России от 11.02.2019 № 103).

ПОДХОДЫ К СОЗДАНИЮ ШАБЛОНА ПОЛЬЗОВАТЕЛЯ МОБИЛЬНОЙ СВЯЗИ В ИНТЕРЕСАХ СЛЕДСТВИЯ

Карпика А.Г.,
канд. тех. наук, доцент,
доцент кафедры информационного
обеспечения ОВД РЮИ МВД России

За последние несколько десятилетий данные мобильного телефона превратились в отдельную тему исследований. Из-за широкого использования смартфонов, цифровые следы, оставшиеся от использования смартфона, предоставляют ценную информацию о человеке в реальном времени.

Эти цифровые следы облегчают изучение поведения человека, что во многих случаях может стать решающим фактором при проведении расследования преступлений. Различные методы и аналитические модели используются для выявления многих аспектов поведения на основе данных мобильного телефона, которые собираются, регистрируются и обрабатываются различными приложениями.

Такие данные, как мобильность пользователя, его модель общения, активность в социальных сетях, участие в общественных мероприятиях с использованием мобильных телефонов представляют собой набор различных пространственно-временных характеристик, а также данных о вызовах, которые могут быть извлечены из устройства.

Например, в контексте криминологии, для раскрытия уголовной сети используются следы общения, которые были оставлены преступ-

никами в течение определенного периода времени и определенного места.

Так, следы, как правило, включают подробную информацию о местах, где преступники получили звонки, временные метки их связи, частота их звонков и периоды их деятельности. Собранные в течение определенного периода времени следы дают представление о моделях общения соответствующих лиц, которые затем могут использоваться для выводов об их преступной деятельности и взаимоотношений.

Так, анализ некоторых источников [1; 2] показал, что анализ следов мобильности преступников на основе их цифровых следов, которые они оставили в своих дома и в других значимых местах (например, на месте преступления), позволил определить, являлись ли перемещения преступников регулярными или случайными. Впоследствии следователи выяснили, что в перемещениях преступников была высокая степень пространственной регулярности.

Пространственно-временные модели мобильности вместе с моделью использования мобильного телефона также могут быть извлечены из данных мобильного телефона для проведения других оперативно-разыскных или следственных мероприятий, например, таких как выявление подозрительной деятельности отдельных лиц, с привязкой к городскими зонам, районам, транспорту.

Шаблон активности. Эта функция представляет общий объем взаимных вызовов (количество входящих и исходящих звонков, сделанных из всех смартфонов), подключенных к одному сотовому ретранслятору в течение определенного периода времени. При этом другие исследователи предлагают создавать шаблоны, основываясь на изменениях активности с течением времени (временные изменения). Они предлагают анализировать данные о количестве вызовов мобильного телефона каждый час в течение недели.

В этой модели выявление человеческого поведения основывается на шаблонах активности (общее количество вызовов) зарегистрированное базовой станцией еженедельно каждый час с понедельника по воскресенье.

Еще одним примером практического применения извлечения шаблонов активности мобильного телефона является отображение распределений групп населения на основе их мобильности. Такой подход позволяет объединить местоположение человека и его мобильность в пространстве и времени, что позволяет анализировать пространственно-временную динамику жителей района, города. Здесь множественные пространственно-временные характеристики могут быть использованы для иллюстрации моделей мобильности человека.

Например, базовая станция идентифицирует географическое местоположение смартфона, с которого был сделан, или получен звонок, так как смартфоны регулярно подключаются к ближайшим сотовым вышкам вместе с временной меткой, фиксирующей том, когда произошло интерактивное событие. Анализ также показывает, являются ли пользователи более активными в дневное или ночное время, в зависимости от того, когда были сделаны звонки.

Различают два типа данных мобильного телефона. Один из них содержит детали взаимодействия между мобильным устройством и сетью. Он описывает данные мобильного телефона и некоторые события. Другой тип данных основан на местоположении сотовой вышки. В первом типе данные содержат детали событий связи, которые происходят, когда мобильные телефоны получают или инициируют телефонные звонки, текстовые сообщения или доступ к Интернету. Подробная информация о каждом сеансе содержится в записи, которая включает в себя идентификатор Caller ID, продолжительность вызова и метка времени.

Этот тип называется «мобильный на основе событий». Здесь данные передают подробности о ведении связи и мобильности каждой стороны, участвующей в вызове на уровне группы (где данные агрегируются на основе группировки определенного количества пользователей в определенной области на основе их соединения с сотовой вышкой в различных пространственных и временных масштабах). Агрегированные данные могут предоставить соответствующие детали, включая идентификатор пользователя, временную метку и идентификатор вышки сотовой связи для каждого из участников вызова. Агрегированные данные мобильного телефона (обычно называемые агрегированными записями, или данными мобильного телефона на агрегированном уровне) отличается от отдельных данных (называются данными мобильного телефона на индивидуальном уровне или данные CDRS) в том смысле, что они анонимно агрегируется в разных пространственных и временных масштабах.

Таким образом, их легче собирать и анализировать, а их обработка проще по сравнению с отдельными данными, потому что они агрегируются на основе устройств мобильных телефонов, которые подключены к сотовой вышке в разных пространственных и временных масштабах.

В результате это позволяет осуществлять наблюдение и мониторинг пространственных и временных колебаний деятельности жителей определенной территории при различных видах измерений

(например, почасовых, ежедневных, сезонных) на основе их моделей перемещения.

Классификация и кластеризация пользователей по параметрам, полученным из информации о местоположении, например посещаемые места или наиболее частые места, в которых присутствуют пользователи. Это позволит отображать уровень мобильной активности в конкретном месте. Результат может быть получен из агрегированных данных, которые отражают пространственно-временные модели мобильности и коммуникационное поведение.

Определение пассивного местоположения мобильного устройства в базовой станции происходит через регулярные промежутки времени, а также всякий раз, когда мобильное устройство включается или выключается, получает сигнал от мобильной сети или изменяет тип соединения. Этот тип данных хранит запись, в которой подробно описывается каждое событие, включая идентификатор Caller ID, метку времени и местоположение (идентификатор соты), где каждая запись геолокации формируется на основании ближайших станций, к которым подключено мобильное устройство.

Таким образом, в каждой географической области существует определенное количество станций, которые охватывают данную область, чтобы обеспечить качество службы связи и оптимизацию нагрузки на соту.

Пространственно-временная информация, предоставленная данными мобильного телефона, может предоставить данные о взаимодействии пользователей в различных ситуациях, например, для изучения взаимосвязи между активностью пользователей и преступлениями, совершаемыми в конкретном районе в конкретное время.

Для повышения эффективности проведения разыскных мероприятий, несомненно, следует использовать и другие, более известные способы повышения оперативности получения и достоверности полученной информации. Перечень данных, которые могут быть получены посредством анализа профиля пользователя мобильного оператора можно представить следующим образом:

- номера телефонов, на которые осуществлялись вызовы (звонки);
- кто, когда и как пополнял счет «анонимного» телефона;
- возможно (если злоумышленник не осторожен), траекторию его перемещений, историю покупок и звонков.

Успех проведения оперативно-разыскных и оперативно-аналитических мероприятий зависит не только от знания и исполнения требований инструкций, регламентирующих процессуальный порядок в этой сфере, но и от понимания сотрудниками полиции информацион-

ных процессов, протекающих в информационных системах вообще и мобильных операторов в частности [3].

Таким образом, понимание механизма формирования следов работы аппарата мобильной связи на стороне оператора и знание алгоритмов сопоставления обнаруженных следов активности «штатного» телефона злоумышленника с «анонимным» позволит обеспечить реализацию ст. 2 Федерального закона от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности», «добывание информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации» и повысить эффективность оперативно-разыскной деятельности сотрудников полиции.

_____

1. Грифитс Дж. Поведение террористов в Великобритании: пространственный и временный анализ [Электронный ресурс]. URL: http://doi.org/10.1016/j.apgeog.2017.06.007 (дата обращения: 13.03.2024).
2. Девиль П., Линард К. Динамическое картирование популяции с использованием данных мобильного телефона [Электронный ресурс]. URL: http://doi.org/10.1073/pnas.1408439111 (дата обращения: 13.03.2024).
3. Карпика А.Г., Лемайкина С.В. Анализ способов противодействия анонимному использованию сетей мобильной связи // Юристъ-Правоведъ. 2020. № 3 (94). С. 141–144.

АКТУАЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРЕСТУПЛЕНИЯХ

Лемайкина С.В.,
старший преподаватель кафедры
информационного обеспечения ОВД
РЮИ МВД России

Технологии, основанные на искусственном интеллекте (далее – ИИ) и машинном обучении (далее – МО), за последние годы значительно расширили свои возможности, стали доступными и получили широкое распространение, и их рост не подает признаков прекращения. Хотя наиболее заметные технологии ИИ рекламируются как таковые (например, «персональные помощники», такие как Алиса,

Amazon Alexa, Siri и Google Home), методы, основанные на обучении, используются гораздо шире. От поиска маршрутов до перевода языков, от биометрической идентификации до проведения политических кампаний, от управления промышленными процессами до логистики поставок продовольствия – ИИ пронизывает современный взаимосвязанный мир на самых разных уровнях.

По мере расширения возможностей и внедрения технологий ИИ возрастают и риски преступной эксплуатации. Возможности для преступлений с использованием ИИ существуют как в специфической вычислительной сфере (пересекающейся с традиционными понятиями кибербезопасности), так и в более широком мире. Некоторые из этих угроз возникают как продолжение существующей преступной деятельности, в то время как другие могут быть новыми. Чтобы адекватно подготовиться к возможным угрозам со стороны ИИ и защититься от них, необходимо определить, что это могут быть за угрозы и каким образом они могут повлиять на нашу жизнь и общество.

Термин «искусственный интеллект общего назначения» используется для обозначения идеи единой интегрированной системы, способной решать множество различных задач одновременно, даже тех, с которыми она никогда не сталкивалась. Хотя данный термин часто встречается, но в настоящее время он остается далекой перспективой, в то время как более конкретные приложения ИИ, такие как машинное зрение и обработка естественного языка, становятся все более распространенными [1].

ИИ может быть вовлечен в преступления различными способами. Очень вероятно, что ИИ, используя свои достижения, может применяться в различных преступлениях, в качестве оружия злоумышленников для оправдания обычных действий: прогнозирование поведения людей или организаций с целью поиска уязвимостей; создание поддельного контента для запугивания или подрыва репутации; совершение поступков, которые люди не могут или не хотят совершить в реальной жизни по причине опасности и так далее. Хотя способы новые, сами преступления могут быть традиционными – кража, вымогательство, шантаж, террор.

В настоящее время люди проводят большую часть своей жизни в онлайн-пространстве, получая там основную долю информации. Их активность в интернете может как улучшить, так и навредить их репутации, и, вероятно, эта тенденция сохранится в обозримом будущем. Сфера онлайн-коммуникаций, где данные являются ценным ресурсом, а информация – источником влияния, представляет идеальные воз-

можности для преступной деятельности, основанной на использовании ИИ, что может иметь серьезные последствия в реальном мире.

Разнообразие преступлений в онлайн-среде велико. Они могут быть направлены на отдельных пользователей, или учреждения, предприятия или клиентов, собственность, правительство, социальную структуру, общественные дискуссии. Они могут быть мотивированы финансовой выгодой, приобретением власти или изменением статуса по отношению к другим. Они могут укреплять или подрывать репутацию или отношения, изменять политику или сеять раздор; такие действия могут быть самоцелью или ступенькой для достижения какой-то дальнейшей цели. Они могут совершаться для смягчения наказания за другие преступления или в попытке избежать его. Ими может двигать желание отомстить, получить сексуальное удовлетворение или достичь религиозных или политических целей.

В статье приводится обсуждение шести преступлений, которые, в целом вызывают наибольшую озабоченность.

Технология «глубокой подделки». Люди склонны верить собственным глазам и ушам, поэтому аудио- и видеосвидетельствам традиционно придается большое значение (а зачастую и юридическая сила), несмотря на долгую историю фотографического обмана. Однако последние разработки в области глубокого обучения, в частности использование GAN значительно расширили возможности создания поддельного контента. Уже сейчас можно создавать убедительные пародии на цели по фиксированному сценарию, а в будущем ожидается появление интерактивных пародий. Здесь предполагают широкий спектр преступных применений технологии «глубокой подделки». Поэтому единственной эффективной защитой могут стать изменения в поведении граждан. Такие изменения в поведении, например, общее недоверие к визуальным доказательствам, можно рассматривать как косвенный общественный вред, возникающий в результате преступления, в дополнение к прямому вреду, такому как мошенничество или ущерб репутации. Если даже небольшая часть визуальных доказательств окажется убедительной подделкой, дискредитировать подлинные доказательства станет гораздо проще, что подорвет уголовное расследование и доверие к политическим и социальным институтам, которые опираются на надежные коммуникации [2].

Автомобили уже давно используются как в качестве механизма доставки взрывчатых веществ, так и в качестве кинетического оружия террора, причем последнее в последние годы становится все более распространенным. В большинстве стран транспортные средства гораздо более доступны, чем огнестрельное оружие и взрывчатка, а ата-

ки с использованием автотранспорта могут осуществляться с относительно небольшими организационными затратами террористами, такими как те, кто заявляет о своей принадлежности к ИГИЛ. Хотя полностью автономных автомобилей с искусственным интеллектом, управляемых водителем, еще нет, многочисленные автопроизводители и технологические компании стремятся создать их, а некоторые из них уже разрешили испытания на дорогах общего пользования. Автономные автомобили потенциально позволят расширить масштабы автомобильного терроризма, поскольку уменьшится необходимость в привлечении водителей, что позволит преступникам-одиночкам совершать многочисленные нападения, даже координируя большое количество автомобилей одновременно [3].

Фишинг – это «социально-инженерная» атака, целью которой является сбор конфиденциальной информации или установка вредоносного программного обеспечения с помощью цифрового сообщения, якобы исходящего от доверенного лица, например, банка пользователя. Злоумышленник злоупотребляет уже существующим уровнем доверия, чтобы убедить пользователя совершить действия, которых он обычно старается избегать, такие как раскрытие пароля или переход по подозрительной ссылке. Злоумышленник полагается на простоту отправки огромного количества цифровых сообщений, чтобы превратить низкий процент откликов в прибыльную прибыль. ИИ способен повысить успешность фишинговых атак, создавая сообщения, которые выглядят более подлинными, например, путем включения информации, полученной из социальных сетей, или подделки стиля доверенного лица. Вместо того чтобы рассылать всем целям одинаковые сообщения, которые, скорее всего, в большинстве случаев не попадут в цель, сообщения можно подбирать с учетом конкретных уязвимостей, выявленных у каждого человека, что позволяет эффективно автоматизировать процесс фишинга [4].

Нарушение работы систем, управляемых ИИ. По мере расширения использования ИИ в правительстве, бизнесе и дома, а также повышения роли, которую выполняют системы ИИ, возможности для атак будут расширяться. Системы, опирающиеся на методы машинного обучения, часто применяются с целью увеличения эффективности и удобства, а не для обеспечения надежности, и могут изначально не рассматриваться как критическая инфраструктура. Здесь можно предвидеть множество криминальных и террористических сценариев, возникающих при целенаправленном нарушении работы таких систем: от повсеместных перебоев с электричеством до заторов на дорогах и сбоев в логистике продуктов питания. Системы, отвечающие за лю-

бые аспекты общественной безопасности, скорее всего, станут ключевыми целями, равно как и системы, контролирующие финансовые операции. В целом чем сложнее система управления, тем труднее ее полностью защитить [5].

Традиционный шантаж предполагает вымогательство под угрозой обнародования доказательств преступлений или правонарушений, а также неудобной личной информации. Ограничивающим фактором в традиционном шантаже является получение таких доказательств: преступление имеет смысл только в том случае, если жертва заплатит за их уничтожение больше, чем стоит их получение. ИИ может быть использован для этого в гораздо больших масштабах, собирая информацию (которая сама по себе не обязательно должна представлять собой улику) из социальных сетей или больших личных массивов данных, таких как журналы электронной почты, история браузера, содержимое жесткого диска или телефона, затем определяя конкретные уязвимости для большого числа потенциальных целей и подбирая сообщения с угрозами для каждой из них. ИИ также может использоваться для создания фальшивых доказательств, например, когда информация обнаруженная уязвимость подразумевает наличие уязвимости без предоставления доказательств [6].

Фальшивые новости – это пропаганда, которая стремится вызвать доверие, будучи или представляясь исходящей из надежного источника. Помимо предоставления ложной информации, фальшивые новости в достаточном количестве могут отвлечь внимание от правдивой информации. ИИ можно использовать для создания множества версий определенного контента, очевидно, из нескольких источников, чтобы повысить его заметность и достоверность; а также для выбора контента или его подачи на индивидуальной основе, чтобы усилить воздействие [7].

Не исключено, что некоторые из этих опасений окажутся преходящими или парадоксальными в рамках обсуждаемых временных масштабов. Тем не менее, с реалистичной точки зрения, это именно та среда, в которой следует понимать текущие разработки ИИ и от которой можно ожидать развития будущих преступлений.

Хотя разработка стратегий по снижению угроз явно не была целью данной статьи, стоит подумать о том, как данный анализ может быть использован для обоснования мер реагирования на потенциальные преступления, которые были выявлены и обсуждены. Один из возможных подходов заключается в том, чтобы рассмотреть компромисс между вредом и возможностью поражения как руководство к действию, на которое можно эффективно направить усилия и расходы.

1. Искусственный интеллект: погружение. Что стоит за каждым типом обучения? [Электронный ресурс]. URL: https://vc.ru/u/2154092-dmitriy-kartvelishvili/882092-iskusstvennyy-intellekt-pogruzhenie-chto-stoit-za-kazhdym-tipom-obucheniya (дата обращения: 08.04.2024).
2. Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В.С. Овчинского. М.: ИНФРА-М, 2021. 630 с.
3. Терроризм и технологии XXI века [Электронный ресурс]. URL: https://zavtra.ru/blogs/terrorizm_i_tehnologii_hhi_veka (дата обращения: 08.04.2024.
4. Фишинг, утечки и искусственный интеллект: киберпрогноз – 2024 [Электронный ресурс]. URL: https://nbj.ru/fingramotnost/fishing-utechki-i-iskusstvennyy-intellekt-/64854 (дата обращения: 08.04.2024).
5. Опасности искусственного интеллекта – 12 экзистенциальных рисков [Электронный ресурс]. URL: https://vc.ru/u/700022-evgeniy-vilkov/1039614-opasnosti-iskusstvennogo-intellekta-12-ekzistencialnyh-riskov (дата обращения: 08.04.2024).
6. Темная сторона нейросетей: как мошенники используют ИИ и как от этого защититься [Электронный документ]. URL: https://tproger.ru/articles/temnaya-storona-nejrosetej--kak-mowenniki-ispolzuyut-ii-i-kak-ot-etogo-zashhititsya (дата обращения: 08.04.2024).
7. Осторожно! Искусственный интеллект научился создавать фейкньюс [Электронный документ]. URL: https://ceur.ru/news/921/item 359056 (дата обращения: 08.04.2024).

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Шумилов Е.Н.,
слушатель Омской академии
МВД России
Слышалов И.В.,
канд. юрид. наук, доцент,
заместитель начальника кафедры
деятельности ОВД в особых условиях
Омской академии МВД России

Внедрение искусственного интеллекта (далее – ИИ) неизбежно приведет к революционным изменениям в производстве, передаче и

хранении информации, а также в ее характеристиках. Искусственный интеллект применяется для совершения киберпреступлений, к примеру, совершения атак на незащищенные информационные ресурсы. В результате этого ИИ очевидно применять и для обеспечения кибербезопасности и противодействия киберпреступности. Машинное обучение используется для анализирования новых угроз и вредоносных программ на основе уже созданных моделей. На текущий момент методы машинного обучения применяются для мониторинга деятельности человека с целью обнаружения предположительно вредоносных действий, прогнозирования появления вредоносных приложений и вредоносных сайтов. Кибербезопасность максимально соприкасается с возможностями автоматизации с помощью искусственного интеллекта. ИИ традиционно используется для борьбы со спамом и обнаружения вредоносных программ, а также используется в киберпреступности, например, для атак на уязвимые информационные системы. Это связано с тем, что он позволяет ускорить атаки, снизить затраты на подготовку для совершения преступлений и избежать необходимости привлечения большого количества ИТ-специалистов, ресурсы которых весьма ограничены, особенно в отношении нелегальной сферы [1]. Помимо эффективности использования ресурсов, технология ИИ создает психологическую дистанцию между злоумышленником и жертвой. Традиционно многие киберпреступления предполагают взаимодействие и часто присутствие других людей, что ограничивает анонимность преступника и часто служит сдерживающим фактором – ИИ функционирующий автономно, может устранить эти барьеры и уменьшить анонимность и дистанцию. Например, с применением фишинга технологические возможности ИИ становятся весьма изощренными. Сейчас мошенники не только присылают одинаковую для всех пользователей ссылку на вредоносное ПО, но и начинают применять рассылку для каждого пользователя индивидуально, при помощи нейросети подстраиваясь под него, на основе полученной информации, собранной, в том числе из социальных сетей. На текущий момент количество фишинговых атак в России увеличилось, в 2022 году обширное распространение приобрели методы таргетированного (массовой рассылки) фишинга с применением известных брендов, выгодных предложений на их покупку в интернет-магазинах, а также розыгрышей призов под видом известных компаний.

Появление пандемии COVID-19 вызвало увеличение удаленно работающих людей, что привело к увеличению пропускной способности трафика, в результате вырос объём пропускного трафика, всплеск которого спровоцировал рост количества рассредоточенных атак типа

«отказ в обслуживании» (DDoS-атака). Что предоставляет злоумышленникам эффективно использовать DDoS-атаки отправляя очень большое количество запросов, а мощностей сервера не хватает на то, чтобы обработать их все, система выходит из строя и шанс обнаружить их при этом низкий. Также сначала пандемии произошел скачек роста регистраций вредоносных доменов, имеющих ключевые слова «корона» и «COVID». На сегодняшний день уже зарегистрированные домены образуют массив для криминальных структур по всему миру.

Кроме того, рост покупок в сети Интернет в связи со значительным развитием и появлением большого количества маркетплейсов, в условиях пандемии повлияло на всплеск теневой Интернет-торговли. К примеру, в «Darknet» увеличилось количество торговых площадок и платформ для распространения незаконных услуг и товаров.

Современные исследования анализируют характеристики конкретных групп, интересы потребителей, посещение определенных сайтов и общение с другими пользователями и группами. Появление ИИ и технологий обработки больших данных в киберпространстве кардинально меняет ситуацию: используя ИИ для изучения больших массивов данных, злоумышленники могут определять приоритеты своих жертв на основе их поведения в сети, социального статуса, роли и правового положения; используя ИИ, преступники могут систематизировать данные, находящиеся в открытом доступе, и различные конфиденциальные сведения, незаконно циркулирующие в Интернете, и идентифицировать жертв за считанные секунды без вмешательства человека. Доверие формируется благодаря длительному взаимодействию в социальных сетях, которое не требует усилий человека. Чатботы, напротив, поддерживают конфиденциальный диалог, имитируя реальные контакты, стиль общения и даже риторику; продуктивные модели искусственного интеллекта могут определить уровень платежеспособности пользователя, его готовность заплатить выкуп и сумму, которую злоумышленник требует за удаление программы. Машинное обучение, используемое для идентификации жертв и нахождение их, значительно снижает затраты ресурсов злоумышленников и многократно увеличивает их шансы на обогащение [1]. Также ИИ активно используется для имитации аудио- и видеоизображений, так называемый «дипфейк». Значение слова deepfake объединяет в себе два типа: «глубокое обучение» (deep learning) и «подделка» (fake). Для создания deepfake применяются генеративно-состязательная сеть (GAN), состоящая из нескольких элементов: генератор, создающий изображения, и дискриминатор, критикующий их. Нейросеть обрабатывает за считанные секунды больной объем данных медиаконтента и

самообучается. В результате чего «дипфейки» носят опасность не только для компаний различного рода, но и для репутации публичных людей, рискующих быть жертвой ложных обвинений и шантажа. Поэтому распространение данного материала должно пресекаться на государственном уровне: к примеру, в Китае опубликованная фейковая информация с применением «дипфейка» является уголовным преступлением. Новейшие нейронные технологии, основанные на использовании ИИ, могут «генерировать движущиеся декорации для видео контента и или удалять объекты, а также активно манипулировать людьми, чтобы они танцевали в кадре». Такие технологии часто используются в незаконных целях, например, для получения паролей и кодов доступа [2].

В современных условиях представляется очевидным, что ИИ необходимо использовать для борьбы с киберпреступностью и обеспечением кибербезопасности. Он способен определять характер атак и незамедлительно принимать необходимые решения по защите. Алгоритмы машинного обучения непрерывно анализируют сеть и подстраиваются под угрозы, чтобы своевременно их предотвратить. К примеру, DDoS-атаки разделяются на несколько видов: хакерские для перегрузки канала, атаки на оборудование и атаки на приложения. В ходе самых сложных атак ИИ анализирует до 46 параметров поведения пользователей, на основе которых выявляет тип киберпреступления и вырабатывает решение.

Сегодня методы машинного обучения используются для мониторинга информационных систем и человеческой деятельности с целью выявления потенциальных вредоносных отклонений и прогнозирования вредоносных приложений, и вредоносных веб-сайтов, а также помогают определить возможные варианты угроз на ранней стадии до момента атаки, на основе анализа о прошлых действиях злоумышленников. Многочисленные технологии ИИ, основанные на естественных вычислениях (например, вычислительный интеллект, нейронные сети, интеллектуальные агенты, искусственный иммунитет, машинное обучение, поиск данных, распознавание образов и т.д.), играют все более важную роль в обнаружении и предотвращении киберпреступлений. Из этого следует выделить, что ИИ – это самоуправляемые, саморегулируемые, самодиагностирующие и самоконтролирующие технологии, позволяющие разрабатывать автономные вычислительные решения, которые адаптируются к условиям использования [3].

Эти предпосылки должны находиться в основе развития настоящего законодательства и методов противодействия киберпреступности. Требуется учитывать возможность применения ИИ, в частности

при улучшении определенных составов преступлений в области компьютерной информации, мошенничества. В связи с этим, информационная безопасность будет подвергаться новым вызовам и требованиям, которые должны лечь в основу разработки законов и инструментов для борьбы с киберпреступностью. Особенно важно, чтобы законодатели рассмотрели возможность использования ИИ для борьбы со многочисленными преступлениями в сфере компьютерного интеллекта, мошенничества и т.д. С точки зрения возможности обеспечения кибербезопасности необходимо ужесточить требования к использованию технологий ИИ при обработке больших объемов данных. Сегодня технологии искусственного интеллекта эффективно применяются для предотвращения и борьбы с незаконной деятельностью в Интернете. В частности, они активно используются для борьбы с дезинформацией: ряд международных организаций, в том числе использующих ИИ, отслеживают дезинформацию и фальшивые новости и регулярно публикуют обновления, опровергающие подобные утверждения. Распространение фальшивых новостей и дезинформации часто не считается уголовным преступлением. Распространение данной информации может исходить от различных субъектов, включая киберпреступников, стремящихся к финансовой выгоде [4].

Сфера кибербезопасности – ключевая в развитии использовании ИИ и машинного обучения. По данным «Лаборатории Касперского», развитие этого направления входят в тройку основных приоритетов для 51 % крупных российских компаний. Необходимо внедрять инновации в этой сфере, для защиты от новых киберугроз. Поскольку хакеры уже применяют ИИ в своей работе для обхода систем защиты – например, в виде ботов, которые владеют алгоритмами обхода CAPTCHA-проверки, поэтому нужно быть на шаг впереди [5].

Таким образом, современная киберинфраструктура очень уязвима к вторжениям и другим угрозам кибербезопасности. Существующих технологий и активного участия человека недостаточно для мониторинга и защиты таких инфраструктур [6]. ИИ может улучшить обнаружение и реагирование на киберугрозы, сделать процессы авторизации и аутентификации наиболее безлопастными, а также не допустить фишинг и вредоносное программное обеспечение. Очевидно, что в сфере применения технологий ИИ в ближайшем будущем будет создан ряд инструментов, способных не только анализировать, группировать данные и предлагать решения, но и принимать в режиме реального времени необходимые меры борьбы с киберугрозами. Но пока еще на данный момент участие человека необходимо в процессе определения, насколько решение, принятое машиной правильно. Поэтому

нужны более совершенные системы кибербезопасности, гибкие, адаптивные и надежные, способные обнаруживать широкий спектр угроз и принимать интеллектуальные решения в режиме реального времени. Так как развитие новых технологий искусственного интеллекта играет все более важную роль в современном киберпространстве, позволяя эффективно выявлять и предотвращать преступления [7]. Можно сказать, что сегодня инструменты информационной безопасности на основе технологий искусственного интеллекта только формируются. Сложно представить, насколько обширно будет их применение через несколько лет, но совершенно точно оно станет основой для нового уровня кибербезопасности.

---

1. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. С. 135–147.
2. Афанасьева Д.В. Применение искусственного интеллекта в обеспечении безопасности данных // Известия Тульского государственного университета. Технические науки. 2020. № 2. С. 151–154.
3. Власенко А.В., Киселёв П.С., Склярова Е.А. Искусственный интеллект и проблемы кибербезопасности // Технология Deepfake, 2021. С. 81–86.
4. Городнова Н.В. Применение искусственного интеллекта в условиях цифровой экономики: проблемы кибербезопасности. М.: Первое экономическое издательство, 2024. 114 с.
5. Грек А. Обратная сторона ИИ: как нейросети работают в руках кибермошенников [Электронный ресурс] // TechInsider: [сайт]. URL: https://www.techinsider.ru/technologies/1567177-obratnaya-storona-ii-kak-neyroseti-rabotayut-v-rukah-kibermoshennikov (дата обращения: 23.02.2024).
6. Шумилин В.П. Проблемы законодательства о киберпреступности // Аграрное и земельное право. 2022. № 5 (209). С. 137–140.
7. Шумилин В.П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4 (77). С. 173–176.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК ОБЪЕКТЫ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ

Киреев Э.Р.,
слушатель факультета подготовки
специалистов ГИБДД
ОрЮИ МВД России
имени В.В. Лукьянова

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена статьями 158, 159, 159.3, 159.6 УК РФ.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» введена ответственность виновных лиц по статье 158 УК РФ за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ).

Аналогичным образом, с целью усиления уголовной ответственности за противоправные действия с использованием электронных средств платежа, изменены диспозиции и санкции статей 159.3 и 159.6 УК РФ.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые на практике нередко используются в качестве инструментария завладения чужим имуществом. В целях борьбы с компьютерной преступностью в УК РФ предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерный доступ к охраняемой законом компьютерной информации (статья 272 УК РФ), создание, использование и распространение вре-

доносных компьютерных программ (статья 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (статья 274.1 УК РФ).

В качестве примера – статистика Верхневилюйского района Республики Саха. Количество подобных хищений с каждым годом увеличивается. Преступления данной категории ежедневно регистрируются правоохранительными органами области. Только за истекший 2020 год на территории района зарегистрировано 19 таких преступлений, в предыдущем году – 2.

Подавляющее большинство анализируемых хищений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании психологических слабостей человека и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке методов извлечения сведений из общедоступных ресурсов сети Интернет. В первую очередь необходимо отслеживать активность модераторов (владельцев) криминальных ресурсов даркнета в обычном интернете (Clearnet). Зачастую первичный поиск клиентов для криминального бизнеса ведется в открытой сети или в «Telegram» [1].

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны

с установленными на них банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Так называемый фишинг – тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Социальная инженерия используется также для распространения троянских коней: эксплуатируется любопытство, либо алчность объекта атаки. Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или гиперсылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты симкарт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные ПО в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

С учетом отмеченной специфики возникают значительные трудности при их раскрытии.

Программное обеспечение (англ. software) – это совокупность программ, обеспечивающих функционирование компьютеров и решение с их помощью задач предметных областей. Программное обеспечение (ПО) представляет собой неотъемлемую часть компьютерной системы, является логическим продолжением технических средств и определяет сферу применения компьютера. Многие субъекты общественных отношений уже не могут существовать и успешно функционировать без взаимного информационного обмена и использования в своих технологических процессах различных программно-технических устройств – средств создания, накопления, хранения, обработки и передачи информации [2].

ПО современных компьютеров включает множество разнообразных программ, которое можно условно разделить на три группы:

1. Системное программное обеспечение (системные программы);

2. Прикладное программное обеспечение (прикладные программы);

3. Инструментальное обеспечение (инструментальные системы).

Уязвимости программ – ошибки, допущенные программистами на этапе разработки программного обеспечения. Они позволяют злоумышленникам получить незаконный доступ к функциям программы или хранящимся в ней данным. Изъяны могут появиться на любом этапе жизненного цикла, от проектирования до выпуска готового продукта. В ряде случаев программисты нарочно оставляют лазейки для про-

ведения отладки и настройки, которые также могут рассматриваться в качестве бекдоров или недекларированных возможностей.

В некоторых случаях возникновение уязвимостей обусловлено применением средств разработки различного происхождения, которые увеличивают риск появления в программном коде дефектов диверсионного типа. Уязвимости появляются вследствие добавления в состав ПО сторонних компонентов или свободно распространяемого кода (open source). Чужой код часто используется «как есть» без тщательного анализа и тестирования на безопасность. Не стоит исключать и наличие в команде программистов-инсайдеров, которые преднамеренно вносят в создаваемый продукт дополнительные недокументированные функции или элементы.

Классификация уязвимостей программ. Уязвимости возникают в результате ошибок, возникших на этапе проектирования или написания программного кода. В зависимости от стадии появления этот вид угроз делится на уязвимости проектирования, реализации и конфигурации. Ошибки, допущенные при проектировании, сложнее всего обнаружить и устранить. Это – неточности алгоритмов, закладки, несогласованности в интерфейсе между разными модулями или в протоколах взаимодействия с аппаратной частью, внедрение неоптимальных технологий. Их устранение является весьма трудоемким процессом, в том числе потому, что они могут проявиться в неочевидных случаях – например, при превышении предусмотренного объема трафика или при подключении большого количества дополнительного оборудования, что усложняет обеспечение требуемого уровня безопасности и ведет к возникновению путей обхода межсетевого экрана. Уязвимости реализации появляются на этапе написания программы или внедрения в нее алгоритмов безопасности. Это – некорректная организация вычислительного процесса, синтаксические и логические дефекты. При этом имеется риск, что изъян приведет к переполнению буфера или появлению неполадок иного рода. Их обнаружение занимает много времени, а ликвидация подразумевает исправление определенных участков машинного кода. Ошибки конфигурации аппаратной части и ПО встречаются весьма часто. Распространенными их причинами являются недостаточно качественная разработка и отсутствие тестов на корректную работу дополнительных функций. К этой категории также можно относить слишком простые пароли и оставленные без изменений учетные записи по умолчанию. Согласно статистике, особенно часто уязвимости обнаруживают в популярных и распространенных продуктах – настольных и мобильных операционных системах, браузерах.

Примером программного обеспечения как объекта преступных посягательств служит следующая ситуация.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, компьютерных сетей. Это дает основание поставить задачу компьютерного права, одним из основных аспектов которого являются так называемые компьютерные посягательства.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

На сегодняшний день сформулированы базовые принципы информационной безопасности, которая должна обеспечивать:

- целостность данных – защиту от сбоев, ведущих к потере информации, а также от неавторизованного создания или уничтожения данных.

- конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач. Для обеспечения защиты персональных данных крайне необходимо систематическое применение институциональных, технических и физических гарантий, которые сохраняют право на неприкосновенность частной жизни в отношении сбора, хранения, использования, раскрытия и любого другого вида обработки персональных данных. Защита любых конфиденциальных данных имеет особое значение, поскольку является неотъемлемой частью защиты жизни, неприкосновенности и человеческого достоинства гражданина [3].

---

1. Матросова Л.Д., Кислицин И.А. Инструменты для поиска оперативно-значимой информации по открытым источникам // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4 (93). С. 67.

2. Матросова Л.Д., Данилов Р.М., Рыбак А.В. Актуальные аспекты деятельности правоохранительных органов по применению навигацион-

ных систем // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 62.
3. Семенов Е.Ю., Лысенко Е.С., Графуткин Е.И. Регулирование обработки персональных данных в России: юридические и технические аспекты // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 69–77. EDN GLTPUX.

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ В ДОКУМЕНТООБОРОТЕ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Белкина М.А.,
курсант факультета
подготовки следователей
ОрЮИ МВД России
имени В.В. Лукьянова
Шумилин В.П.,
канд. пед. наук, доцент кафедры
информационных технологий
в деятельности ОВД
ОрЮИ МВД России имени
В.В. Лукьянова

Электронная подпись играет важную роль в обеспечении безопасности и доверия в электронном документообороте, включая правоохранительные органы. Она позволяет подтвердить авторство документов, предотвратить подделку, обеспечить невозможность отрицания подписи и обеспечить целостность информации.

С ЭП не получится работать сразу. Чтобы шифровать и подписывать документы, недостаточно только иметь сертификат и закрытый ключ, для работы нужно устанавливать специальные программы. С помощью этих программ, которые работают по определённому стандарту шифрования (в России – ГОСТ 34.10-2018), обеспечивается связь закрытого и открытого ключа с документами [1].

Подписание документа производится в несколько этапов:

Хеш документа шифруется с помощью закрытого ключа.

Полученная подпись добавляется к документу.

К документу прикрепляется сертификат проверки.

Так как сертификаты, выдаваемые удостоверяющим центром, тоже подписываются с помощью электронной подписи, подменить сертификат невозможно. На сайте удостоверяющего центра, как правило, можно скачать открытый ключ проверки, хеш которого должен совпадать с хешем открытого ключа владельца. Таким образом, доказывается его достоверность.

Существуют различные виды электронной подписи, каждый из которых имеет свои особенности и применяется в различных сферах.

Квалифицированная электронная подпись: это наиболее надежный и высокий уровень электронной подписи, который обладает юридической значимостью. Квалифицированная подпись требует использования сертифицированного удостоверяющего центра (СУЦ), который выпускает квалифицированный сертификат, подтверждающий подлинность подписи. Такой сертификат связывает личность владельца подписи с открытым ключом и обеспечивает доверие к подписи сторонними участниками. Квалифицированная электронная подпись широко используется в правоохранительных органах, где требуется высокий уровень безопасности и доказательства в суде.

Простая электронная подпись: простая подпись является основным типом электронной подписи и не требует использования СУЦ. Она создается с использованием пары ключей (закрытый и открытый) владельца подписи. Простая подпись используется для обычных электронных документов и обеспечивает авторство и целостность, но не имеет юридической значимости, как квалифицированная подпись.

Симметричная электронная подпись: в отличие от асимметричной криптографии, симметричная подпись использует один и тот же ключ для создания и проверки подписи. Это позволяет уменьшить вычислительную нагрузку, но требует безопасного распространения ключа между сторонами. Симметричная подпись редко используется в практике, так как асимметричные подписи обеспечивают большую безопасность.

Гибридная электронная подпись: гибридная подпись объединяет преимущества асимметричной и симметричной криптографии. При использовании гибридной подписи генерируется случайный симметричный ключ, который используется для шифрования документа. Затем этот ключ шифруется с помощью открытого ключа получателя и включается в подпись. Такой подход обеспечивает высокий уровень безопасности и эффективность [2].

Система подписания документов с помощью электронной подписи выглядит следующим образом:

Электронная подпись присоединяется не к цифровому документу. ЭП ставится на его сжатую версию – хэш. Таким образом, сокращается время шифрования, так как хэш файла весит меньше, чем сам файл.

Для создания хэша применяются криптографические хэш-функции. При данном способе объёмный текст файла не делится на отдельные модули и сохраняет свой порядок.

После создания хэша, закрытый ключ его шифрует и передаёт получателю вместе с сертификатом электронной подписи.

Открытый ключ ЭП адресата расшифровывает информацию и проверяет подлинность сертификата отправителя.

Закрытый ключ электронной подписи хранят в памяти компьютера или физических носителях: USB-токенах и смарт-картах. Согласно закону № 63-ФЗ «Об электронной подписи», ответственность за хранение закрытого ключа несёт владелец.

В данной статье были рассмотрены основные понятия, виды и принципы электронных документов, электронного документооборота и электронной подписи. Электронный документ представляет собой информацию в электронной форме, а электронный документооборот представляет процесс обмена, управления и хранения электронными документами. Электронная подпись играет важную роль в обеспечении аутентификации, целостности и невозможности отрицания подписи при обмене электронными документами.

В работе отмечено, что использование электронной подписи в документообороте правоохранительных органов имеет ряд преимуществ, таких как повышение эффективности работы, сокращение временных затрат на обработку документов, повышение безопасности и минимизация рисков потери или фальсификации информации. Кроме того, электронная подпись обеспечивает доверие к авторству и подлинности электронных документов [3].

Однако внедрение электронной подписи и электронного документооборота также сталкивается с вызовами и проблемами, такими как необходимость обучения сотрудников, обеспечение совместимости систем, а также разработка правового и нормативного регулирования.

Дальнейшее исследование в области использования электронной подписи в документообороте правоохранительных органов представляет важный научный интерес. Это позволит углубить понимание преимуществ и ограничений данной технологии, а также разработать рекомендации по успешному внедрению в этой сфере. Дополнительные исследования могут включать анализ законодательства, оценку

эффективности и безопасности внедрения электронной подписи, а также рассмотрение практических примеров и рекомендаций для правоохранительных органов.

Таким образом, использование электронной подписи в документообороте правоохранительных органов представляет собой важный шаг в современной цифровой трансформации. Ее применение позволяет повысить эффективность работы, обеспечить безопасность и достоверность электронных документов, а также сократить временные и ресурсные затраты. Однако для успешной реализации необходимо учитывать особенности и требования данной сферы, обеспечивать обучение и поддержку сотрудников, а также разрабатывать соответствующее правовое и нормативное регулирование [4].

_____

1. Об электронной подписи: Федер. закон Рос. Федерации от 6 апреля 2011 г. № 63-ФЗ (ред. от 28 декабря 2022 г.) // Собр. законодательства Рос. Федерации. 2011. № 15, ст. 2036.
2. Шумилин В.П. Проблемы законодательства о киберпреступности // Аграрное и земельное право. 2022. № 5 (209). С. 137–140.
3. Шумилин В.П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4 (77). С. 173–176.
4. Лысенко Е.С., Семенов Е.Ю. Борьба с преступностью в условиях развития информационного общества // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4 (93). С. 57–64. EDN OLDPDP.

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА СЛУЖБЕ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Сидорова М.В.,
канд. пед. наук, доцент кафедры
административного права
и административной деятельности ОВД
ОрЮИ МВД России имени
В.В. Лукьянова

Состояние современного мира стремительно изменилось за последние годы, осуществлен переход от «индустриального общества» к

«обществу информационному». Активно модернизируются все сферы общественной жизни, обновляется человеческий потенциал в условиях реального времени, изменяется образ жизни.

Сегодня использование информационных технологий в российском обществе, кардинальным образом поменяло жизнь его граждан. Изменения коснулись различных сфер их деятельности, в связи с тем, что информация стала важнейшим стратегическим, управленческим ресурсом наряду с ресурсами – человеческим, финансовым, материальным. Производство и потребление информации составляют необходимую основу не только эффективному функционированию и развитию различных сфер общественной жизни, но и способствует созданию благоприятных условий для реализации прав и свобод граждан, защиты их от противоправных посягательств.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы предполагает формирование в России [1] единого информационного пространства, в основе которого заложено формирование знаниевого ресурса, способствующего не только реализации прав граждан на удовлетворении потребности в получении необходимой для них информации, в части касающейся своевременности, качественности, достоверности, но и созданию условий, способствующих расширению информационных горизонтов, с учетом реальной действительности, получению знаний с помощью информационных и коммуникационных технологий. Формирование информационного знаниевого ресурса осуществляется путем развития науки, реализации образовательных и просветительских проектов, создания для граждан общедоступной системы взаимоувязанных знаний и представлений, обеспечения безопасной информационной среды для несовершеннолетних, поддержки традиционных форм распространения знаний, в том числе их применения в интересах личности, общества и государства.

Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» провозгласил использование достижений науки и техники, современных технологий и информационных систем основным принципом деятельности полиции [2].

Информационные технологии проникли во все сферы деятельности органов внутренних дел, начиная от подготовки ведомственных управленческих решений, до их реализации в рамках оперативно-служебной, административной деятельности в зоне обслуживания.

Необходимо отметить, что в последние годы особое внимание уделяется руководством ведомства вопросам применения современных информационных технологий в информационно-аналитическое

обеспечение деятельности органов внутренних дел оперативно-служебной деятельности полиции.

Безусловно, проделана большая работа по внедрению в эту деятельность различных современных автоматизированных информационных систем и программно-технических комплексов, в частности: внедрены типовые программные решения по интеграции данных; реализованы шаги по организации единого информационного пространства в системе МВД России; категорированы основные подходы и определены уровни формирования информационных массивов на региональном уровне и в стране в целом. Внедрение цифровых технологий профильными полицейскими подразделениями и службами позволили предоставлять государственные услуги в электронном формате физическим, юридическим лицам не посещая их, в том числе и МФЦ. Активно используется гражданами, формат электронного обжалования штрафов в области дорожного движения, а также предоставления соответствующих государственных услуг в области дорожного движения, Данная информационная технология, способствует оперативному взаимодействию сотрудников подразделений ГИБДД с гражданами, организациями в решении их профессионально-служебных вопросов.

Достаточно эффективно в ГИБДД МВД России реализуется цифровой системный продукт «Паутина», который позволяет разыскивать угнанные и покинувшие место ДТП автомобили с использованием дорожных камер. Внедрение данной технологии осуществлено во многих субъектах Российской Федерации. Из статистики, представленной МВД России, в 2023 году количество краж и угонов транспортных средств резко снизилось (на 22,9 %, чем за аналогичный период прошлого года), одновременно раскрываемость подобных преступлений достигла максимального значения – 68 % [3]. Полагаем, что не только профессиональные действия полицейских способствовали достижению данного показателя, но и успешность применения информационно-программного комплекса «Паутина».

Регистрационный учет по месту пребывания граждан, осуществляется сотрудниками управления по вопросам миграции, в завершающей стадии находится реализация цифрового взаимодействия с гостиницами в части передачи информации о посетителях. В МВД России, ежегодно по месту пребывания регистрируются более 3 млн человек [4]. Востребованность применения информационных, телекоммуникационных систем в органах внутренних подтверждается и статистикой. Ежегодно, ведомственные информационные ресурсы обра-

батывают боле 2 млн запросов, десятки граждан получают услуги в электронном формате [5].

Среди широкого перечня инновационных технологий внедряемых в деятельность полиции, особое внимание уделяется применению технологий искусственного интеллекта. Данная цифровая площадка призвана оказывать помощь полицейским в превенции правонарушений и противостоянии им. С помощью информационных систем и программных комплексов с применением технологий машинного распознавания образов, способные, в том числе, выделять и распознавать в потоке лиц, находящихся в розыске, либо подозреваемых в совершении преступлений, похищенные или вызывающие подозрение транспортные средства, а также осуществлять поиск связей, выявлять подозрительные действия и т.п.

Сегодня в органах внутренних дел используются информационные технологии н, созданные на основе определенных параметров и значений информационного интеллекта, например, информационные системы «Криминалист», «PredPol», программы «COMPAS», «ShotSpotter» [6].

Совершенствуется работа программных комплексов, направленных на распознавание образов, способные, в том числе, выделять и распознавать в потоке лиц, находящихся в розыске, либо подозреваемых в совершении преступлений, похищенные или вызывающие подозрение транспортные средства. Процедура биометрической инденфикации позволяет производить поиск по массивам информации, содержащим фотоизображения лиц, в том числе: неопознанных трупов; лиц, находящихся в розыске и пропавших без вести; лиц, содержащихся в информационных системах МВД России.

Все это позволяет упорядочить и системно организовать все основные связи между подразделениями органов внутренних дел на всех уровнях управленческой деятельности (федеральном, региональном, районном), а также упростить доступ полицейских к информационным ресурсам, определить порядок фиксации, сбора необходимой информации для осуществления ими своих служебных полномочий.

Сегодня особые требования предъявляются не только к разработке, отбору необходимого арсенала информационных и телекоммуникационных технологий, способствующих эффективности выполнения сотрудниками органов внутренних дел поставленных служебных задач, но и определенные требованиям должны соответствовать и полицейские способные успешно их применять в практической деятельности. Представляется, что наиболее эффективной окажется такая реализация и внедрение АИС, при которой добавление и замена функ-

ций будет проходить поэтапно [7]. Процесс формирования необходимых компетенций в рассматриваемой сфере по своему содержательному наполнению представляется достаточно сложным, емким, в силу наличия большого количества технологических действий, о которых должен знать своевременный полицейский, уметь ими пользоваться, и быть готовыми к их защите, например, электронным документооборотом (с использованием цифровой подписи) [8], служебной электронной почтой, информационными базами органов внутренних дел, информационными системами иных государственных органов, иметь навыки в области информационной безопасности и защиты информации.

---

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]: Указ Президента Рос. Федерации от 09.05.2017 № 203. Доступ из справ.-правовой системы «КонсультантПлюс».
2. О полиции [Электронный ресурс]: Федер. закон Рос. Федерации от 7 февраля 2011 г. № 3-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
3. Количество угонов в России снижается, а количество их раскрытий растет [Электронный ресурс]. URL: https://rg.ru/2023/02/06/kolichestvo-ugonov-v-rossii-snizhaetsia-a.
4. Забавка В.И. Регистрационный учет граждан Российской Федерации в условиях цифровизации [Электронный ресурс] // Вестник экономической безопасности. 2024. № 1. URL: https://cyberleninka.ru/article/n/registratsionnyy-uchet-grazhdan-rossiyskoy-federatsii-v-usloviyah-tsifrovizatsii (дата обращения: 06.06.2024).
5. Искусственный интеллект на службе в полиции [Электронный ресурс]. URL: https://news.rambler.ru/internet/48715031/?utm_content=news_media&utm_medium=read_more&utm_source=copylink.
6. Нейронное дело: как ИИ помогает в борьбе с преступностью [Электронный ресурс]. URL: https://iz.ru/1569903/alena-svetunkova/ neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu?
7. Семенов Е.Ю. Основные проблемы внедрения автоматизированных информационных систем в деятельность органов внутренних дел // Научный портал МВД России. 2022. № 1 (57). С. 36–40. EDN WMLLZJ.
8. Шумилин В.П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник

Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4 (77). С. 173–176.

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Екимцев С.В.,
старший преподаватель кафедры
оперативно-разыскной деятельности
ОВД ОрЮИ МВД России
имени В.В. Лукьянова
Голощапова А.Ю.,
слушатель факультета подготовки
следователей ОрЮИ МВД России
имени В.В. Лукьянова

В обеспечение безопасности на железнодорожном транспорте вовлечено большое количество лиц, что указывает на важность такого направления деятельности, поскольку защищенность объектов транспорта гарантирует безопасность личности, общества, а в отдельных случаях и государства в целом. Ключевыми субъектами, в полномочия которых входит обеспечение общественной безопасности и правопорядка на объектах железнодорожного транспорта, являются сотрудники, осуществляющие оперативно-разыскную деятельность и другие подразделения органов внутренних дел.

Отметим, что для решения проблем, связанных с угрозами совершения преступных деяний террористической и экстремисткой направленности, сотрудники подразделений органов внутренних дел на транспорте при предупреждении и пресечении деяний противоправной направленности используют технологию профайлинга [1].

Профайлинг представляет собой один из способов обеспечения безопасности и, по мнению В.М. Статного, «его необходимо рассматривать в качестве элемента системы психологического сопровождения оперативно-служебной деятельности органов внутренних дел» [2].

Суть применения этой технологии в практике органов внутренних дел на транспорте сводится к выявлению потенциально опасных пассажиров в ходе осуществления повседневной деятельности. В ее основе находится принцип построения профиля человека, находящегося на объекте железнодорожного или любого иного вида транспорта.

Необходимо заметить, что технология профайлинга предполагает вероятную причастность пассажира к совершению противоправного деяния, которая требует дальнейшей проверки при осуществлении досмотровых мероприятий. Тем самым данная технология поможет вовремя сотрудникам, осуществляющим оперативно-разыскную деятельность противодействовать терроризму и экстремизму на железнодорожном транспорте.

Обращаем внимание, что важным мероприятием, проводимым при использовании технологии профайлинга, является опрос пассажира. Опрос является оперативно-разыскным мероприятием. При его производстве сотрудник, осуществляющий оперативно-разыскную деятельность, должен сделать акцент, что осуществляется для обеспечения безопасности пассажира, что позволит наладить психологический контакт и создать положительную установку. Длительность такого опроса примерно 3-4 минуты. Но в течение этого времени сотрудник должен сформировать четкое представление об этом лице, его поведении, а также определить, представляет ли он потенциальную опасность для других лиц, объектов железнодорожного транспорта и общества в целом. Если сотрудник полиции приходит к выводу, что пассажир представляет потенциальную опасность, то он отправляет его на проведение личного досмотра.

Хочется отметить, что сотрудник, осуществляющий оперативнорозыскную деятельность и использующий в своей деятельности профайлинг, должен владеть сведениями о действующих террористических организациях, о разыскиваемых лицах, а также оперативной обстановкой в зоне оперативного обслуживания, что позволит ему четко и грамотно выполнять возложенные на него служебные обязанности.

В случае если опрос, досмотр багажа, личный досмотр сопровождаются негативной психологической реакцией со стороны пассажира, то сотрудник органа внутренних дел на транспорте должен проявлять такт и деликатность, чтобы потенциальный преступник не заподозрил, что ему не доверяют, поскольку это может оказать влияние на результаты профайлинга.

Технология профайлинга при необходимости может осуществляться с применением технических средств для предупреждения террористических актов и иных противоправных проявлений на объектах железнодорожного транспорта [3].

Помимо технологии профайлинга для недопущения совершения административных правонарушений и преступных деяний на объектах железнодорожного транспорта, а также незаконного вмешатель-

ства в деятельность таких объектов могут использоваться специальные технические средства.

Одним из таких средств выступает программно-технический комплекс ПТК «Розыск-Магистраль», благодаря которому проводится постоянная отработка пассажиропотока с целью выявления лиц, которые находятся в розыске, а также причастных к совершению деяний экстремисткой и террористической направленности. Применение этого комплекса позволяет автоматически находить лиц, находящихся в федеральном розыске, и сравнивать имеющиеся о них данные в базе с базой данных приобретаемых билетов. Когда разыскиваемое лицо приобретает билет, информация об этом сразу попадает на сервер ПТК «Розыск-Магистраль» [4].

Таким образом, можем сделать вывод о том, что активное использование в деятельности сотрудников, осуществляющим оперативно-разыскную деятельность на транспорте технологии профайлинга способствует снижению деяний противоправной направленности. Также это повлияет на повышение уровня безопасности на объектах железнодорожного транспорта. Ведь это обуславливается тем, что состояние транспортной защищенности имеет прямую зависимость от применения разных современных методов, подходов и технологий, а также от комплексных действий проводимых сотрудниками органов внутренних дел на транспорте. Для эффективности осуществления профилактической деятельности на объектах железнодорожного транспорта технология профайлинга должна применяться совместно с иными методами и средствами в деятельности сотрудников, осуществляющим оперативно-разыскную деятельность. Как раз одним из таких средств является программно-технический комплекс ПТК «Розыск-Магистраль». Благодаря данному комплексу проводится постоянная обработка пассажиров с целью выявления лиц, которые находятся в розыске, а также причастных к совершению деяний экстремисткой и террористической направленности.

---

1. Занина Т.М., Агаркова Н.А. Организация деятельности патрульно-постовой службы полиции по обеспечению общественного порядка и безопасности на объектах железнодорожного транспорта // Вестник Воронежского института ФСИН России. 2019. № 4. С. 209–213.
2. Статный В.М. Технология профайлинга в системе психологического сопровождения оперативно-служебной деятельности органов внутренних дел // Психология XXI века: сборник материалов VIII между-

народной научно-практической конференции молодых ученых. СПб., 2012. С. 30–37.
3. Занина Т.М., Агаркова Н.А. Основные направления деятельности органов внутренних дел на транспорте в рамках реализации Государственной программы «Обеспечение общественного порядка и противодействия преступности» на объектах железнодорожной инфраструктуры // Вестник Пермского института ФСИН России. 2021. № 3 (42). С. 106–113.
4. Горовой В.В. Некоторые направления по обеспечению безопасности транспортного комплекса Российской Федерации // Транспортное право и безопасность. 2020. № 4 (36). С. 210–217.

НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ, СОВЕРШЕННЫХ С ПОМОЩЬЮ СЕТИ «ИНТЕРНЕТ» БЕСКОНТАКТНЫМ СПОСОБОМ

Смирнов И.М.,
канд. ист. наук,
старший преподаватель кафедры
оперативно-разыскной деятельности
ОВД ОрЮИ МВД России
имени В.В. Лукьянова
Крысина Т.Е.,
курсант факультета
факультета подготовки следователей
ОрЮИ МВД России
имени В.В. Лукьянова

Уголовные дела по преступлениям, связанным с незаконным оборотом наркотических средств, психотропных веществ и их аналогов (далее – «наркотики»), в практической деятельности правоохранительных органов, как правило, возбуждаются при наличии достоверной информации, содержащейся в результатах оперативно-разыскной деятельности (далее – ОРД). Указанная ситуация осложняется тем, что практически всегда отсутствует один из составляющих элементов состава преступления – потерпевший, который мог бы сообщать достоверную информацию оперативным сотрудникам о поражении своих прав и причиненном ему ущербе. Полагаем, что в результате активной цифровизации российского общества и внедрении современ-

ных IT-технологий практически во все сферы общественной жизни, деятельность наркопреступников достигла высокого уровня конспирации, при котором производство традиционных оперативно-разыскных мероприятий (далее – ОРМ) становится неэффективным. В представленной ситуации речь идет о преступлениях в сфере незаконного оборота наркотических средств с использованием информационно-коммуникационной сети «Интернет», осуществляемых бесконтактным способом. В контексте рассматриваемой проблемы необходимо уделить внимание тому, что в сети «Интернет» с помощью таких мессенджеров как «Telegram», «ВКонтакте» и т.п. злоумышленники осуществляют деятельность по вербовке молодых людей, среди которых есть и несовершеннолетние лица. Вербующие обещают данной категории граждан значительный постоянный доход за выполнение определенных действий, о которых сразу не сообщают. Стоит отметить, что выбор преступников в осуществлении агитации молодежи на осуществление незаконного сбыта наркотических средств объясняется тем, что данные лица имеют достаточно глубокие знания в области использования компьютерных технологий, но не всегда грамотны в сфере уголовного законодательства Российской Федерации, следовательно, должным образом не осознают противозаконность своих действий [1].

Многие авторы в своих исследовательских работах и в практической деятельности обращают внимание на то, что преступления в сфере незаконного оборота наркотических средств осуществляются группой лиц, которые объединены в сообщество с единым руководящим центром. Данное наркосообщество имеет специфические признаки, например, такие как: наличие определенной структуры, разделение функций между участниками, соблюдение дисциплины.

Традиционно в структуре подобных ОПГ выделяют несколько уровней (ступеней), с характерной жесткой соподчиненностью.

Первая ступень – административно-организаторская линия. Деятельность данных лиц заключается в поставке запрещенных веществ в целях последующего сбыта наркотиков на определенной территории.

Вторая ступень – это обеспечивающая линия. Прежде всего к ней относятся «диспетчеры» («дроповоды»), чья деятельность непосредственно заключается в получении информации и обработке деталей в процессе получения «заказа» от субъекта, который испытывает зависимость от наркотиков. Функции диспетчера связаны с координацией действий «закладчика». Он контролирует получение от покупателя финансовой оплаты за «продукт». К данной ступени относятся

«массажисты» – лица, осуществляющие выбор помещения, для хранения и фасовки наркотических средств, и оплачивающие его аренду. Также к обеспечивающим участникам относится «кассир» («финансовый директор»), обеспечивающий контроль за финансовым оборотом и распределяющий деньги между всеми членами наркосообщества. Подчеркнем, что использование современных IT-технологий способствует обеспечению анонимности передачи оплаты за наркотики, чаще всего с помощью криптовалюты и иных видов токенов.

Третья ступень – линия исполнения. К ним относятся «закладчики» или так называемые «дропы». Получая необходимые сведения от «диспетчера» и под его непосредственным контролем, они реализуют свои функции по закладке наркотических средств в установленном ранее месте, адрес которого сообщается потребителю через информационно-коммуникационную сеть «Интернет». Следует отметить, что «курьер» или «бегунок» обеспечивает доставку уже расфасованных наркотических средств, а также несет ответственность за их своевременное пополнение у «закладчика» [2].

Необходимо отметить, что в данном преступном сообществе профессиональная иерархия предусматривает перевод сотрудника на вышестоящую должность при наличии хороших рекомендаций в процессе осуществления своих непосредственного функций.

Таким образом, каждое лицо, являющееся членом преступного сообщества, осуществляющего свою незаконную деятельность бесконтактным способом, имеет регламентированные инструкции: по правильности расфасовки наркотических средств; в какое место и время суток необходимо осуществлять закладку, а также по организации мер конспирации; как грамотно использовать современные технологии для сокрытия информации через разнообразные иностранные и отечественные прокси-серверы; расшифровка и применение лексических выражений для обозначения мест хранения наркотиков; как правильно вести себя в случае задержания с поличным сотрудниками оперативных подразделений.

Стоит подробнее остановиться на механизме осуществления сбыта наркотических средств бесконтактным способом в сети «Интернет».

Лицо, зависимое от наркотических средств, при помощи собственного мобильного устройства посредством отправления сообщения на известный абонентский номер заказывает у «диспетчера» необходимый вид товара, после чего ему сообщается сумма, которую необходимо оплатить с использованием современной техники и электронной платежной системы. Наркоприобретатель для оплаты нарко-

тических средств пользуется широко известными в современном мире платежными системами, пользующимися популярностью благодаря своей анонимности (ЮMoney, WebMoney, Qiwi, Payeer, AdvCash, Skrill, Perfect Money, PayPal, BestChange). Данные системы позволяют совершать переводы без необходимости регистрации или предоставления документов [3].

Таким образом, вся цепочка преступного события начинается с получения денег от заказчика. После этого диспетчер дает указания закладчику о том, где и когда необходимо разместить наркотики, и передает данные инструкции покупателю. Интересный момент заключается в том, что оба участника, и закладчик, и диспетчер, не имеют представления друг о друге, и весь обмен информацией происходит только через различные мессенджеры в информационно-коммуникационной сети «Интернет», такие как «Viber», «WhatsApp», «Telegram», а также через сервисы одноразовых сообщений, к примеру «Privnote».

После того, как диспетчер получил оплату от покупателя за приобретенный товар, он сообщает через мессенджер координаты местонахождения «закладки». Реализуя этот метод управления наркобизнесом, участники определенно распределяют свои обязанности, что обеспечивает безукоризненную организацию. Следует отметить, что для конспирации члены наркосообщества используют специальную лексику, не прямо связанную с наркотиками или преступной деятельностью. Для повышения эффективности сокрытия участников наркобизнеса в сотовых устройствах используются сим-карты, зарегистрированные на подставных людей, поскольку за денежные вознаграждения лица с низкой социальной ответственность готовы выполнить любые, даже противозаконные, действия. Необходимо отметить, что на данную категорию граждан по корыстным или иным мотивам могут быть оформлены банковские счета, реквизиты которых вскоре передаются организаторам наркобизнеса.

Для эффективности конспирации своей преступной деятельности участники накросообщества систематически меняют операторов мобильной связи, телефоны, банковские учётные записи, а также привлекают других людей с низкой степенью социальной ответственности, готовых оказать помощь за вознаграждение. Важно подчеркнуть, что общение через мобильные телефоны между участниками преступного сообщества ограничено передачей самой критической информации. Следовательно, в процессе телефонного общения преступники используют минимум слов, которые подвергают шифрованию,

например, изменение названий банков, улиц, домов, мест закладок и т.п. (противоположные к названиям улиц, изменение номеров домов).

В контексте рассмотрения процесса производства оплаты с помощью современных электронных платежных терминалов необходимо уделить внимание следующим аспектам. Во-первых, государство не может отслеживать и контролировать денежные операции, во-вторых, также основные ее преимущества состоят в анонимности, быстроте перевода и возможностью использовать «цифровые валюты». Следовательно, указанные выше обстоятельства оказывают негативное влияние на процесс документирования преступной деятельности наркосообществ и фактически обесценивают прежние рекомендации и методы работы сотрудников оперативных подразделений [4]. Таким образом, из всего вышесказанного следует сделать логический вывод о том, что эффективность деятельности оперативных сотрудников по документированию зависит от понимания схемы совершения преступлений в сфере незаконного оборота наркотических средств бесконтактным способом с помощью информационно-коммуникационной сети «Интернет».

Для изобличения участников преступного сообщества, осуществляющих деятельность в сфере незаконного оборота наркотических средств, сотрудники оперативных подразделений придерживаются алгоритма, состоящего из двух основных направлений.

Во-первых, следует обнаружить «диспетчерский центр», где принимаются заказы на наркотики от потребителей и осуществляется координация действий курьеров.

Во-вторых, необходимо выявить личности членов преступного сообщества, которые выполняют функции закладчиков.

Таким образом, в процессе проведения негласных ОРМ сотрудники оперативных подразделений устанавливают личности курьеров и закладчиков в максимально короткий период, что в дальнейшем способствует выявлению иных участников наркобизнеса по их ролям и функциональными обязанностями.

Основные проблемные вопросы в практической деятельности сотрудников связаны с процессом документирования результатов проверочной закупки наркотических средств, проводимой в сети «Интернет». Особенность проведения данного негласного мероприятия в том, что оплата за приобретаемые наркотические средства реализуется с помощью системы безналичных расчетов, следовательно, отсутствует непосредственный контакт между покупателем и сбытчиком.

На первом этапе проверки поступившей информации сотрудники оперативных подразделений обращают внимание и скрупулезно

фиксируют два важных факта: наличие наркотиков и их незаконного сбыта, при этом круг лиц преступного сообщества останется неизвестным. Поэтому сотрудники принимают активные меры, в том числе применяют новейшие IT-технологии, чтобы выявить причастных к незаконной деятельности. Для этого они используют комплексные методы оперативно-разыскной работы, направленные на выявление местонахождения нарушителей закона.

Оперативные органы осуществляют действия по мониторингу информационно-коммуникационной сети «Интернет», через различные интернет-платформы (например, Yandex, Rambler, Google и т.п.) выявляют сайты и контактные данные лиц, которые предлагают осуществить покупку запрещенных веществ. После чего происходит основной сбор сведений о личности участников наркобизнесса с помощью применения технических средств, в том числе для проверки сайтов и форумов, созданных для сбыта и приобретения наркотиков.

С помощью полученных сведений оперативным сотрудникам становятся известны номера мобильных телефонов, что способствует проведению негласных ОРМ, направленных на установление реквизитов банковских карт, на которые перечисляются денежные средства за наркотические средства. Таким образом, перечисленные действия возможны лишь при осуществлении взаимодействия оперативных сотрудников с подразделениями специальных технических мероприятий.

Дальнейший процесс документирования преступной деятельности заключается в проведении подробного анализа собранной информации о количестве лиц, участвующих в сбыте наркотиков, методах их действий и местонахождении. После установления фигурантов и документирования их преступной деятельности оперативные сотрудники осуществляют их задержание.

---

1. Кушпель Е.В., Кулешов П.Е. Некоторые аспекты криминалистической характеристики незаконного сбыта наркотических средств, совершенного бесконтактным способом // Международный журнал прикладных и фундаментальных исследований. 2016. № 2. С. 119–122.
2. Богданов А.В. Информационно-телекоммуникационная сеть Интернет как один из наиболее востребованных ресурсов в противодействии незаконному обороту наркотиков // Вестник Московского университета МВД России. 2018. № 2. С. 34.

3. Введенская О.Ю. Способ незаконного сбыта наркотических средств с использованием сети Интернет и телекоммуникационных технологий // Вестник КРУ МВД России. 2020. № 2. С. 22.
4. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 5. С. 243.

КРАТКИЙ ОБЗОР ВСЕМИРНОГО ДОКЛАДА О НАРКОТИКАХ ЗА 2023 ГОД УПРАВЛЕНИЯ ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ ООН

Малик В.И.,
канд. юрид. наук,
преподаватель кафедры
оперативно-разыскной деятельности
ОВД ОрЮИ МВД России
имени В.В. Лукьянова

Согласно Всемирному докладу о наркотиках за 2023 год [1], опубликованный Управлением ООН по наркотикам и преступности (УНП ООН), сохраняются рекордные объемы незаконных поставок наркотиков и все более гибкие сети их оборота усугубляют пересекающиеся глобальные кризисы и создают проблемы для служб здравоохранения и правоохранительных органов.

По новой информации, оценка глобального количества людей, использующих инъекционные наркотики, в 2021 году составит 13,2 миллиона человек, что на 18 % превышает предполагаемое значение. Общее количество людей, употребляющих наркотики по всему миру в 2021 году, превысило 296 миллионов человек, на 23 % больше, чем за предыдущее десятилетие. За это же время количество людей, страдающих зависимостью от наркотиков, сильно выросло и достигло 39,5 миллиона человек, что на 45 % больше, чем за последние 10 лет.

В докладе есть специальная глава, посвященная незаконному обороту наркотиков и преступлениям, наносящим ущерб окружающей среде в бассейне Амазонки, а также разделы, посвященные клиническим испытаниям психоделиков и использованию каннабиса в медицинских целях; употребление наркотиков в гуманитарных учреждениях; инновации в сфере лечения наркозависимости и других услуг; наркотики в условиях конфликтов.

Во Всемирном докладе о наркотиках за 2023 год также подчеркивается, как социальное и экономическое неравенство вызывает проблемы, связанные с наркотиками, и само обусловлено ими; разрушение окружающей среды и нарушения прав человека, вызванные незаконной торговлей наркотиками; и растущее доминирование синтетических наркотиков.

По информации из отчета, запрос на помощь при расстройствах, связанных с употреблением наркотиков, остается неудовлетворенным в значительной мере. В прошлом году только каждый пятый больной с этими расстройствами получил лечение, и при этом различия в доступе к помощи в разных регионах только ухудшались. Среди всех возрастных групп молодежь оказывается наиболее уязвимой к наркотикам, и в определенных местах проблемы с расстройствами, связанными с употреблением психоактивных веществ, становятся серьезными. В регионе Африки 70 % пациентов, получающих помощь, не достигли возраста 35 лет [2].

В докладе утверждается, что общественное здравоохранение, профилактика и доступ к лечебным услугам должны быть приоритетными во всем мире, иначе из-за проблем, связанным с наркотиками на «дне» окажется все больше людей. В докладе также подчеркивается необходимость принятия мер правоохранительными органами, чтобы идти в ногу с гибкими моделями криминального бизнеса и распространением дешевых синтетических наркотиков, которые легко вывести на рынок.

Некоторые бедные и уязвимые группы населения, например, проживающие в районе трех границ между Бразилией, Колумбией и Перу, оказались в ловушке в сельских районах с высокой распространенностью преступлений, связанных с наркотиками. Их отдаленное расположение делает для них чрезвычайно трудным получение лечебных услуг, ресурсов или защитой со стороны государства.

Приоритет общественного здравоохранения при регулировании медицинского использования контролируемых наркотиков.

Недавние исследования о применении регулируемых наркотиков, включая психоделики, для лечения душевных расстройств, вызванных употреблением наркотических веществ, показали перспективные результаты. Однако в отчете отмечается, что быстрый темп развития может нарушить усилия в разработке политики, призванной защитить интересы общественного здоровья от коммерческих интересов. Без тщательно продуманных и хорошо исследованных механизмов доступ к психоделикам для нуждающихся в лечении может быть недостаточным, что повлечет за собой обращение пациентов на неле-

гальные рынки или злоупотребление психоделиками в немедицинских целях [3].

Дешевое, простое и быстрое производство синтетических наркотиков радикально изменило многие незаконные рынки наркотиков. Преступники, производящие метамфетамин – доминирующий в мире нелегально производимый синтетический наркотик – пытаются уклониться от реагирования правоохранительных органов и используя новые пути синтеза, обойти операционные базы неконтролируемых прекурсоров.

Фентанил радикально изменил рынок опиоидов в Северной Америке, что привело к ужасным последствиям. В 2021 году большинство из примерно 90 000 случаев смерти от передозировки опиоидами в Северной Америке были связаны с нелегально изготовленным фентанилом.

Каннабис на сегодняшний день остается наиболее часто употребляемым наркотиком в мире. В 2021 году каннабис употребляли около 219 миллионов человек, или 4 % населения мира. Число людей, употребляющих каннабис, увеличилось на 21 % за последние десять лет. В Америке на севере страны уровень употребления каннабиса остается самым высоким, поскольку в 2021 году его употребляли 17,4 % населения в возрасте от 15 до 64 лет. Каннабис остается основным наркотиком, вызывающим проблемы у большинства людей, проходящих лечение в Африке.

Основной проблемой на глобальном уровне приходится на каннабис, что отчасти объясняется широкой распространенностью его потребления: по оценкам, 41 % случаев расстройств, связанных с употреблением наркотиков, во всем мире связаны с употреблением каннабиса (2019 год). В 2021 году около 46 % стран заявили, что каннабис является первым веществом, вызывающим такие расстройства, а 34 % – что он является основной причиной обращения за наркологической помощью.

По оценкам, в 2021 году 60 миллионов человек употребляли опиоиды, что составляет 1,2 % населения мира. Половина из них проживала в южной или Юго-Западной Азии. Из общего числа людей, употреблявших опиоиды в 2021 году, по оценкам, 31,5 миллиона человек употребляли опиаты, в основном героин. Во всем мире употребление опиоидов в 2021 году оставалось стабильным, после небольшого увеличения в период с 2017-го по 2019 год, около 38 % людей, проходивших лечение от употребления наркотиков в 2021 году, назвали опиоиды основным употребляемым наркотиком. Опиоиды остаются самыми смертоносными наркотиками; на их долю прихо-

дится две трети смертей, непосредственно связанных с наркотиками (в основном от передозировок) [4].

В 2022 году площади, занятые под выращивание опийного мака, во всем мире увеличились на 28 %. Производство опия снизилось на 3 %, тем не менее сохраняется долгосрочная тенденция к росту. В 2022 году на Афганистан по-прежнему приходилась большая часть (80 %) мирового незаконного производства опиума, балканский маршрут остается основным маршрутом незаконного оборота опиатов, а в 2021 году объем изъятий резко возрос после того, как в 2020 году разразилась пандемия COVID-19. Объемы изъятий фармацевтических опиоидов, которые в долгосрочной перспективе имеют тенденцию к росту, резко возросли в 2021 году.

Две вспышки злоупотребления опиоидами – фентанилом в Северной Америке и трамадолом в Северной и Западной Африке, на Ближнем и Среднем Востоке и в Юго-Западной Азии – продолжают представлять значительный риск для здоровья. В Африке в последние годы наблюдались признаки увеличения немедицинского использования трамадола и причиненного им вреда. В Северной Америке число смертей от передозировки фентанила достигло беспрецедентного уровня во время пандемии COVID-19. Доступ к фармацевтическим опиоидам для обезболивания и паллиативной помощи по-прежнему значительно различается в странах с низким и средним уровнем дохода и странах с высоким уровнем дохода.

---

1. Всемирный доклад о наркотиках за 2023 год [Электронный ресурс] // Управление по наркотикам и преступности ООН. URL: https://www.unodc.org/unodc/index.html (дата обращения: 04.04.2024).
2. Доклад Секретариата по поводу незаконного оборота наркотиков (E/CN.7/2017/5) [Электронный ресурс] // Управление по наркотикам и преступности Организации Объединенных Наций. URL: https://undocs.org/Home/Mobile?FinalSymbol=E%2FCN.7%2F2017%2F5&Language=E&DeviceType=Desktop&LangRequested=False (дата обращения: 04.04.2024).
3. Куликов А.В., Шелег О.А. Особенности возбуждения уголовных дел о преступлениях, связанных с незаконным оборотом наркотических средств // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 98–105.
4. Единая конвенция о наркотических средствах от 30.03.1961 с поправками, внесенными в нее в соответствии с Протоколом 1972 года // Бюллетень международных договоров. 2000. № 8. С. 15–20.

ДЕЛОПРОИЗВОДСТВО В ОРГАНАХ ВНУТРЕННИХ ДЕЛ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Понтелеева М.А.,
курсант факультета подготовки
следователей ОрЮИ МВД России
имени В.В. Лукьянова
Сущенко С.А.,
канд. юрид. наук,
преподаватель кафедры
оперативно-разыскной деятельности
ОВД ОрЮИ МВД России
имени В.В. Лукьянова

В настоящее время трудно представить деятельность не только органов, но и различных организаций, предприятий без оформления их деятельности в виде документов. В системе ОВД документ – это совокупность информации, а также соответствующих реквизитов, созданных государственными органами, организациями, органами местного самоуправления, имеющая соответствующее оформление и включенная в документооборот ОВД. Делопроизводство – это процесс, который состоит из четырех элементов: документирование, документооборот, оперативное хранение документов и использование их в повседневной деятельности.

Делопроизводство обеспечивает весь процесс системы управления, способствует выполнению оперативных задач сотрудниками ОВД, обеспечивая сохранность всей документации, ее быстроту нахождения, экономию времени на составление сотрудниками документов [1]. Основным документом, регламентирующим деятельность в данной сфере, является инструкция по делопроизводству в ОВД РФ, утвержденной приказом МВД России от 20.06.2012 № 615.

В настоящее время можно выделить следующие проблемы, возникающие в сфере делопроизводства в органах внутренних дел:

1. Устаревшая форма осуществления – сотрудники не используют в своей деятельности электронный документооборот, что облегчало бы решение служебных и оперативных задач. В органах внутренних дел, к сожалению, широко используется бумажная документация, что очень трудоемко и занимает огромное количество времени при работе с ней;

2. Недостаточный уровень квалификации работников – отсутствие профессиональных умений и навыков, которые необходимы

для успешного документооборота в ОВД. Данная проблема может привести к неправильному оформлению документов, а в дальнейшем к снижению уровня эффективности деятельности органов внутренних дел;

3. Отсутствие четких стандартов и требований при оформлении документов, из чего вытекают трудности при решении задач правоохранительными органами [2];

4. Необходимость одновременного перевода всех структурных подразделений на электронный документооборот, ведь данный процесс является долгим и кропотливым.

Выделяются следующие пути решения данных проблем:

1. Внедрение электронного документооборота в деятельность правоохранительных органов, что будет способствовать повышению эффективности их деятельности, а также облегчению работы с документами, быстрому их поиску и оформлению, а также обороту [3];

2. Повышение квалификации работников органов внутренних дел путем прохождения ими обучения, что повысит уровень их компетенции;

3. Нормативное закрепление стандартов и требований, предъявляемых к документам;

4. Материально-техническое обеспечение всех структурных подразделений необходимыми ресурсами, средствами и технологиями для осуществления ими электронного документооборота.

В органах внутренних дел функционирует информационно-телекоммуникационная система (ИМТС). Это система, которая обеспечивает информационно-телекоммуникационное взаимодействие между сотрудниками МВД России, а также доступ их к базам данных. ИМТС ставит следующие задачи в сфере документооборота в органах внутренних дел:

1. Повышение квалификации сотрудников путем получения ими образования без нанесения ущерба времени для выполнения закрепленных за ними обязанностей.

2. Обеспечение организации взаимодействия ОВД РФ и международной полиции Интерпол.

3. Ведение базы данных различных уровней общего и специального пользования.

4. Обеспечение конфиденциальности документов для обеспечения с ними работы соответствующих подразделений.

5. Использование различных автоматизированных систем при решении служебных задач сотрудниками органов внутренних дел.

Также в настоящее время на базе интегрированной телекоммуникационной сети ОВД эффективно функционирует Единая система информационно-технического обеспечения деятельности ОВД (ИСОД). Это совокупность сервисов, которые необходимы для осуществления сотрудниками своей деятельности. В нее входят как повседневные сервисы (доступные всем) и сервисы обеспечения оперативно-разыскной деятельности (прикладные), которые доступны сотрудникам в зависимости от их должностных обязанностей. Существуют такие системы как СЭП – сервис электронный почты, предназначенный для обмена информации между сотрудниками, и СЭД – система электронного документооборота – система автоматизации работы с электронными документами на протяжении всего их жизненного цикла [4].

Таким образом, в настоящее время активно развивается область делопроизводства в органах внутренних дел. Осуществляется активное внедрение различных программ и сервисов для перевода всех структурных подразделений на электронный документооборот. Роль делопроизводства велика. Оно обеспечивает эффективность работы с документами, их правильное оформление, простоту работы, а также взаимодействие подразделений друг с другом.

---

1. Астахова А.О. Характеристика документационного обеспечения в системе органов внутренних дел // Научный компонент. 2019. № 2 (2). С. 95–107.

2. Звонарёва А.Ю., Васильева И.Н. Документационное обеспечение и режим секретности в управленческой деятельности в органах внутренних дел Российской Федерации: курс лекций. М.: Академия управления МВД России, 2021. 96 с.

3. Сущенко С.А. «Электронные доказательства» в уголовном процессе США // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 1 (94). С. 228–235.

4. Шумилин В.П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4 (77). С. 173–176.

ИСПОЛЬЗОВАНИЕ ОРГАНАМИ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ МВД РОССИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ, НАПРАВЛЕННОЙ НА ВОЗМЕЩЕНИЕ УЩЕРБА, ПРИЧИНЕННОГО ПРЕСТУПЛЕНИЕМ

Нехаев И.Н.,
адъюнкт ОрЮИ МВД России
имени В.В. Лукьянова

Отечественной и зарубежной истории известно несчетное множество этапов, которые оказали неизгладимое влияние на становление и развитие последующих поколений. Не является и исключением XXI век, ознаменованный развитием информационных и телекоммуникационных технологий, как одних из наиболее актуальных и динамично развивающихся отраслей. Несмотря на высокий темп развития таких технологий в нашей стране, очевидно, что Российская Федерация, пытаясь преодолеть, пройденный ранее развитыми странами технологический скачок, в настоящее время, к сожалению, все еще находится в догоняющей позиции, относительно стран Европы и некоторых стран Азии.

Согласно сведениям Международного союза электросвязи, относительно количества активных интернет пользователей, на развивающиеся страны приходится около 3,5 миллиардов пользователей, а совокупное количество всех пользователей всемирной компьютерной сети (www – World Wide Web) составляет около 5,35 миллиардов пользователей. При этом, на развитые страны приходится в среднем 86 % распространения такого статистического показателя, как уровень проникновения интернета среди населения. Российское государство, в свою очередь, входит в число лидеров по уровню проникновения интернета.

Неоспоримым является и все большее распространение интернет пользователями в информационных системах персональной информации. Например, с помощью электронной почты направляются цифровизированные копии личных документов, в том числе удостоверяющих личность; распространяются и реквизиты банковских счетов и карт, для возможности совершения онлайн-платежей в магазинах, сервисах доставки, маркетплейсах, сервисах такси и прочее; посредством мессенджеров передается иная, конфиденциальная информация.

В этой связи, констатируя действительно глубокое проникновение информационных технологий в повседневные отношения граждан и возводя этот аспект в качестве одного из приоритетных направлений внутренней политики, утверждена Указом Президента Российской Федерации от 09.05.2017 № 203 утверждена Стратегия развития информационного общества в РФ, на 2017–2030 годы. Стратегия закрепляет формирование информационного пространства, развитие информационных, а также коммуникационных технологий и соответствующей им инфраструктуры. Кроме этого, предусмотрено и совершенствование беспроводных технологий связи, виртуальной и дополненной реальности, промышленного интернета и искусственного интеллекта программой «Цифровая экономика Российской Федерации», утвержденной Правительством РФ 28.07.2017.

Использование в правоохранительной деятельности информационных технологий предусмотрено рядом нормативных правовых актов. Так, согласно ст. 11 Федерального закона «О полиции» полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

В соответствии с п. 2 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Имеющиеся очевидные изменения течений информационных процессов, оказывают влияние и на деятельность органов внутренних дел в целом, а в частности органов предварительного следствия МВД России, например, в вопросах возмещения вреда, причиненного преступлением. Обуславливается этот тезис в первую очередь процессами обмена информацией между субъектами этой информацией располагающей и нуждающейся в ней. В силу этого, требуют совершенствования и модернизации уже существующие модели обработки, сбора, получения и передачи информации.

Проблема возмещения вреда, причиненного преступлением, остро стоит перед современным обществом. В 2023 году ущерб от преступлений (по оконченным и прекращенным уголовным делам) составил 284,3 млрд рублей. Указанная сумма сопоставима, к примеру, с бюджетом ФСИН России на 2022 год, который составил 247,9 млрд рублей.

Научный интерес представляют данные официальной статистики, представленные Судебным департаментом Верховного Суда Рос-

сийской Федерации. Так, общая сумма ущерба от преступлений, определенная по судебным актам, в 2020 году составила 69 670 147 276 руб., тогда как сумма возмещения – 6 526 948 049 руб. (около 9,4 % от общей суммы причиненного ущерба). В 2022 году – 32 323 013 629 руб. и 10 052 943 929 руб. соответственно (около 31 % от общей суммы причиненного ущерба).

На значимость деятельности правоохранительных органов по обеспечению возмещения вреда, причиненного преступлением, ежегодно указывает в своих докладах Уполномоченный по правам человека в Российской Федерации Т.Н. Москалькова. Омбудсмен обращает внимание на наличие проблем, связанных с защитой прав и законных интересов потерпевших в досудебном производстве. Речь идет, в том числе, и о трудностях, возникающих при разрешении вопроса о возмещении вреда, причиненного преступлением. По мнению Т.Н. Москальковой, которые ей неоднократно высказывались по этому вопросу, решению обозначенных проблем могли бы способствовать: разработка, внедрение и использование цифрового законодательства [1], а кроме этого внедрение электронного взаимодействия граждан и должностных лиц посредством мессенджеров, чатов или электронных приемных [2, с. 14].

Применение информационных технологий в деятельности органов предварительного следствия МВД России, по возмещения вреда, причиненного преступлением направлено на: 1) оптимизацию затраты времени при документообороте с надзирающими службами – вышестоящие следственные органы, органы прокуратуры, суд; 2) снижение времени доступа лица, ведущего расследование по уголовному делу к справочным ресурсам, содержащим сведения имущественного характера, а так же о денежных средствах содержащихся в банковских учреждениях. Отдельным направлением ведомственного контроля расследования уголовных дел совершенных против собственности граждан, а так же по иным преступлениям, по которым дополнительным объектом преступлений выступают имущественные отношения, возможно обеспечение деятельности руководителей следственного органа информационными технологиями, позволяющими производить полноценный анализ и оценку эффективности вверенного подразделения по возмещению ущерба, причиненного преступлениями.

О.Н. Селедникова имеет мнение, относительно ненадлежащей работы по обеспечению возмещения причиненного преступлением ущерба. Ученая отмечает: детерминантом этого выступает несовершенство законодательства, которое ограничивает оперативное обнаружение имущества и денежных средств, за счет которых это возме-

щение и должно происходить [3, с. 82]. В действительности, стоит согласиться с представленным мнением, так как, законодательных актов, определяющих разработку, внедрение и использование единой информационной системы, позволяющей обеспечить сбор и совокупный анализ сведений об имуществе, имеющихся денежных средства, ценных бумагах, криптовалюте и ее количестве, в банковских и иных государственных, коммерческих или некоммерческих организациях и учреждениях нет. Также по настоящее время не налажено межведомственное электронное взаимодействие между равнозначными, не находящимися в обоюдном подчинении следственными органами и органами дознания (дознание МВД России, дознание ГПН Федеральной противопожарной службы МЧС России, органы предварительного следствия МВД России, Следственный комитет Российской Федерации и др.). Также такого электронного взаимодействия нет и между указанными органами и прокурором, судом, в вопросах о предоставлении процессуальных документов (их цифровых копий), обосновывающих ходатайства о проведении следственных действий: обысков и наложений ареста на имущество.

По мнению Ж.В. Цыренова, основным проблемным вопросом использования информационных технологий в деятельности органов предварительного следствия МВД России, является недостаточное использование средств комплексного получения информации из открытых интернет-ресурсов, а так же из государственных и муниципальных систем [4, с. 138]. Мнение ученого является весьма интересным, однако, с ним мы можем согласиться лишь отчасти и предположить, что неиспользование указанных систем не случайно. Возможно, представители судейского корпуса, при рассмотрении уголовных дел, в которых в качестве доказательств или иных ориентирующих сведений, приобщенных к материалам уголовного дела, представлены копии или изображения, истребованные из таких систем, воспринимаются не однозначно и не могут поддаваться юридической оценке, как полученные не из официального источника, то есть полученные с нарушением норм Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ).

Невозможно недооценивать значимость информационных технологий, уже интегрированных в отечественный уголовный процесс. Так, как правильно отмечается в юридической литературе, является возможным обеспечение трансляции информации по каналам связи без необходимости физического перемещения носителя или обладателя информации [5, с. 172], что позволяет производить следственные и

иные процессуальные действия, а также непроцессуальные мероприятия в короткий промежуток времени.

Мы, в свою очередь, после совершения краткого анализа и установления степени использования информационных технологий, а также предполагая их потенциал, применимый в рамках предварительного следствия, считаем, что органы предварительного следствия органов внутренних дел и иные ведомственные следственные подразделения заинтересованы в создании для использования в расследования специального программного обеспечения, могущего использоваться в вопросах возмещения вреда. Таким техническим решением могла бы являться замкнутая облачная мультисервисная среда, которая позволила бы осуществлять обмен информацией имущественного характера, в том числе, содержащую охраняемую законом тайну, между следственными органами и государственными учреждениями, а впоследствии и частными компаниями в отрасли информационных технологий, примером, одной из которых, может являться МКАО «Яндекс», как крупнейший представитель отрасли информационных технологий в Российской Федерации.

Таким образом, современные информационные технологии оказывают высокий уровень поддержки, в обработке больших массивов информации неструктурированных данных. Кроме этого, полноценное их внедрение в деятельность подразделений, осуществляющих предварительное следствие, увеличит степень оперативности получения информации имущественного характера, в том числе о финансовых и банковских операциях, движении денежных средств, наличии в собственности имущества у физических и юридических лиц.

На наш взгляд, основными направлениями усовершенствования процесса использования информационных технологий станут внедрение технологий межведомственного электронного взаимодействия, а так же создание сервиса формирования унифицированных запросов.

---

1. Выступление Президента Российской Федерации на расширенном заседании коллегии Генеральной прокуратуры Российской Федерации 19 марта 2019 г. [Электронный ресурс]. URL: https:// kremlin.ru (дата обращения: 26.06.2019).
2. Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2023 г. // Рос. газ. 2023. 10 июня. С. 12–16.
3. Селедникова О.Н. Некоторые проблемы возмещения имущественного вреда, причиненного преступлением, на стадии предварительно-

го расследования // Административное и муниципальное право. 2012. № 8. С. 80–85.
4. Цыренов Ж.В. использование информационных технологий в деятельности следственных органов по возмещению ущерба, причиненного преступлениями // Вестник Восточно-Сибирского института МВД России. 2020. № 4 (95).
5. Проказин Д.Л., Семенов Е.А., Ляпин А.И. Развитие видеотехнологий в уголовном процессе России // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3(96). С. 171–178.

Сборник научных статей

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Подписано в печать 27.06.2024. Формат 60x90 1/16.
Усл. печ. л. – 5,81. Тираж 20 экз. Заказ № 888.

Орловский юридический институт МВД России имени В.В. Лукьянова.
302027, г. Орел, ул. Игнатова, 2.