**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

Проблемы информационного обеспечения деятельности правоохранительных органов

**Сборник статей
11-й Всероссийской научно-практической конференции
24 мая 2024 года**

**Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2024**

УДК 351.74:002
ББК 67.401.114
П 78

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России имени
И.Д. Путилина

Выпускается с 2015 года.

П 78 Проблемы информационного обеспечения деятельности правоохранительных органов : сборник статей 11-й Всероссийской научно-практической конференции, 24 мая 2024 года. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2024. – 245 с.
ISBN 978-5-91776-583-9

В сборнике 11-й Всероссийской научно-практической конференции представлены научные статьи, в которых исследуются проблемы противодействия компьютерным преступлениям и обеспечения информационной безопасности.

Предназначен для курсантов, слушателей, адъюнктов, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 351.74:002
ББК 67.401.114

ISBN 978-5-91776-583-9

НОВЫЕ ТЕНДЕНЦИИ В ПРИМЕНЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОВД В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Акапьев В.Л.,
кандидат педагогических наук, доцент;
Араниди Ю.П.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье представлено исследование новых тенденций в области информационных технологий, которые могут быть использованы органами внутренних дел для решения задач, стоящих перед сотрудниками оперативно-разыскной деятельности.

Ключевые слова: оперативно-разыскная деятельность, информационные технологии, автоматизированные информационные системы, динамика преступности.

NEW TRENDS IN THE USE OF INFORMATION TECHNOLOGY TO SOLVE THE TASKS OF THE DEPARTMENT OF INTERNAL AFFAIRS IN OPERATIONAL INVESTIGATIVE ACTIVITIES

Akapyev V.L.,
Candidate of Pedagogical Sciences;
Aranidi Y.P.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article presents a study of new trends in the field of information technology, which can be used by internal affairs agencies to solve the tasks facing employees of operational investigative activities.

Keywords: operational investigative activities, information technologies, automated information systems, crime dynamics.

В современном мире нельзя представить жизнь без информационных технологий, которые определяют уровень развития общества как определенной страны, так и всего мира в целом. Под влиянием информатизации оказываются различные сферы человеческой жизнедеятельности, в том числе государственное управление. Различные виды технологий все чаще используются в деятельности правоохранительных органов, в том числе в оперативно-разыскной деятельности.

Для того чтобы лучше разобраться, как и какими информационными технологиями пользуются сотрудники оперативно-разыскной деятельности, необходимо определить их профессиональные процессы, в которых могут использоваться выше упомянутые технологии:

1. Проверка сообщений, а также осуществление прослушивания телефонных и других устройств.

2. Осуществление поиска важных для дел справок и информации.

3. Реализация обыска необходимых помещений, транспортных средств и других объектов.

4. Получение доступа к информации с компьютерных устройств.

Базовым направлением в применении информационных технологий является использование автоматизированных информационных систем и баз данных. Для того чтобы увеличить качество работы и сократить время выполнения служебных задач, сотрудники органов внутренних дел (далее – ОВД) используют автоматизированные информационные системы и базы данных, которые значительно сокращают время на обработку поступающей информации. Так, в Российской Федерации формируются и применяются различные системы и базы данных, которые появляются в процессе взаимодействия различных ведомств (например, АИС «Оповещение», АИПС «Опознание»).

В силу недостаточного опыта и незнания всех тонкостей оперативно-разыскной деятельности у молодых сотрудников возникают различные препятствия при раскрытии преступлений. Существуют информационно-рекомендательные системы, с помощью которых передается сохраняется опыт в виде информации, а также появляются новые знания. Преимуществом такой системы является доступность, поскольку не требуется иметь специальные навыки для понимания необходимой информации. К примерам информационно-рекомендательные системы относятся: «азартные игры», «серийные преступления» и т.п.

Одним из самых лучших примеров оперативно-разыскного мероприятия (далее – ОРМ) можно назвать «прослушивание телефонных переговоров», оно реализуется с помощью автоматизированной информационной системы – системы технических средств по обеспечению ОРМ. С помощью СОРМ можно отслеживать и фиксировать любые передаваемые пользователем знаки, сигналы, звуки, изображения или голосовую информацию по радиосистеме. Также СОРМ позволяет производить отбор необходимых сообщений, для этого ему понадобится IP-адрес, номер телефона.

Если смотреть на СОРМ с технической точки зрения, то оно включает в себя:

а) комплекс аппаратно-программных средств, которые расположены на объектах связи;

б) программные средства СОРМ, которые находятся на удаленном пункте управления;

в) каналы передачи данных, с помощью которых возникает связь между средствами, расположенными на объектах связи и на удаленном пункте управления.

На сегодняшний день интернет является удобнейшим поиском информации, но также его открытость позволяет совершать различного рода преступления. Интернет дает отличную возможность оперативным сотрудникам получать информацию о предстоящих преступлениях.

Так, многообразие информации в интернете можно разделить на 2 группы:

а) информация, которая может послужить доказательством по делу;

б) информация, помогающая сотрудникам расследовать преступления.

Как показывает практика, отличным способом предотвращения преступлений может являться обычный опрос пользователей, которые могут знать информацию, представляющую интерес для сотрудников органов внутренних дел. Также с помощью Интернета представляется возможность поиска украденных вещей. Так, например, на известном сайте «Avito» можно найти достаточное количество информации или же выйти напрямую к преступникам, которые продают похищенную вещь.

Если посмотреть на статистику, то мы можем заметить, что преступления в экономической сфере становятся актуальнее с каждым годом. Для определения латентной экономической преступности используются экономико-математические методы (включая электронно-вычислительную технику). Они не только позволили сотрудникам ОВД сократить время, но и увеличить качество анализа экономических и других видов информации и сведений, необходимых для выявления указателей на совершенную латентную преступность. Через интернет или по мобильной связи совершается ⅔ всех мошеннических преступлений и 17% краж. В сравнении с 2020 годом таких краж стало на 9,6% меньше, а интернет-мошенничеств и мошенничеств по телефону – больше на 5,1%.

В процессе деятельности сотруднику ОВД необходимо фиксировать оперативно необходимые данные с помощью аудио и видеофиксации. По нашему мнению, наиболее перехваченными устройствами являются компьютеры, телефоны, а также веб-камеры.

Подводя итоги вышесказанному, мы можем сделать вывод, о том что сегодня интернет является отличным помощником для решения служебных задач сотрудников ОВД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (последняя редакция) // Собрание законодательства Российской Федерации. – 2003. – Ст. 2.

2. Омелин В.Н., Квитко А.В. Информационные технологии в оперативно-разыскной деятельности органов внутренних дел // Научный портал МВД России. – 2011. – № 4. – С. 68–73.

3. Информационные технологии управления в органах внутренних дел [Электронный ресурс]. – URL: https://knigogid.ru/books/1898092-informacionnye-tehnologii-upravleniya-v-organah-vnutrennih-del?ysclid=lvlbjfj8m228255535

4. Основы информатики и информационных технологий в ОВД: учебное пособие / Прокопенко А.Н., Жукова П.Н., Дрога А.А., Страхов А.А. – Белгород: Белгородский юридический институт МВД России им. И.Д. Путилина, 2016. – 143 с.

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ КОМПЕТЕНЦИИ ДОЗНАНИЯ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОНЫХ ТЕХНОЛОГИЙ

Александров А.Н.,
кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются важные вопросы нормативного регулирования порядка получения в кредитных организациях сведений по операциям и счетам граждан при расследовании дознавателями преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, а также актуальные проблемы правоприменительной практики по уголовным делам о преступлениях компетенции дознания. Обращается внимание на недостатки в нормативном правовом регулировании отношений и необходимость своевременного получения дознавателем интересующих сведений, имеющих значение для эффективного раскрытия и расследования преступлений, связанных с хищением имущества и денежных средств граждан посредством использования современных информационно-телекоммуникационных технологий. Приводятся примеры правоприменительной практики, свидетельствующие о существовании в настоящее время проблемных вопросов повышения результативности действий уполномоченных органов и должностных лиц при расследовании преступлений. Формулируются выводы и предложения по исправлению недостатков в нормативном правовом регулировании и повышению эффективности действий органа дознания, направленных на охрану прав граждан, потерпевших от преступлений.

Ключевые слова: сведения по счетам граждан, кредитные организации, следователь, дознаватель, уголовное дело, досудебное производство.

TOPICAL ISSUES OF COUNTERACTION AND INVESTIGATION OF CRIMES AND INQUIRIES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Alexandrov A.N.,
Candidate of Law, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article deals with important issues of regulatory regulation of the procedure for obtaining information in credit institutions on transactions and accounts of citizens during the investigation by investigators of crimes committed using information and telecommunication technologies, as well as current problems of law enforcement practice in criminal cases of crimes of the competence of the inquiry. Attention is drawn to the shortcomings in the regulatory legal regulation of relations re-

lated to the need for the investigator to receive timely information of interest that is important for the effective disclosure and investigation of crimes related to the theft of property and money of citizens through the use of modern information and telecommunications technologies. Examples of law enforcement practice are given, indicating the existence at the present time of problematic issues of improving the effectiveness of the actions of authorized bodies and officials in the investigation of crimes. Conclusions and proposals are formulated to correct deficiencies in regulatory legal regulation and improve the effectiveness of the actions of the body of inquiry aimed at protecting the rights of citizens who have suffered from crimes.

Keywords: information on citizens' accounts, credit organizations, investigator, inquirer, criminal case, pre-trial proceedings.

Согласно официальным сведениям МВД России наблюдается ежегодный рост количества совершаемых преступлений, связанных с хищением имущества и денежных средств граждан, посредством использования современных информационно-телекоммуникационных технологий. Только за 2020 год число преступлений в данной сфере возросло на 73,4%, в том числе с использованием сети Интернет – на 91,3%. В 2021 году зарегистрировано 517 722 преступлений, в 2022 году – 522 065 а по итогам 2023 года зафиксировано 676 951 таких преступлений[1]. Значительное количество рассматриваемых преступлений из числа зарегистрированных относятся к компетенции дознавателей органов внутренних дел Российской Федерации.

Подавляющее большинство расследуемых преступлений связано с хищением денежных средств граждан посредством совершения операций по их счетам, открытым в кредитных организациях, соответственно, такие сведения имеют большое значение как для установления и доказывания способа совершения преступления, так и для установления лица (лиц), его совершившего, и других обстоятельств. Быстрое раскрытие и своевременное расследование таких преступлений напрямую зависит от быстроты получения дознавателем интересующих сведений.

Согласно положениям ст. 26 Федерального закона Российской Федерации «О банках и банковской деятельности» справки по операциям, счетам и вкладам граждан кредитной организацией выдаются по запросу органам предварительного следствия по делам, находящими в их производстве, при наличии согласия руководителя следственного органа[2]. Вместе с тем подобный механизм получения справок по счетам и вкладам физических лиц для сотрудников специализированных подразделений дознания не предусмотрен, в связи с чем для

[1] Официальный сайт МВД России [Электронный ресурс]. – URL://https://мвд.рф/ (дата обращения: 20.05.2024).

[2] Федеральный закон от 02.12.1990 № 395-1 (ред. от 12.12.2023) «О банках и банковской деятельности» (с изм. и доп., вступ. в силу с 01.05.2024) // Собрание законодательства РФ. 1996. № 6. Ст. 492.

получения указанных сведений дознавателю требуется последовательно выполнить ряд необходимых процессуальных и организационных действий.

Необходимо отметить тот факт, что еще в 2018 году в МВД России приступили к разработке проекта закона о внесении изменений в ст. 26 вышеназванного Федерального закона. В качестве обоснования такой необходимости эксперты ведомства поясняли, что, согласно действующей редакции этой статьи, только следователь с согласия руководителя следственного органа уполномочен получать справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также по операциям и вкладам физических лиц. Вместе с тем к подследственности дознавателей также отнесены преступления, связанные с движением денежных средств по счетам граждан и юридических лиц. Однако дознаватель имеет право получать информацию только о счетах подозреваемых (обвиняемых) или лиц, несущих по закону материальную ответственность за их действия, в рамках ч. 7 ст. 115 (Наложение ареста на имущество) Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) для обеспечения исполнения приговора. Отсутствие у дознавателя полномочий, аналогичных полномочиям следователя, не позволяет обеспечить своевременное выполнение следственных действий, направленных на сбор доказательств, что существенно затрудняет установление виновного лица, влечет нарушение прав потерпевших на доступ к правосудию и обуславливает низкий процент возмещаемости ущерба по данной категории дел.

В этой связи экспертами МВД России и Министерства юстиции Российской Федерации предлагалось включить дознавателя в перечень должностных лиц, правомочных запрашивать в кредитных организациях сведения о вкладах и счетах физических лиц, операциях и счетах юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица[1].

Однако до настоящего времени названные планируемые изменения в ст. 26 Федерального закона Российской Федерации «О банках и банковской деятельности» так и не внесены. Дознаватели могут получить интересующие сведения только в порядке, предусмотренном уголовно-процессуальным законодательством.

Так чтобы получить справку по операциям и счетам физического лица, в порядке ч. 1 ст. 165 УПК РФ дознаватель должен подготовить постановление о возбуждении перед судом ходатайства о производстве выемки документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях. Такое ходатайство дознаватель обязан согласовать с надзирающим прокурором и при его получении направить в районный суд для рассмотрения по существу. Следует отметить, что в обоснование своего ходатайства дознаватель обязан приложить к нему соответствующие копии материалов уголовного дела.

[1] СПС «Гарант» [Электронный ресурс]. – URL: https://www.garant.ru/news/1220532/ (дата обращения: 20.05.2024).

В случае удовлетворения судом заявленного ходатайства дознаватель должен обеспечить предоставление в кредитную организацию постановления суда. При этом одновременное производство выемки документов, содержащих информацию о вкладах и счетах граждан осуществить не представляется возможным по причине необходимости подготовки и оформления банком необходимых документов. Как показывает практика, временной период с момента подготовки дознавателем постановления о возбуждении перед судом ходатайства о разрешении производства выемки документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, до проведения такой выемки в банке составляет от 30 суток до трех месяцев[1]. Указанный период времени складывается из следующих фактических действий дознавателя: подготовки, согласования с надзирающим прокурором ходатайства перед судом о разрешении производства выемки; получения постановления суда и направление его почтовой связью в офис соответствующего банка (кредитной организации); ожидания сообщения о готовности запрашиваемых сведений и возможности производства выемки в банке; фактического производства выемки документов, содержащих интересующие сведения. Большую часть вышеназванного временного периода занимает подготовка банком официальных сведений по операциям, счетам и вкладам граждан. При этом, подчеркнем, такие сведения готовит только головной офис кредитной организации (банка). И даже если по месту производства предварительного расследования существует отделение соответствующего банка, то оно может предоставить запрашиваемые сведения только после их направления из центрального офиса.

В качестве примера приведем уголовное дело, расследуемое дознавателем по обвинению гражданина М. в совершении преступления, предусмотренного ч. 1 ст. 159 УК РФ. В ходе дознания установлено, что М. (число, месяц) 2023 года около 00 часов 30 минут находился по месту жительства (точный адрес), где у него возник преступный умысел, направленный на хищение денежных средств пользователей сайта размещения объявлений «Авито» под вымышленным предлогом продажи им сотового телефона. С целью реализации своего преступного умысла М. в своем аккаунте умышленно разместил ложное объявление о продаже не имевшегося у него сотового телефона марки «Самсунг» модели «Гэлэкси С8», выданного за собственный, с указанием продажной цены 2 500 рублей, в сопровождении фотографий, найденных в интернете, умышленно введя тем самым в заблуждение пользователей социальной сети «Авито», заведомо не намереваясь выполнить взятые на себя обязательства. После получения (число, месяц) 2023 года в 03 часа 00 минут сообщения от гражданина Н. о желании приобрести указанный в объявлении сотовый телефон, у М. возник преступный умысел, направленный на хищение путем обмана у Н. денежных средств под предлогом продажи ему указанного в объявлении сотового телефона, обозначив свои условия о необходимости производства оплаты в сумме

[1] Материалы, предоставленные объединенным филиалом кафедр уголовного процесса и уголовно-правовых дисциплин на базе Отдела организации дознания УМВД России по Белгородской области.

300 рублей за доставку его до Сахалинской области, тем самым обманув Н. относительно своих истинных намерений. В продолжение своего преступного умысла, направленного на хищение денежных средств путем обмана, М. подключил интернет со своего сотового телефона марки «Айфон» модели «6» к домашнему компьютеру (ноутбуку), зашел на сайт «Почта России», заполнил заявку на отправление товара, сделал скриншот экрана компьютера и переместил его в окно компьютерной программы «Пэинт» (Paint), где с помощью инструмента «кисть» изменил в трек-номере цифры и отправил переделанную в вышеуказанной программе фотографию заявки гражданину Н., тем самым ввел последнего в заблуждение относительно отправления товара. Таким образом, Н. со счета (точный номер) своей банковской карты (точный номер), открытого (число, месяц) 2023 в дополнительном офисе Дальневосточного филиала ПАО КБ «Восточный» посредством приложения «Восточный экспресс банк» (число, месяц) 2023 года в 19 часов 36 минут осуществил перевод денежных средств на сумму 2 850 рублей, где 2 500 рублей составляет оплата за якобы отправленный сотовый телефон марки «Самсунг» модели «Гэлэкси С8», 300 рублей составляет оплата за доставку вышеуказанного телефона и 50 рублей – комиссия за перевод денежных средств на указанный М. расчетный счет (точный номер) банковской карты (точный номер), открытого на имя М. в дополнительном офисе ПАО «Сбербанк России», расположенном по адресу: г. Белгород, проспект Богдана Хмельницкого, д. 160. Завладев похищенными денежными средствами, М. распорядился ими по собственному усмотрению. Таким образом, М. (число, месяц) 2023 года в 19 часов 36 минут, умышленно из корыстных побуждений, путем обмана похитил денежные средства в сумме 2 800 рублей, принадлежащие Н., причинив тем самым последнему материальный ущерб на вышеуказанную сумму[1].

По данному уголовному делу дознавателю необходимо было получить в кредитной организации официальные сведения о движении по счетам соответствующих участников уголовного судопроизводства, в целях установления обстоятельств, подлежащих доказыванию. С момента возбуждения уголовного дела дознавателем и до фактического изъятия в ходе выемки в банке необходимых сведений прошло 68 суток.

При этом у может возникнуть вопрос: а почему нельзя было попросить самого потерпевшего, чтобы он лично обратился в кредитную организацию с заявлением о предоставлении сведений по операциям своего счета? Ответом на такой вопрос является следующие объяснение: поскольку сведения, содержащиеся в соответствующей справке кредитной организации по уголовному делу признаются в качестве доказательств, то в целях обеспечения их достоверности дознаватели исключают возникновение возможных рисков признания их недопустимыми либо надзирающим прокурором, либо судом при рассмотрении уголовного дела по существу. Факт предоставления лично потерпевшим справки,

[1] Материалы, предоставленные объединенным филиалом кафедр уголовного процесса и уголовно-правовых дисциплин на базе Отдела организации дознания УМВД России по Белгородской области.

которую он запросил в кредитной организации, не может гарантировать возникновение различного рода сомнений на предмет наличия недостоверных сведений. Поэтому правоприменительная практика специализированных подразделений дознания не использует такой способ в вопросе собирания доказательств по причине обеспечения допустимости доказательств по уголовным делам.

В свою очередь, практика предварительного следствия по уголовным делам о преступлениях, совершаемых с использованием современных информационно-телекоммуникационных технологий, свидетельствует о положительном эффекте нормативного правового регулирования вопроса выдачи справок по операциям и счетам граждан органам предварительного следствия при наличии согласия руководителя следственного органа.

Так, для получения следователем необходимых сведений ему необходимо направить электронной почтой соответствующий запрос, который обрабатывается кредитной организацией в течение суток с последующим ответом. Более того, на примере Следственного управления УМВД России по Белгородской области заключенное соглашение со Сбербанком России предусматривает упрощенную процедуру направления запросов следователями и получения ответов из отделений банка посредством электронного документооборота. Соответствующая программа устанавливается на персональном компьютере следователя, который расследует преступления в указанной сфере, что позволяет ему, не покидая рабочего места, максимально быстро и гарантированно получать запрашиваемую информацию в кредитных организациях. В отдельных случаях выписки об операциях по банковскому счету или счету банковской карты предоставляется кредитной организацией следователю на оптическом диске, который приобщается к материалам уголовного дела, а содержащаяся на нем информация признается и приобщается в качестве доказательства[1].

Пример: в ходе расследования уголовного дела по обвинению гражданина И. в совершении ряда преступлений, предусмотренных ч. 4 ст. 159 УК РФ, установлено, что гражданин И. совершил несколько умышленных тяжких преступлений против собственности в составе организованной группы с Б., Г. и лицами, не установленными в ходе следствия. По каждому эпизоду преступной деятельности гражданина И. следователем в кредитных организациях запрашивались сведения по операциям и счетам граждан, которые в короткие сроки (в течение 2–3 дней) предоставлялись посредством записи необходимой информации на оптический диск.

Таким образом, приведенные примеры очевидно свидетельствуют об эффективности предварительного расследования по уголовному делу, которое значительно сложнее в расследовании. И если бы следователю приходилось получать необходимые сведения по счетам граждан в том же порядке, который законодательно предусмотрен по уголовным делам компетенции дознания, то

[1] Материалы, предоставленные объединенным филиалом кафедр уголовного процесса и уголовно-правовых дисциплин на базе Следственного управления УМВД России по Белгородской области.

сроки предварительного расследования были бы достаточно продолжительными, а его эффективность крайне низкой.

Анализ нормативного регулирования и правоприменительная практика по данному вопросу свидетельствует о наличии явного пробела, который существенно затрудняет и затягивает производство дознания по уголовным делам о преступлениях, совершаемых с использованием современных компьютерных технологий. Отсутствие у дознавателя возможностей, аналогичных возможностям следователя, на получение информации о вкладах и счетах граждан в банках и кредитных организациях не позволяет обеспечить своевременное выполнение следственных действий, направленных на сбор доказательств, а соответственно, и соблюдение принципа разумности сроков уголовного судопроизводства, а также затрудняет установление виновного лица, влечет нарушение прав потерпевших на доступ к правосудию и обуславливает низкую эффективность деятельности по возмещению имущественного ущерба по данной категории уголовных дел.

В этой связи в целях повышения эффективности оперативно-служебной деятельности при раскрытии и расследовании преступлений считаем целесообразным внесение изменений в ст. 26 Федерального закона Российской Федерации «О банках и банковской деятельности», предусмотрев выдачу кредитной организацией также подразделениям дознания справок по операциям и счетам граждан при наличии согласия начальника органа дознания. Соответственно, целесообразно названную норму после слов «…а при наличии согласия руководителя следственного органа – органам предварительного следствия» дополнить словами «а также при наличии согласия начальника органа дознания – подразделениям дознания».

Скорейшее принятие очевидных и давно назревших предлагаемых изменений в законодательство позволит обеспечить повышение эффективности раскрытия и расследования преступлений компетенции дознания, совершаемых с использованием информационно-телекоммуникационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 02.12.1990 № 395-1 (ред. от 12.12.2023) «О банках и банковской деятельности» (с изм. и доп., вступ. в силу с 01.05.2024) // Собрание законодательства РФ. 1996. № 6. Ст. 492.

ОНЛАЙН-МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Атеш К.Н.,
Калашникова А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматривается проблема онлайн-мошенничества с использованием искусственного интеллекта. Актуальность данной темы состоит в том, что с развитием IT-технологий электронный документооборот внедряется во все сферы деятельности. Именно поэтому необходимо проводить мониторинг и анализ преступлений в секторе кибербезопасности. Также за последнее десятилетие развитие искусственного интеллекта приводит все к большим потерям финансовой, социальной и политических сфер.

Ключевые слова: мошенничество, кибербезопасность, угроза, искусственный интеллект, злоумышленники.

ONLINE FRAUD USING ARTIFICIAL INTELLIGENCE

Atesh K.N.,
Kalashnikova A.A.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: the article discusses the problem of online fraud using artificial intelligence. The relevance of this topic is that with the development of IT technologies, electronic document management is being introduced into all areas of activity. This is why it is necessary to monitor and analyze crimes in the cybersecurity sector. And over the last decade, the development of artificial intelligence has led to ever greater losses in the financial, social and political spheres.

Keywords: fraud, cybersecurity, threat, artificial intelligence, attackers.

Злоумышленники активно используют технологии искусственного интеллекта для создания более убедительных фейков и контролирования поведения пользователей для реализации корыстных мошеннических целей.

Мошенничества с использованием искусственного интеллекта (далее – ИИ) представляют собой новый и эволюционирующий вид киберпреступлений, где злоумышленники используются технологии искусственного интеллекта для создания усложненных, изощренных и трудно обнаружимых атак. Рассмотрим некоторые примеры мошенничества с использованием ИИ:

1. Фишинг и мошеннические атаки. Злоумышленники используют ИИ для персонализированных фишинговых сообщений, которые адаптированы под конкретного пользователя с целью получения выгоды путем выстраивания условий доверия пользователя (интересы, поведение).

2. Мошенничества в финансовой сфере.Для проведения манипуляций на финансовых рынках зачастую злоумышленники пользуются методами машинного оборудования, которые основаны на ИИ. Целью данного вида мошенничества является незаконное обогащение на крупных финансовых рынках [3].

3. Социальная инженерия. Использование ИИ для создания фейковых медиа профилей, целью которого является манипулирование общественным мнением или организации атак на конкретные личности.

4. Создание дипфейков. Применение технологий ИИ для генерации и создания реалистичных голосовых и видеозаписей как известных лидеров или политиков для распространения дезинформации, так и обычных пользователей, с целью шантажа и вымогательства денежных средств после взлома аккаунтов для наиболее реалистичного предлога и эффективного метода достижения корыстных целей.

5. Фальсификация идентификации.Создание злоумышленниками искусственных биометрических данных (лица, отпечатков пальцев и т.д.), при помощи которых возможно обходить системы аутентификации пользователя.

Средства борьбы с мошенничеством с использованием ИИ:

1. Внедрение средств обнаружения и предотвращения, которые позволят оперативно отслеживать, мониторить и пресекать попытки использования ИИ в корыстных целях.

2. Использование систем сбора и анализа аномалий (отклонений), а также машинного обучения для выявления нестандартных или подозрительных паттернов в поведении как систем, так и пользователей.

3. Предотвращение фальсификации информации путем применения криптографии и безопасных методов обработки персональных данных, ввод в доступную систему пользователей двухуровневой аутентификации.

4. Использование блочкейна для создания прозрачных и невозможных изменению записей, что поможет в предотвращении фальсификации данных [1].

Важным аспектом уменьшения количества киберпреступлений с использованием ИИ на предприятиях является своевременное обучение персонала, позволяющее сократить возможность утечки со счетов денежных средств. Также оно играет ключевую роль в укреплении общей кибербезопасности организации. Постоянно изменяющаяся среда угроз требует от персонала быть в курсе последних тенденций и обладать навыками по противодействию разнообразным кибератакам.

Эффективные методы обучения:

1. Проведение симуляций кибератак и сценариев для обучения персонала реальным ситуациям, связанным с применением новых видов мошенничеств при использовании ИИ.

2. Использование онлайн-платформ и вебинаров для удобного и систематического обучения.

3. Регулярное обновление программ с учетом последних тенденций в кибербезопасности.

Обучение персонала становится важным звеном в стратегии кибербезопасности. Эффективные методы обучения играют решающую роль в укреплении киберстойкости и общей безопасности цифрового пространства.

Искусственный интеллект применяется также в отношении граждан. С его развитием почти каждый инцидент в данной сфере не обходится без применения социальной инженерии. Злоумышленники используют сгенерированные голоса, фото – и видеоматериалы близких пользователю людей для упрощения овладевания его денежными средствами. Для того чтобы обезопасить граждан, необходимо повышать уровень осведомленности пользователей. Только личная бдительность и критический подход к полученной информации позволит распознать угрозу или манипуляцию и предотвратить их последствия.

Таким образом, из вышеперечисленного можно сделать вывод о том, что необходимо регулярно анализировать показатели и уровень преступности онлайн-мошенничества с использованием ИИ для обеспечения безопасности не только каждого пользователя, но и на уровне государства в целом. Для этого необходимо проводить ряд мероприятий, гарантирующих выявление и пресечение противоправных деяний в IT-сфере.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Амиргамзаев Г.Г., Магомедова Х.А. Использование блокчейн-технологии для хранения учетных данных // Наука: общество, экономика, право. – 2020. – № 2. – С. 268–273.

2. Емельянова О.В. Использование искусственного интеллекта для обнаружения преступлений / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 10-й Всероссийской научно-практической конференции, Белгород, 19 мая 2023 года. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2023. – С. 72–76.

3. Скрипниченко В.Ю., Исаева О.Н. Мошенничество как угроза экономической безопасности государства // ИПЭФ. – 2022. – № 1.

4. Куриленко Ю.А., Любаева Д.С. Мошенничества в сфере компьютерной информации / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 10-й Всероссийской научно-практической конференции, Белгород, 19 мая 2023 года. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2023. – С. 125–128.

5. Основы кибербезопасности в деятельности сотрудников правоохранительных органов / Прокопенко А.Н., Страхов А.А., Ковалева Е.Г., Акапьев В.Л., Гаврющенко А.П., Рыбальченко А.Ю. – Белгород, 2023.

6. Страхов А.А., Прокопенко А.Н. Криминальный потенциал искусственного интеллекта / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 10-й Всероссийской научно-практической конференции, Белгород, 19 мая 2023 года. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2023. – С. 164–172.

7. Чирьева В.Е., Смирнов В.М. Проблемы внедрения искусственного интеллекта и машинного обучения в технологии кибербезопасности // Тенденции развития науки и образования. – 2023. – № 98-4. – С. 154–157.

ПЕРСПЕКТИВЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ НА СОВРЕМЕННОМ ЭТАПЕ

Богачева М.В.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассмотрены перспективы информационного обеспечения деятельности органов внутренних дел на современном этапе.

Ключевые слова: органы внутренних дел, информационное обеспечение, оперативно-справочные информационные ресурсы, обмен информацией.

PROSPECTS OF INFORMATION SUPPORT FOR THE ACTIVITIES OF INTERNAL AFFAIRS BODIES AT THE PRESENT STAGE

Bogacheva M.V.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in this paper, the prospects of information support for the activities of internal affairs bodies at the present stage are considered.

Keywords: internal affairs bodies, information support, operational and reference information resources, information exchange.

Эффективная деятельность органов внутренних дел невозможна без организации их информационного обеспечения, для чего в министерстве на протяжении 30 лет проводится последовательная и целенаправленная работа. Создаются базы и банки данных, которые впоследствии объединяются общие информационные ресурсы. Внедряется электронный документооборот, как в отдельных территориальных органах внутренних дел, так и на уровне МВД России в целом. Развиваются телекоммуникационные системы и средства связи, соответствующие мировому уровню. Завершена работа по стандартизации учета пользователей единой информационно-телекоммуникационной сети МВД России. Подавляющее большинство информационных ресурсов министерства объединено на базе централизованных центров обработки данных.

При этом не вызывает сомнений, что как оперативно-служебная, так и управленческая деятельность органов внутренних дел требует соответствующего информационного обеспечения [1]. В частности, поиск и использование информации. Как накопленной в информационных ресурсах министерства, так и полученной из других государственных органов в результате информационного обмена является одной из основ оперативно-служебной деятельности.

В органах внутренних дел созданы разыскные и оперативно-справочные информационные ресурсы, сконцентрированы сведения государственной дактилоскопической регистрации и другие экспертно-криминалистические ресур-

сы. Собирается информация о преступлениях и лицах, их совершивших, правонарушениях, лицах, пропавших без вести, неопознанных трупах. Отдельно необходимо упомянуть информационные ресурсы о гражданах России, выданных им документах (водительских удостоверениях, общегражданских и заграничных паспортах), мигрантах и выданных им документах. Также осуществляется регистрация транспортных средств и оружия, различных происшествий и иная информация. Можно констатировать, что количество объектов учета в информационных ресурсах МВД России исчисляется сотнями миллиардов записей. Осуществляется постоянный обмен оперативной и справочной информацией с правоохранительными органами Российской Федерации, государствами СНГ, другими иностранными субъектами через Интерпол.

Все вышеперечисленные информационные ресурсы используются для информационного обеспечения раскрытия и расследования преступлений, правонарушений, поиска преступников, противодействия противоправной и террористической деятельности и в других оперативно-служебных целях.

Информационное взаимодействие между подразделениями МВД России, органами внутренних дел, государственными органами и организациями является основой управленческой деятельности. Для информационного обеспечения управленческой деятельности органов внутренних дел созданы различные ресурсы. Активно используется статистическая информация, внедрены системы электронного документооборота, в том числе на общегосударственном уровне. Применяются различные справочные правовые системы, кадровые и финансовые информационные ресурсы [2]. Значительная часть других видов деятельности также осуществляется в электронном виде, в том числе оказание государственных услуг.

В последнее десятилетие в развитии информационного обеспечения МВД России наблюдаются одновременно две взаимодополняющие тенденции. С одной стороны, активно взаимодействуют между собой имеющиеся базы и банки данных, создана система ИСОД МВД России, обеспечившая совместную интеграцию различных информационных ресурсов. Также выстроена цельная система обеспечения кибербезопасности, работающая на единых принципах и объединившая все защищаемые информационные системы в один защитный контур. Подобный подход позволяет значительно облегчить защиту информации, уменьшить используемые материальные и вычислительные ресурсы, осуществлять централизованную обработку больших данных, начать внедрение в деятельность органов внутренних дел технологий искусственного интеллекта.

С другой стороны, в деятельность полиции повсеместно внедряются различные мобильные устройства. Осуществляется переход от стационарных рабочих мест к использованию смартфонов, ноутбуков, планшетов и иных носимых устройств. В то же время использование устройств, не включенных в защищенный контур стационарной информационно-телекоммуникационной сети, создает существенные угрозы кибербезопасности. При этом если мобильные устройства имеют возможность подключения к сети связи и электричеству, например в линейном пункте полиции, пункте участкового уполномоченного полиции или на посту Госавтоинспекции, то их функционал может быть фактически неотличим от стационарных АРМ. А в случае применения полностью

мобильных устройств, в том числе там, где не действует мобильная связь, возникают проблемы с доступом к централизованным информационным ресурсам. Особенно характерна данная проблема для органов внутренних дел на транспорте и дорожной патрульной службы.

Оценивая другие проблемы развития информационного обеспечения органов внутренних дел, необходимо отметить, что количество накапливаемой информации в МВД России растет с каждым годом. Количество записей огромно, однако подразделения и службы или не осведомлены о их наличии, либо имеют к данной информации доступа. Многие сервисы ИСОД предназначены исключительно для конкретных служб. Кроме того, все попытки анализа направлены преимущественно на вычисление соотношений относительно показателей прошлого года или просто сбор статистических сведений. При этом предметного анализа по отдельным проблемным вопросам, выявление тенденций, предотвращение организованных преступлений и правонарушений системно не осуществляется. Работа ведется преимущественно здесь и сейчас, а деятельность на перспективу, в том числе с использованием информационных ресурсов, на уровне районного органа внутренних дел не проводится.

Представляется, что накопленные объемы информации позволяют осуществлять реальный анализ оперативной обстановки в конкретном регионе или муниципальном образовании: выявление зависимости криминогенной обстановки от экономической ситуации, миграционной ситуации, транспортной доступности; влияние специальной военной операции на обстановку в регионе; близость к фронту, а также другие факторы. Органы внутренних дел обладают всеми возможностями для того, чтобы не только знать, что происходит на конкретной территории, но и прогнозировать, происходящее, а также принимать своевременные меры к исправлению ситуации вместе в другими государственными органами. В данной сфере необходимо самое перспективное направление для использования технологий искусственного интеллекта. Это в свою очередь, требует, разработки методик анализа, которые должны быть нормативно закреплены преимущественно на межведомственном уровне или на уровне субъекта Российской Федерации.

Другим направлением развития информационного обеспечения оперативно-служебной деятельности является расширение возможностей использования накопленной информации для раскрытия и расследования преступлений. Проведенная работа по интеграции информационных ресурсов уже дает существенный положительный эффект. Однако в дальнейшем она потребует системности, углубления и расширения, а также распространения достигнутой возможности сквозного поиска по определенным базам данных на все накопленные информационные ресурсы. Российская полиция с точки зрения информационного обеспечения еще довольно далека от возможностей, демонстрируемых, например, в сериале про «федеральную экспертную службу», несмотря на то, что она по сюжету является частью полиции.

Все сведения, которые обычно ищут сыщики в кино, есть в распоряжении реальных оперативников но они сосредоточены в различных базах и банках данных, требуют обращения к «смежникам», к гражданским базам данных, написание запросов на получение информации в коммерческих организациях.

В отдельных случаях для проведения оперативно-разыскных мероприятий требуется разрешение суда, а ряд сведений может быть предоставлен исключительно в рамках возбужденного уголовного дела. Представляется, что информационное обеспечение органов внутренних дел должно пройти длительный путь по дальнейшей интеграции баз и банков данных, созданию возможностей глобального поиска, разработке новых поисковых инструментов.

Отдельно необходимо остановиться на проблемах противодействия организованной преступности, совершающей преступления с использованием информационно-телекоммуникационных технологий. Расширение данного вида преступлений объясняется тем, что они осуществляются с поддержкой иностранных спецслужб, преимущественно с территории Украины. Как отметил Министр внутренних дел России Владимир Колокольцев в интервью журналисту Павлу Зарубину 7 апреля 2024 года, органы внутренних дел начинают свое участие в противодействии данному виду преступлений после того, как деньги были уже украдены и, как правило выведены из страны[1]. В этой связи представляется важным углубление информационного взаимодействия между соответствующими подразделениями органов внутренних дел и банковским сообществом, привлечение сотрудников полиции для предотвращения преступных схем на этапе совершения преступлений и блокирование вывода денежных средств из России. Также требуются изменения в законодательство, которые повлияют на банки и компании мобильной связи и существенно уменьшат возможности преступников по совершению преступлений.

Подводя итог рассмотренным выше перспективам развития информационного обеспечения органов внутренних дел, можно констатировать, что МВД России совершило значительный рывок на пути к созданию всеобъемлющего единого полицейского информационного пространства. Однако ряд вопросов так и не нашел своего развития. Первым из них является создание возможностей сквозного поиска по всем базам данных МВД России, а также по базам данных других правоохранительных и государственных органов. Это позволит вывести информационное обеспечение процессов раскрытия и расследования преступлений на принципиально новый уровень. Вторым вопросом является создание методик анализа оперативной обстановки на основании информации, имеющейся в базах и банках данных МВД России и других ведомств. Создание компьютерного моделирования ситуации для конкретных муниципальных образований, прогнозирование криминогенной и социальной обстановки не на основании экспертных оценок, а на основании знаний является необходимым на современном этапе. Уверены что данное направление является наиболее перспективным для внедрения технологий искусственного интеллекта в деятельность органов внутренних дел.

[1] В. Колокольцев: за год раскрыто 45 тысяч преступлений прошлых лет [Электронный ресурс]. – URL: https://smotrim.ru/article/3891617 (дата обращения: 14.04.2024).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анищенко В.Н., Мацкевич Р.С. Управление интеллектуальными ресурсами органов внутренних дел при обеспечении экономической безопасности России: монография. – Москва: ВНИИ МВД России. – 254 с.
2. Дюков А.В. Организация системы информационно-правового обеспечения деятельности органов внутренних дел: дис. ... канд. юрид. наук. – Москва, 2009. – 371 с.

БЕЗОПАСНОСТЬ В СЕТИ: КАК РАСПОЗНАТЬ МОШЕННИЧЕСКОЕ ПИСЬМО

Большунов Е.Г.;
Поликарпов Е.С.,
кандидат технических наук, доцент
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в работе исследуется мошенничество информационно-телекоммуникационной сети с использованием фишинговых писем. Приводятся типовые приемы, используемые злоумышленниками, на примере реальных писем электронной почты, а также выделяются основные маркеры для идентификации. По результатам исследования предлагается алгоритм проверки электронных писем.

Ключевые слова: информационная безопасность, кибербезопасность, мошенничество в Сети, фишинг, повышение осведомленности, социальная инженерия.

NETWORK SECURITY: HOW TO RECOGNIZE A FRAUDULENT EMAIL

Bolshunov E.G.;
Polikarpov E.S.,
Candidate of Technical Sciences, Associate Professor
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: the article discusses fraud in the information and telecommunications network using phishing emails. Typical techniques used by attackers based on the example of real emails are given, and the main markers for identification are highlighted. Based on the results of the study, an email verification algorithm was proposed.

Keywords: information security, cybersecurity, online fraud, phishing, awareness raising, social engineering.

Проблема мошенничества в сфере электронных почтовых сервисов на данный момент является одной из самых опасных. Это обусловлено тем, что электронной почтой с каждым годом пользуется все большее число граждан. Согласно сетевой статистике среди российских пользователей электронной почты преобладают следующие домены: mail.ru – 70,1%, yandex.ru – 18,1%, gmail.com – 7,7% и менее 4% – все остальные. Число пользователей ежедневно увеличивается, о чем свидетельствуют показатели активных пользователей лидера электронных почтовых сервисов mail.ru – 17 миллионов активных пользователей в день и 49 миллионов в месяц. Взрывной рост числа пользователей электронной почты обусловлен прежде всего ее доступностью и простотой как для рядового пользователя, так и для представителей организаций, возможностью управления различными процессами в бизнесе, а также внедрением современных технологий: облачные хранилища, умные ответы, голосовые помощники и др.

С другой стороны, с активным развитием цифровых технологий происходит адаптация к современным условиям в части совершения множества преступлений, в том числе мошенничества с использованием электронной почты. Именно поэтому пользователи электронных почтовых сервисов все чаще становятся жертвами мошенничества. Так, согласно статистике национального агентства финансовых исследований (НАФИ) в 2023 году 82% опрошенных россиян сообщили, что за последние месяцы в отношении их была совершена как минимум одна попытка мошенничества. Порядка 40% опрошенных заявили, что получили сообщения и электронные письма, содержащие вирусы или вредоносные ссылки, переход по которым связан со следующими финансовыми угрозами:

– блокировка устройства пользователя с условием разблокировки после оплаты;

– кража персональных данных пользователя, в том числе информации о банковских счетах и картах.

Вышеперечисленные статистические сведения подтверждают актуальность тематики настоящей работы, которая определяется потребностью совершенствования системы предупреждения и противодействия деятельности, связанной с мошенничеством в электронной почте.

Главной целью исследования является формирование рекомендаций по борьбе с мошенничеством в электронной почте, которые ориентированы для каждого пользователя электронных почтовых сервисов.

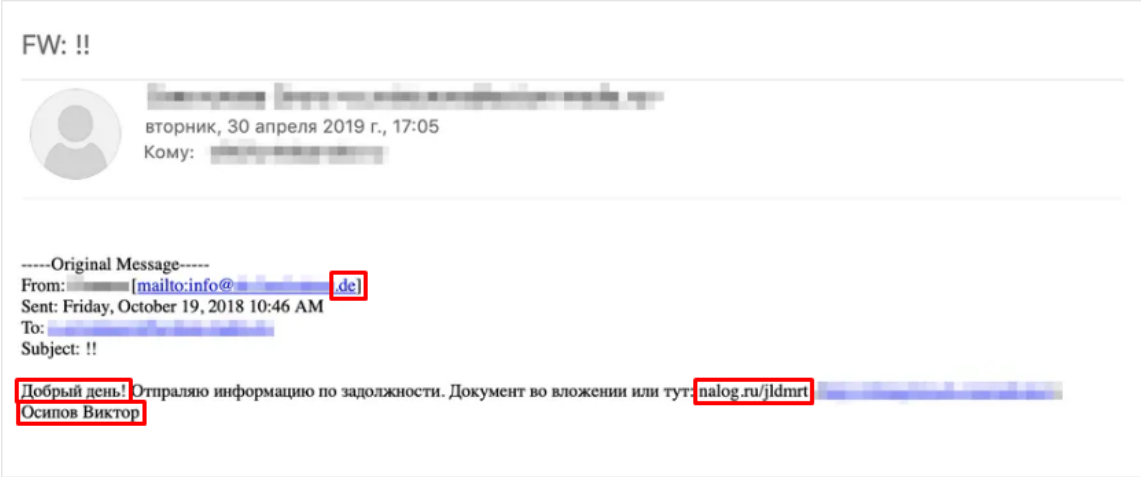
Способы мошенничества с использованием электронной почты можно условно разделить на следующие виды:

– письма от «государственных» организаций;

– письма от коллег по работе;

– выигрыши в лотерею и иные сомнительные способы получения денежных средств.

Разберем каждый их них на конкретном примере, попытаемся определить призгпки, а также выделим «красные флаги» («красный флаг» – предупреждающий знак или сигнал об опасности).


FW: !!

вторник, 30 апреля 2019 г., 17:05
Кому:

-----Original Message-----
From: [mailto:info@ .de]
Sent: Friday, October 19, 2018 10:46 AM
To:
Subject: !!

Добрый день! Отпраляю информацию по задолжности. Документ во вложении или тут: nalog.ru/jldmrt
Осипов Виктор

Рисунок 1. Мошенническое письмо «налоговой» службы

В повседневной деятельности человек часто обращается к представителям государственных структур, например в налоговую службу, пенсионный фонд или к правоохранительным органам, за помощью и разъяснением интересующих его вопросов. Однако необходимо помнить, что и злоумышленники нередко представляются работниками государственных организаций, воздействуя на пользователя методами социальной инженерии (получают необходимую информацию используя доверчивость, слабую осведомленность или неосторожность пользователя), побуждают его совершать действия, которые могут привести к утечке его персональных данных, в том числе банковских учетных данных.

В качестве примера рассмотрим письмо от представителей «налоговой службы», представленное на рисунке 1.

На данном рисунке цветом выделены «красные флаги». Как было сказано ранее, это то, на что необходимо обратить внимание в первую очередь:

1. info@ah-fussleisten.de – почтовый адрес отправителя заканчивается доменом .de, который является национальным доменом верхнего уровня для Германии. В то же время Федеральная налоговая служба Российской Федерации (ФНС РФ) имеет почту info@mon.gov.ru
2. nalog.ru/jldmrt – изначально кажется, что это сайт nalog.ru, на котором мы можем ознакомится с отправленной информацией, не вызывает подозрений. Однако настоящая ссылка на поддельный, зеркальный сайт, скрывается далее.
3. «Добрый день!» или, например, «Осипов Виктор» – такое оформление часто выдает мошеннические письма. Обезличенное приветствие, а также отсутствие должности специалиста и контактов для обратной связи – еще один повод закрыть и удалить данное письмо.

Таким образом, при получении электронных писем от «государственных» организаций необходимо внимательно ознакомиться с содержимым, сверить почтовые адреса, номера телефонов, а также иные контактные данные, а при

возникновении каких-либо подозрений обратиться к представителям организаций по контактам, указанным на их официальных ресурсах.

Основная проблема при работе с почтой – невнимательность. И нередко такая невнимательность может привести к утечке конфиденциальной информации, потере финансовых активов, компрометации безопасности сети, а также большим репутационным рискам. Так, например, специалистами «Ростелекома» в рамках проверки сотрудников организации было составлено фишинговое (фишинг от англ. phishing – процесс выманивания конфиденциальной информации у человека) электронное письмо (см. рис. 2).

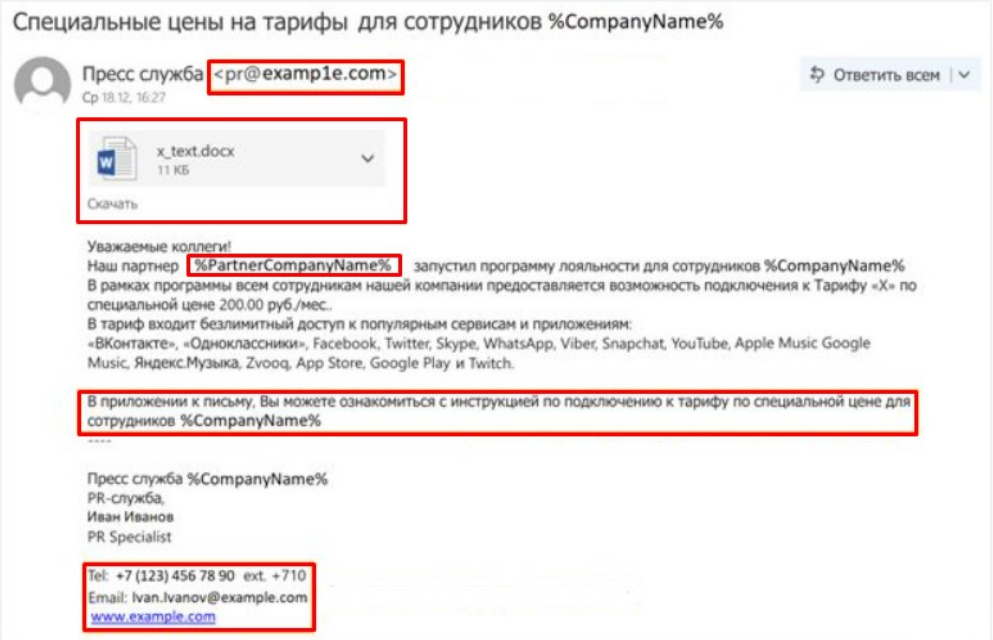


Рисунок 2. Мошенническое письмо от «коллег»

Из 88 сотрудников организации, получивших данное письмо, 26 человек (29,5% проверяемых лиц) скачали прикрепленный документ, тем самым подвергли компанию риску компрометации данных.

Поэтому, прежде чем открывать полученное письмо, переходить по ссылкам и скачивать вложенные файлы, необходимо обратить внимание на следующие признаки фишинга:

1. pr@examp1e.com – искаженное доменное имя. Злоумышленники часто используют омоглифы (омоглиф – графически одинаковые или похожие друг на друга знаки, имеющие разное значение). В данном случае «l» заменено на «1».

2. Документ x_text.docx. Название документа не отражает его содержания, и во вложении может быть безобидный на первый взгляд документ Microsoft Office, который при этом содержит вредоносные макросы (макрос – набор команд и инструкций, группируемых вместе в единую команду для автоматического выполнения задачи). Записанные злоумышленниками макросы запускают загрузку вредоносного программно-

го обеспечения на устройство пользователя. В ином случае в прикрепленном файле может находиться вирус, который шифрует все данные на компьютере и требует денежные средства за их дешифровку.

3. Текст, побуждающий к выполнению действий. Злоумышленники используют различные психологические методы, внушая жертвам чувство срочности, страха или необходимости выполнения перечисленных действий.

4. Контакты. Прежде чем устанавливать вложенные файлы или переходить по ссылкам, необходимо проверить, соответствует ли телефон, сайт и адрес реальным контактам организации, указанной как отправитель. Если есть возможность, следует перезвонить автору письма или обратиться к ИТ-специалисту организации.

Довольно часто злоумышленники для привлечения внимания пользователей отправляют письма с выигрышами в лотерею, выплатами в рамках благотворительной акции и иными способами обогащения. Доверчивым пользователям обещают приз за прохождение небольшого опроса или высокооплачиваемую работу, для которой не нужен опыт, а все что нужно сделать для получения – перейти по ссылке или ввести учетные данные банковского приложения (см. рис. 4).

После перехода по указанной ссылке компьютер заражается вредоносным программным обеспечении (далее – ВПО), которое крадет сохраненные пароли или повреждает файлы. Также возможны ситуации, когда при переходе на фишинговый сайт необходимо оплатить небольшую комиссию для получения денежных средств.

Рассмотрим основные признаки мошеннического письма, связанного с получением выплат и иных вознаграждений:

1. uni.edu – такой домен обычно ассоциируется с университетскими (uni – university, edu – education) электронными адресами. Получение письма о вознаграждении «от крупных спонсоров компании» выглядит подозрительно, так как университетский почтовый ящик не используется для этих целей.

2. wriggigi1159 – имя пользователя выглядит как случайно сгенерированное, что может быть признаком того, что адрес создан для совершения мошеннических действий.

3. «Переход к опросу» и «Отказаться от приза или передать его другому» – фальшивые ссылки, которые ведут на сайт, где необходимо оставить данные банковской карты для получения приза. Также при нажатии устанавливает сомнительный pdf-файл, который может содержать в себе ВПО. Если ссылка при наведении на URL – адрес курсора выглядит подозрительно, и ее не следует открытвать.

4. Отсутствие информации о человек или о компании. Письмо не содержит информации о представителях компании или их контактах, а также является безличным, так как не обращено к конкретному пользователю, а ко всем сразу.

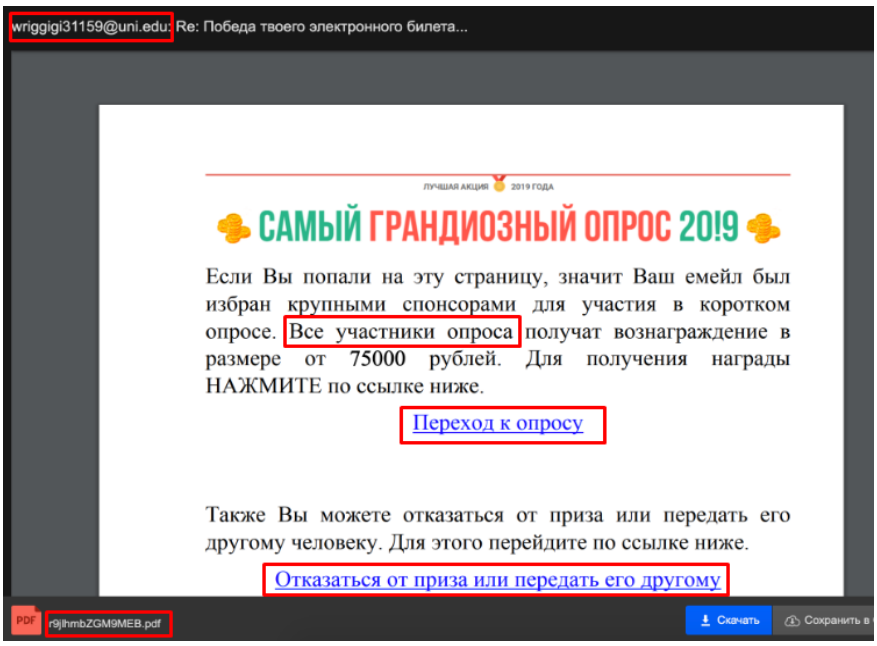


Рисунок 3. Мошенническое письмо с «гарантированным выигрышем»

Таким образом, чтобы не стать жертвой мошенников при использовании электронной почты, необходимо придерживаться следующих правил:

1. Проверять подлинность полученного письма, прежде чем отправлять информацию о себе или переходить по ссылкам.
2. Быть осторожным со «срочными» письмами, которые предлагают призы, быстрый заработок или содержат просьбы, не требующие отлагательств.
3. Использовать встроенные фильтры электронной почты для блокирования подозрительных входящих писем.

Рисунок 4. Алгоритм проверки электронных писем

Проведенное исследование показывает, что злоумышленники используют самые разнообразные подходы, чтобы обмануть ничего не подозревающих пользователей. Также следует отметить, что текущие социально-политические события в стране и мире мгновенно попадают в тематику фишинговых писем (COVID, финансовый кризис, санкции, специальная военная операция и т.д.). Такая стремительная адаптация злоумышленников требует реакции и как со стороны правоохранительных органов так и повышенной бдительности от граждан.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. – 2017. – № 20.
2. Дашян М.С. Право информационных магистралей: вопросы правового регулирования в сфере Интернет. – Москва: Волтерс Клувер, 2017.
3. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. – 2008. – № 2.
4. Нил П. Выигрывайте без боя: эффективная защита от социальной инженерии, фишинга и других видов кибератак. 2018.
5. Основы кибербезопасности в деятельности сотрудников правоохранительных органов / А.Н. Прокопенко [и др.]. – Белгород, 2023. – 153 с.
6. Граховский В., Трощенков Д. Техники социальной инженерии в информационной безопасности. – Москва: БХВ-Петербург, 2015.
7. Ланевский В.М. Технологии противодействия социальной инженерии. – Москва: КомКнига, 2016.
8. Бондарев А.М. Фишинг: методы и технологии защиты. – Санкт-Петербург: БХВ-Петербург, 2017.
9. Симонов В.Ф. Эффективность борьбы с социальной инженерией и фишингом в информационной безопасности. – Москва: Горячая линия – Телеком, 2019.

ОСОБЕННОСТИ СБОРА И АНАЛИЗА ИНФОРМАЦИИ, ПОЛУЧЕННОЙ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

Борисенко А.В.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: технологии OSINT возникли в связи с необходимостью собирать актуальную и общедоступную информацию. С помощью OSINT можно найти конкретную информацию, которая содержит определенные знания или дает неоспоримые преимущества. С момента создания данной технологии был проведен ряд исследований, в ходе которых предложены и разработаны новые способы использования OSINT. В дополнение к OSINT еще одной областью исследований, ставшей мировым трендом, становится сфера искусственного интеллекта.

Ключевые слова: кибербезопасность, искусственный интеллект, разведка по открытым источникам, OSINT, информационная безопасность.

FEATURES OF COLLECTING AND ANALYZING INFORMATION OBTAINED FROM OPEN SOURCES

Borisenko A.V.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: OSINT technologies arose due to the need to collect relevant and publicly available information. With OSINT, you can find specific information that has certain knowledge or provides undeniable advantages. Since the creation of this technology, a number of studies have been conducted, during which new ways of using OSINT have been proposed and developed. In addition to OSINT, another area of research that has become a global trend is the field of artificial intelligence.

Keywords: cybersecurity, artificial intelligence, open source intelligence, OSINT, information security.

Методы кибербезопасности меняются ежедневно и находятся в постоянной динамике в то же время появляются, новые вызовы и угрозы [1, 2]. Поддержание актуальности знаний является ключом к безопасности в Сети. Разведка с открытым исходным кодом (далее – OSINT) является важным инструментом, используемым для различных целей, таких как обеспечение безопасного Интернета, конкурентный анализ и поддержание кибербезопасности. В этих областях особенно востребована возможность получения общедоступной информации, например для лучшего понимания угрозы и создание системы защиты информационных систем от кибератак. OSINT расшифровывается как Open-

source intelligence – разведка по открытым источникам[1]. Это концепция, описывающая поиск, сбор, анализ и использование информации из открытых источников, включающая применяемые методы и инструменты.

Интернет и другие средства массовой информации все чаще используются для публикаций и обмена информацией. Простота доступа к Сети позволяет людям легче находить и публиковать информацию любого типа [3, 4]. Хотя публикация информации имеет значительные преимущества, такие как сбор информации для исследователей во многих областях деятельности человека, маркетинг и социальная психология, существенным недостатком становится проблема информационной безопасности, в частности сохранение конфиденциальности информации [5, 6], что создает необходимость организации комплексной системы защиты информации.

Для поиска и изучения этой информации в Интернете существуют инструменты, методы и подходы, которые позволяют выполнять реализацию мероприятий по открытым источникам. Эти действия могут проводиться в самых разных источниках: в социальных сетях, научных страницах, геолокациях и сайтах. Интеллектуальная система с открытым исходным кодом – это концепция, используемая для описания поиска и получения информации из общедоступных источников, а также применяемых методов и инструментов.

Объем информации, которую можно найти и собрать, довольно велик, а открытые источники, где эта информация встречается, крайне разнообразны. OSINT по-прежнему считается развивающейся областью, в том числе благодаря стремительному совершенствованию технологий искусственного интеллекта (далее – ИИ) [5, 6]. Область искусственного интеллекта разделена на направления. В качестве примера таких направлений можно рассмотреть обработку голоса, распознавание образов, робототехнику и машинное обучение. Все эти области ИИ могут быть применены в OSINT, которая представляет собой обширную и разнообразную информацию из нескольких открытых источников, а область искусственного интеллекта является общемировой тенденцией. Поэтому при рассмотрении вопроса организации OSINT необходимо опираться на исследования, направленные на изучения ИИ.

Эта задача в сочетании с большим объемом конфиденциальных данных и информации, доступной в Интернете, привела к необходимости создания рекомендаций при работе в сети Интернет, появления стандартов, инструментов и технологий по противодействию действий злоумышленников, использующих инструментарии OSINT, т.е. концепции, которые направлены на поиск, сбор, обработку, анализ и использование информации из открытых источников, доступ к которой на законных основаниях может получить любое физическое лицо или организация. OSINT находит, выбирает и извлекает эту информацию из открытых источников, а также анализирует найденную информацию для получения аналитических данных, в том числе и о возможностях ее использования.

[1] Официальный сайт компании «Лаборатория Касперского» [Электронный ресурс]. – URL: https://www.kaspersky.ru.

Поскольку OSINT – это быстрый и эффективный способ проведения углубленных проверок безопасности, рассматриваемая технология может использоваться и правоохранительными органами для поиска противоправного контента в сети Интернет. Основным сервисом, упрощающий процессы сбора и обработки информации, является OSINT framework (см. рис. 1).

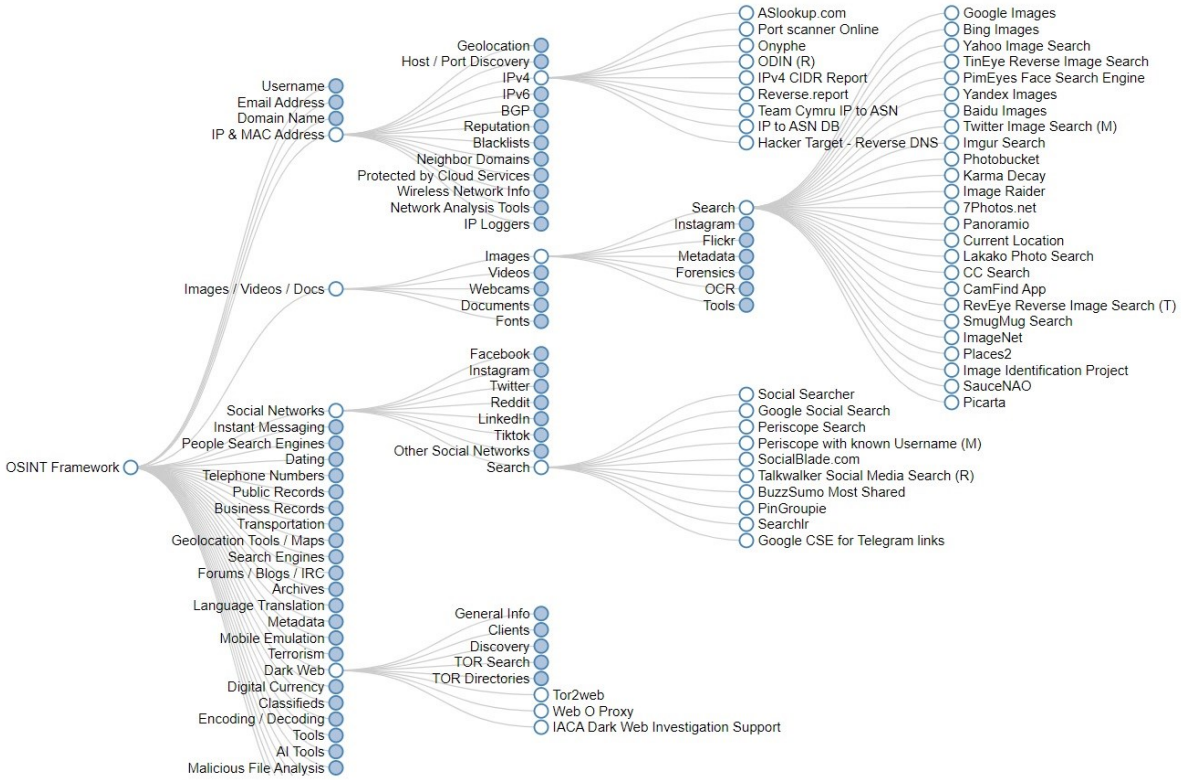


Рисунок 1. Интерфейс OSINT framework

Таким образом, для поиска информации могут применяться абсолютно разные инструментарии, а подробная их классификация позволяет уменьшить время ее поиска. Примером дружественного использования технологии OSINT является сканирование входящего трафика на предмет сомнительной корреспонденции и попыток проведения атак злоумышленниками посредством фишинга.

Основная цель OSINT Framework — предоставить данные и информацию, собранные OSINT, в хорошо структурированном виде, помогая пользователям принимать верные решения и улучшать меры безопасности, а также выявлять возможные угрозы и управлять рисками. Инструменты и методы кибербезопасности постоянно развиваются. Аналогичным образом структура разведки с открытым исходным кодом позволяет компаниям и пользователям быть на шаг впереди возможных рисков, используя объем информации, которая им доступна. OSINT можно использовать как один из современных методов обеспечения кибербезопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Польман Д.А. Кибербезопасность в цифровой экономике / Инновации молодежной науки: тезисы докладов Всероссийской научной конференции молодых ученых с международым участием, Санкт-Петербург, 24–28 апреля 2023 г. – Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2023. – С. 452–454.

2. Борисенко А.В. Человеческий фактор в системе кибербезопасности / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 10-й Всероссийской научно-практической конференции, Белгород, 19 мая 2023 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – С. 27–31.

3. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник. – Москва: РИОР: ИНФРА-М, 2022. – 202 с.

4. Сэрра Э. Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании / пер. с англ. – Москва: Альпина ПРО, 2022. – 189 с.

5. Джалилов Э.З., Карасев П.И. Кибербезопасность и искусственный интеллект / Кибербезопасность: технические и правовые аспекты защиты информации: сборник научных трудов I Национальной научно-практической конференции, Москва, 24–26 мая 2023 года. – Москва: МИРЭА – Российский технологический университет, 2023. – С. 172–175.

6. Ермолаев А.С., Великанов В.В. Роль и место искусственного интеллекта в сфере обеспечения кибербезопасности // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 12-2. – С. 71–75.

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Бубнов В.В.,
кандидат экономических наук, доцент
(Московский авиационный институт
(национальный исследовательский университет);
Дубинина Н.М.,
кандидат юридических наук, доцент;
Атаев Т.Т.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: статья посвящена перспективным направлениям внедрения нейросетей в правоохранительной деятельности, рассматриваются вопросы использования искусственного интеллекта в условиях цифровой трансформации правоохранительных органов.

Ключевые слова: нейросети, искусственный интеллект, правоохранительная деятельность, безопасность, практика.

SOME ASPECTS OF THE USE OF NEURAL NETWORKS IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Bubnov V.V.,
Candidate of Economics, Associate Professor
(Moscow Aviation Institute (National Research University) (MAI));
Dubinina N.M.,
Candidate of Law, Associate Professor;
Ataev T.T.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: the article is devoted to promising areas of implementation of neural networks in law enforcement, discusses the use of artificial intelligence in the context of digital transformation of law enforcement agencies.

Keywords: neural networks, artificial intelligence, law enforcement, security, practice.

В последние годы в компьютерных науках активно развивается особое направление – «искусственный интеллект», получившее широкую популярность благодаря своей способности самостоятельно обрабатывать и анализировать большие объемы данных, значительно облегчая информационно-аналитическую деятельность человека.

Искусственный интеллект через нейронные сети моделирует структуру и работу человеческого мозга и как компьютерная технология нацелен на решение творческих задач, присущих человеку. Нейронная сеть через математическую модель используется как разновидность машинного обучения. Развитие этого направления приобретает особую важность для правоохранительных органов в условиях широкого внедрения цифровых технологий.

Прежде всего это связано с большим документооборотом. Уголовно-процессуальные, оперативно-разыскные, административно-процессуальные, организационно-распорядительные и другие документы нуждаются в тщательной проверке и обработке. На сегодняшний день функции нейросетей включают в себя анализ текста на нахождение в нем ошибок. Внеся в систему не только правильное написание слов, но и образцы заполнения тех или иных документов, возможно сократить время на осуществление аналогичной однотипной работы человеком.

В настоящее время в России функционируют сервисы, которые способны осуществлять задачи такого рода. Компания Digital Design, используя методы семантического анализа и тональности текста, классификации и кластеризации документов, позволяет выявлять аномалии в проверяемых договорах, обрабатывать корреспонденцию посредством систем искусственного интеллекта, автопротоколировать ход собрания. Digital Design[1] показала себя с положительной стороны, являясь партнером различных российских университетов. Думается, что используемые технологии обработки информации могут представлять определенный интерес в деятельности правоохранительных органов.

Внедрение метода искусственного интеллекта, способного непрерывно реализовывать свой функционал, поможет модернизировать работу по учету сообщений о происшествиях и преступлениях. Так, на основе постоянного мониторинга формируемой базы данных по специальным ключевым словам нейросеть могла бы распознавать ту или иную разновидность правонарушения, обеспечивая сотрудников правоохранительных органов актуальной информацией.

Одной из популярных функций нейросетей является распознавание и классификация объектов. Это позволяет идентифицировать то или иное лицо либо же предмет, обращаясь к миллионам баз данных в режиме реального времени, что вносит весомый вклад в расследование многих противоправных деяний, а также обеспечивает безопасность охраняемых объектов.

NtechLab – российская компания, являющаяся прорывом в области внедрения нейросети в вопросе распознавания объектов, мировой лидер в аспекте видеоаналитики. Продукт компании FindFace Multi предлагает различные направления для использования своего функционала: контроль доступа по лицу, пресечение мошенничества, распознавание клиентов и др. NtechLab имеет опыт работы в области обеспечения безопасности. Так, видеоаналитика компании помогла осуществлять охрану общественного порядка при проведении

[1] Классификация документов: кластеризация и генерация ответов Digital Design [Электронный ресурс]. – URL: https://digdes.ru/nlab/intellektualnaya-obrabotka-tekstov (дата обращения: 11.05.2024).

чемпионата мира по футболу в 2018 году. Около пятисот привлеченных камер на территории метрополитена, стадионов и иных мест позволили добиться точности подсчета посетителей порядка 99,4%, идентифицировать и принять необходимые меры к задержанию около ста человек из разыскных баз [4; 5].

Среди основных целей национального развития России на период до 2030 года Указом Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития России до 2030 года» была упомянута «цифровая трансформация» [1]. В условиях цифровизации каждая из сфер жизни требует изменений, которые будут способствовать улучшению показателей. Опираясь на все вышесказанное, следует вывод, что внедрение искусственного интеллекта действительно необходимо для более качественной работе правоохранительных органов.

Говоря о функционале нейросетей, можно определить большой перечень возможностей, которыми обладает эта разновидность машинного обучения. Но в то же время следует отметить, что, хотя по своей сути нейросеть действительно значительно облегчает человеческий труд, вбирая в себя стандартизированную работу, человеческий разум с творческим мышлением и неординарным подходом она в настоящее время полноценно заменить не сможет.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // СПС «КонсультантПлюс».

2. Как мы уместили распознавание 7 типов документов в одну модель, и что из этого вышло [Электронный ресурс]. – URL: https://habr.com/ru/companies/sberbank/articles/714404/ (дата обращения: 11.05.2024).

3. Меняйло Д.В., Назаренко И.С., Шутова Е.Н. Современные информационно-аналитические системы обработки видеоинформации в деятельности правоохранительных органов России / Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел: сборник материалов Всероссийской научно-практической конференции, Ростов-на-Дону, 28 апреля 2023 года. – Ростов-на-Дону, 2023. – С. 73–78.

4. Распознавание лиц и силуэтов людей, автомобилей и номерных знаков NtechLab [Электронный ресурс]. – UR: https://ntechlab.ru/ (дата обращения: 11.05.2024).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ ОБРАЗОВАНИЯ В СИСТЕМЕ МВД РОССИИ

Гизатуллин М.Г.,
кандидат технических наук, доцент
(Уральский юридический институт МВД России; АО «Уралтрансмаш»)

Аннотация: рассматривая стратегию развития Российской Федерации, необходимо отметить, что образование становится ключевым направлением (фактором) развития Российской Федерации, своего рода вектором совершенствование потенциала страны в различных областях (сферах) деятельности. Качество образования выступает как критерий, который позволяет гражданам Российской Федерации взглянуть на то, как организуется и реализуется образование (образовательный процесс) в Российской Федерации как с позиции участников образовательного процесса, так и с точки зрения различного рода регуляторов данной области (сферы) деятельности. Образование представляет собой непрерывный процесс становления личности (индивида) в рамках освоения той или иной области (сферы) деятельности при получении (формировании) знаний, умений, навыков и/или опыта деятельности. Образовательная деятельность в образовательных организациях высшего образования системы МВД России, территориальных органах (в том числе в центрах профессиональной подготовки) является достаточно важным и приоритетным направлением МВД России в области становления высококвалифицированных кадров (сотрудников органов внутренних дел Российской Федерации), профессионалов своего дела. Вопросы в области образования (в том числе цифровой грамотности) для образовательных организаций высшего образования системы МВД России, территориальных органов МВД России являются актуальными и приоритетными как для самих субъектов и объектов данных организаций и органов, так и для министерства в целом. В рамках проводимого исследования автором рассматриваются некоторые аспекты (общие и частные) направления образовательного процесса в образовательных организациях высшего образования системы МВД России, территориальных органах МВД России.

Ключевые слова: органы внутренних дел Российской Федерации, образование, ннформационные технологии, образовательный процесс.

INFORMATION TECHNOLOGIES IN THE FIELD OF EDUCATION IN THE SYSTEM OF THE MINISTRY OF THE INTERIOR OF RUSSIA

Gizatullin M.G.,
Candidate of Technical Sciences, Associate Professor
(Ural Law Institute of the Ministry of the Interior of Russia; JSC «Uraltransmash»)

Abstract: considering the development strategy of the Russian Federation, it should be noted that education is becoming a key direction (factor) in the development

of the Russian Federation, a kind of vector for the development of the country's potential in various fields (spheres) of activity. The quality of education acts as a criterion that allows citizens of the Russian Federation to look at how education (educational process) is organized and implemented in the Russian Federation from the perspective of both participants in the educational process and various regulators of this field (sphere) of activity. Education is a continuous process of formation of a personality (individual) within the framework of mastering a particular area (sphere) of activity from the position of obtaining (forming) knowledge, skills, and/or experience of activity. Educational activities in educational institutions of higher education of the Ministry of the Interior of Russia, territorial bodies of the Ministry of the Interior of Russia (including in vocational training centers) is quite an important and priority area of the Ministry of the Interior of Russia in the field of formation of highly qualified personnel (employees of the interior affairs bodies of the Russian Federation), a kind of professionals “in their field”. Issues in the field of education (including “digital literacy”) for educational institutions of higher education of the Ministry of the Interior of Russia, territorial bodies of the Ministry of the Interior of Russia are relevant and priority both for the subjects and objects of these organizations and bodies, and for the Ministry of the Interior of Russia as a whole. As part of the research, the author examines some aspects (general and private) of the educational process in educational institutions of higher education of the Ministry of the Interior of Russia, territorial bodies of the Ministry of the Interior of Russia.

Keywords: the interior affairs bodies of the Russian Federation, education, information technology, the educational process.

Образовательная деятельность в образовательных организациях высшего образования системы МВД России (далее – ОО) и территориальных органах МВД России, в том числе в центрах профессиональной подготовки (далее – ТО), организуется и реализуется в соответствии с рядом нормативных правовых актов (далее – НПА) в области образования, а также в соответствии с локальными нормативными актами (далее – ЛНА) ОО и ТО.

Основным НПА в области образования для ОО и ТО является федеральный закон Российской Федерации «Об образовании в Российской Федерации» [1]. В соответствии с данным НПА и другими НПА в области образования ОО и ТО осуществляют разработку ЛНА в области образования.

Для ОО и ТО можно выделить ряд основополагающих ЛНА в области образования, а именно: основные образовательные программы высшего и среднего профессионального образования по определенным специальностям и/или направлениям подготовки; основные программы профессионального обучения; дополнительные профессиональные программы (программы повышения квалификации) (далее – программы) и т.д..

Обучающиеся (курсанты, слушатели) как ОО, так и ТО по данным программам в том или ином объеме изучают учебные дисциплины (модули), которые раскрывают общие и частные вопросы в области информационных технологий.

В рамках изучения обучающимися учебных дисциплин (модулей) данной предметной области, необходимо отметить, что у обучающихся формируются общие, общекультурные, профессиональные и профессионально-служебные компетенции, формируется такое направление, как «цифровая грамотность».

Данные учебные дисциплины (модули) с позиции учебно-методического обеспечения чаще всего представлены следующими компонентами: программы; тексты лекций; методические разработки для проведения семинаров; методические разработки для проведения практических занятий; методические разработки для проведения лабораторных работ; методические рекомендации по организации самостоятельной работы и т.д.

Такие компоненты, как программы, как правило, разрабатываются:

– на основе примерных программ, разработанных ОО;

– ОО, реализующими данные программы обучения на местах.

Наименование тем учебных дисциплин (модулей) и их количество, объем учебных часов в различных ОО и ТО может варьироваться в соответствии со спецификой и местом дислокации ОО и ТО.

Рассматривая ОО и ТО с позиции тех или иных категорий лиц (работников и сотрудников), можно отметить следующее:

1. Вольнонаемные работники, поступающие на работу в ОО и ТО (на первоначальном этапе своей деятельности и в последующем) сталкиваются со следующими трудностями (проблемами), связанными со следующим видами работ:

– с операционной системой Microsoft Windows;

– с текстовыми и табличными редакторами (программные продукты, работающие под управлением операционной системы Microsoft Windows: Microsoft Office, Open Office, Libre Office, Мой офис, Р7-Office);

– с операционной системой Astra Linux;

– с текстовыми и табличными редакторами (программный продукт, работающий под управлением операционной системы Astra Linux: Libre Office);

– с ИСОД МВД России;

– реализация выполнения требований Инструкции по делопроизводству в органах внутренних дел Российской Федерации (далее – ОВД РФ) при работе с текстовыми и табличными редакторами [2].

У вольнонаемных работников ОО и ТО данные трудности (проблемы) возникают по следующим причичинам:

– слабые знания и недостаточные умения и навыки работы с операционной системой Microsoft Windows;

– слабые знания и недостаточные умения и навыки работы с текстовыми и табличными редакторами, работающими под управлением операционной системы Microsoft Windows;

– отсутствие знаний, умений и навыков работы с операционной системой Astra Linux;

– отсутствие знаний, умений и навыков работы с текстовыми и табличными редакторами, работающими под управлением операционной системы Astra Linux;

– отсутствие знаний, умений и навыков работы в области формирования электронных документов в МВД России;

– отсутствие знаний, умений и навыков работы с ИСОД МВД России.

2. Сотрудники ОВД РФ ОО и ТО, вновь принимаемые на службу на соответствующие должности и с соответствующим уровнем образования (до и после прохождения обучения в центрах профессиональной подготовки ТО), на первоначальном этапе прохождения службы и в последующем сталкиваются с теми же трудностями (проблемами), что и вольнонаемные работники при трудоустройстве в ОО и ТО. Необходимо отметить, что в центрах профессиональной подготовки ТО сотрудники ОВД РФ изучают некоторые общие и частные вопросы в области информационных технологий по соответствующим циклам (модулям).

3. Сотрудники ОВД РФ ОО и ТО, проходящие службу на протяжении нескольких лет, также сталкиваются с аналогичными трудностями (проблемами).

Переход ОО и ТО с зарубежной операционной системы Microsoft Windows на отечественную операционную систему Astra Linux в рамках процесса импортозамещения стал своего рода «проблемой» для ряда как вольнонаемных работников, так и сотрудников ОВД РФ (в большей степени даже не с позиции работы с операционной системой Astra Linux, а с позиции работы с предустановленным офисным пакетом Libre Office).

Чем же выражена данная «проблема»?

Во-первых, данные категории лиц «привыкли» к интерфейсу операционной системы Microsoft Windows и офисному пакету Microsoft Office.

Переход на отечественную операционную систему Astra Linux, и в особенности организация принципов работы с зарубежным офисным пакетом Libre Office, вызвали своего рода «отторжение» у данных категорий лиц к обоим программным продуктам. Реализация новых продуктов сопровождается долгой адаптацией данных категорий лиц.

Во-вторых, иной алгоритм подключения внешних носителей информации к устройству, работающему под управлением операционной системы Astra Linux, а также иной алгоритм установки программного обеспечения также вызвали непринятие нового продукта.

В-третьих, особенности работы с офисным пакетом Libre Office по сравнении с офисным пакетом Microsoft Office для данных категорий лиц являются существенными. Рассматривая офисный пакет Libre Office как альтернативу офисному пакету Microsoft Office, необходимо отметить, что практически все задачи, реализуемые в офисном пакете Microsoft Office можно выполнить и в офисном пакете Libre Office. Однако это будет требовать от данных категорий лиц дополнительного изучения материала (справки) по работе с новым продуктом, а также большего количества операций, которые должен совершить тот или иной пользователь.

В-четвертых, ввиду отчасти некорректной работы ряда компонентов офисного пакета Libre Office и определенного рода происходящих сбоев (в некоторых случаях) при работе с продуктом это также приводит к и неохотной работе данных категорий лиц с продуктом.

С учетом вышесказанного необходимо отметить, что ОО и ТО следует прорабатывать данного рода проблемные вопросы в приоритетном порядке.

При этом достаточно важным направлением в области образовательного процесса является рассмотрение следующих позиций.

1. При трудоустройстве вольнонаемных работников в ОО и ТО необходимо организовывать с данными категориями лиц работу:

– по формированию знаний, умений и навыков по работе с офисным пакетом Libre Office под управлением операционной системы Astra Linux;

– по формированию знаний, умений и навыков в области составления электронных документов в соответствии с НПА [2];

– по формированию знаний, умений и навыков по работе с сервисами ИСОД МВД России.

Если речь идет о вольнонаемных работниках ОО, то необходимо осуществлять данного рода работу с данными категориями лиц как в самих ОО, так и направлять данные категории лиц на обучение в и иные учебные центры в области образования.

Если речь идет о вольнонаемных работниках ТО, то необходимо осуществлять такую работу с данными категориями лиц в самих ТО или направлять данные категории лиц на обучение в ОО и иные учебные центры в области образования.

2. При принятии на службу сотрудников ОВД РФ в ОО и ТО (как до момента их направления в центры профессиональной подготовки, так и после их возвращения их них) необходимо организовывать с данными категориями лиц работу такую же, как и с вольнонаемными работниками ОО и ТО.

3. В процессе прохождения службы сотрудников ОВД РФ в ОО и ТО, необходимо организовывать с данными категориями лиц работу, аналогичной работе с вольнонаемными работниками ОО и ТО.

4. В ОО и центрах профессиональной подготовки ТО по учебным дисциплинам (модулям) в области информационных технологий необходимо:

– увеличить количество тем и учебных часов с реализацией занятий в учебных компьютерных классах с офисным пакетом Libre Office под управлением операционной системы Astra Linux (если это еще не реализовано);

– увеличить количество учебных часов по тематике, связанной с ИСОД МВД России с реализацией занятий на полигонах ИСОД МВД России и в учебных компьютерных классах с программным продуктом, имитирующим организацию и принципы работы ИСОД МВД России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СПС «КонсультантПлюс».

2. Приказ МВД России от 20.06.2012 № 615 «Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

ПОСТРОЕНИЕ СПУТНИКОВЫХ НАВИГАЦИОННО-МОНИТОРИНГОВЫХ СИСТЕМ В ИНТЕРЕСАХ МВД РОССИИ С ИСПОЛЬЗОВАНИЕМ ПЕРСОНАЛЬНЫХ ВИДЕОРЕГИСТРАТОРОВ

Гилев И.В.;
Попов И.Е.,
кандидат технических наук
(Воронежский институт МВД России)

Аннотация: в статье приводится описание роли навигационно-мониторинговых систем в органах внутренних дел при охране общественного порядка и обеспечении общественной безопасности. Обозначена проблема оснащения мобильной навигационной аппаратурой потребителей пеших нарядов полиции. Предложено решение, основанное на использовании персональных видеорегистраторов для определения местоположения мобильных нарядов, а также схема передачи данных и интеграции указанных средств в передачи геоданных и интеграции в навигационно-мониторинговую систему МВД России.

Ключевые слова: навигационно-мониторинговые системы, геопозиционирование, видеорегистраторы, мобильные наряды полиции органы внутренних дел.

CONSTRUCTION OF SATELLITE COMMUNICATION LINES IN THE INTERESTS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIATHE PROTECTION OF PUBLIC ORDER

Gilev I.V.;
Popov I.E.,
Candidate of Technical Sciences
(Voronezh Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article describes the role of navigation and monitoring systems in internal affairs agencies in maintaining public order and ensuring public safety. The problem of equipping consumers of foot police units with mobile navigation equipment is outlined. A solution is proposed based on the use of personal video recorders to determine the location of mobile units, as well as a data transmission scheme and integration of these tools into the transmission of geodata and integration into the navigation and monitoring system of the Ministry of Internal Affairs of Russia.

Keywords: navigation and monitoring systems, geo-positioning, video recorders, mobile police squads, internal affairs agencies.

В настоящее время с помощью систем геопозиционирования и мониторинга подвижных объектов в МВД России решаются задачи по управлению силами и средствами органов внутренних дел, задействованными в охране общественного порядка (ППСП, ДПС и участковые уполномоченные полиции),

осуществляется раскрытие преступлений с использованием данных спутниковых противоугонных систем, производится контроль за состоянием служебного транспорта и др. Следует отметить, что интеграция навигационно-мониторинговых систем в деятельность органов внутренних дел происходит за счет внедрения и использования инфраструктуры «ЭРА-ГЛОНАСС» [1;2], которая реализована в виде отдельного сервиса в Единой системе информационно-аналитического обеспечения деятельности МВД России.

Навигационная аппаратура потребителей чаще всего размещается в патрульных автомобилях сотрудников ДПС и ППСП, однако оснащению персональной мобильной навигационной аппаратуры потребителей пеших нарядов полиции в настоящее время не уделено должного внимания.

В связи с этим актуальной задачей является определение местоположения мобильных нарядов, трансляция потокового видео с места происшествия и документирование правонарушений [3]. В качестве решения вышеуказанных задач могут использоваться персональные видеорегистраторы, в частности «Дозор-78», в который встроен модуль «ГЛОНАСС/GPS» для определения местоположения мобильных нарядов полиции. В качестве каналов передачи потокового видео с персональных регистраторов «Дозор-78» могут использоваться сети мобильной связи с обязательным шифрованием передаваемых данных или промышленные точки доступа Wi-Fi, которыми оборудован подвижный узел связи, используемый в подразделениях МВД России при проведении массовых мероприятий или ликвидации последствий чрезвычайных ситуации. Схема интеграции персональных регистраторов в навигационно-мониторинговую систему МВД России приведена на рисунке 1.

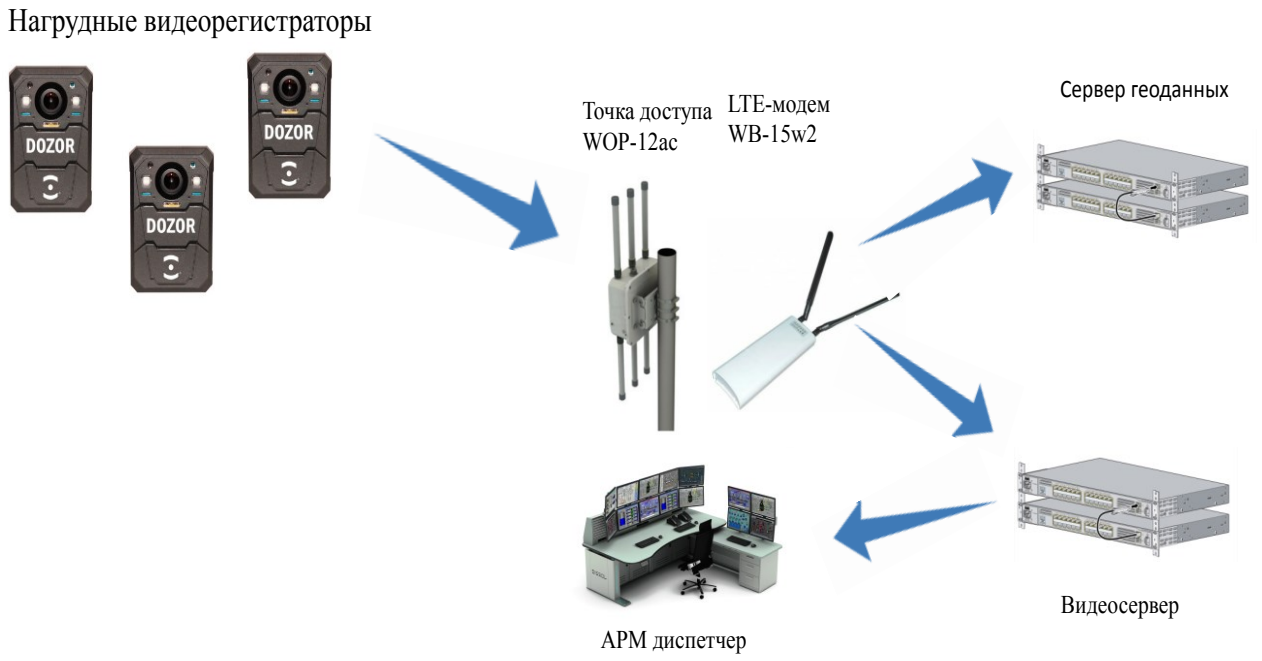


Рисунок 1. Схема интеграции персональных регистраторов
в навигационно-мониторинговую систему МВД России

Реализация указанных возможностей оборудования и предложенной схемы позволит значительно улучшить деятельность органов внутренних дел за счет сокращения времени реагирования на изменение оперативной обстановки на временных постах и маршрутах патрулирования, а также повысить эффективность управления силами и средствами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 17 мая 2007 г. № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации» // СПС «КонсультантПлюс».

2. Приказ МВД России от 31 декабря 2008 г. № 1197 «Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России» [Электронный ресурс] // СТРАС «Юрист».

3. Технологии спутникового мониторинга подвижных объектов в служебной деятельности подразделений органов внутренних дел: методические рекомендации. – 2-е изд., перераб. – Калуга: Калужский филиал ФКУ НПО «СТиС» МВД России, 2022. – 84 с.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Дубинина Н.М.,
кандидат юридических наук, доцент;
Пупкова М.С.
(Московский университет МВД России имени В.Я. Кикотя);
Бубнов В.В.,
кандидат экономических наук, доцент
(Московский авиационный институт
(национальный исследовательский университет)

Аннотация: статья посвящена обсуждению возможностей и перспектив применения искусственного интеллекта в правоохранительной деятельности органов внутренних дел.

Ключевые слова: искусственный интеллект, органы внутренних дел, оперативно-разыскная сфера, распознавание образов, информация.

THE USE OF ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF INTERNAL AFFAIRS AGENCIES

Dubinina N.M.,
Candidate of Law, Associate Professor;
Pupkova M.S.,
(Kikot Moscow University of the Ministry of the Interior of Russia);
Bubnov V.V.,
Candidate of Sciences in Economics, Associate Professor
(Moscow Aviation Institute (National Research University)

Abstract: the article is devoted to the discussion of the possibilities and prospects of using artificial intelligence in law enforcement activities of internal affairs bodies.

Keywords: artificial intelligence, internal affairs agencies, operational investigative sphere, pattern recognition, information.

В настоящей статье под термином «искусственный интеллект» (далее – ИИ) понимается функционирование любых искусственных систем, максимально имитирующих деятельность человеческого мозга по выработке и реализации разнообразных решений. Характерная черта и особенность таких систем, использующих технологии ИИ, заключается в компьютерной обработке больших массивов оцифрованных, структурированных и формализованных данных. Это позволяет определить ИИ как компьютерную технологию.

При этом в системах с ИИ в зависимости от постановки конкретных задач могут быть реализованы разнообразные технологии, такие как нейросети, машинное обучение, логическое программирование, генетическое программирование, теория игр и др. Например, системы, реализованные на нейросетях, с помощью специальных математических моделей могут решать следующие задачи: а) проведение математических вычислений; б) определение объектов или явлений по изображениям или по звуковым файлам; в) разработку и принятие решений на основе опыта.

Искусственный интеллект сегодня активно развивается, расширяется практика его применения в разных сферах человеческой деятельности. Это обусловлено тем, что ИИ автоматизирует многие действия человека, в том числе и рутинного характера, позволяет быстро и оперативно осуществлять множество операций для достижения разнообразных целей.

Обсуждение проблем широкого и эффективного внедрения ИИ, на наш взгляд, является актуальным и важным для любой сферы деятельности, поскольку его использование И перспективно и технологично [1, с. 72]. Вопрос будущего заключается в том, как сильно разовьются технологии ИИ и насколько они станут совершенными.

Вместе с тем уже сегодня технологии искусственного интеллекта активно применяются в самых разных сферах, в том числе в деятельности органов внутренних дел. В рамках осуществляемого в МВД России планомерного перехода от устаревших технологий к современным цифровым решениям технологии искусственного интеллекта рассматриваются в качестве одного из приоритетных направлений цифровой трансформации ведомства.

Применение ИИ позволяет облегчить и качественно улучшить деятельность сотрудников органов внутренних дел по сбору и анализу больших объемов данных, необходимых для выполнения разнообразных оперативно-служебных задач. При этом на содержательном уровне могут решаться важные формализованные задачи распознавания и классификации объектов и процессов различной природы, например прогнозирования развития социально-экономической, политической и криминогенной обстановки в регионе, для предотвращения, раскрытия преступлений и т.д.

Говоря о сложности обработки больших массивов данных, использующихся в практической деятельности органов внутренних дел, следует заметить, что в целом первичная информация не имеет четкой структуризации и системности, поэтому ее анализ, обработка и систематизация требует использования специальных математических моделей и больших временных затрат [2, с. 56]. ИИ способен анализировать такие данные, структурировать их, выделять определенные свойства и особенности, что с успехом используется, например, в задачах прогнозирования преступлений, выявления подозрительных действий и т.п.

Сегодня можно обучить ИИ, реализованный с использованием технологии нейросетей, распознанию объектов и образов благодаря применению дискриминантного анализа и кластеризации. Например, система FINDFACE находит конкретного человека в толпе, среди огромной массы людей, идентифицирует его по заранее заданным параметрам, отслеживает перемещения определенных фигур, дифференцирует силуэты. В 2018 г., когда в России проводился чемпионат мира по футболу, с помощью системы FINDFACE разыскали и задержали почти сто правонарушителей непосредственно во время проведения футбольных матчей. В 2018 г. система FINDFACE была интегрирована в систему видеонаблюдения Москвы и Тюмени[1].

Такие системы, как FINDFACE, могут быть с успехом применены и более широк: для обнаружения и задержания правонарушителей, для контроля граждан, недавно освободившихся из мест заключения, для обеспечения безопасности на различных предприятиях. Системы обнаружения, оснащенные функциями ИИ, могут выявить конкретных людей, транспортные средства и другие объекты, фигурирующие, например, в уголовных делах. Подобные системы, использующие технологии ИИ, способны улучшить деятельность органов внутренних дел по самым различным направлениям: в оперативно-разыскной сфере, в профилактике и прогнозировании преступлений, в работе с докумен-

[1] МВД привлечет нейросети к поиску правонарушителей [Электронный ресурс]. – URL: https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei (дата обращения: 14.05.2024).

тами и обработке заявлений, поступающих от граждан – а также могут быть использованы в процессе обучения сотрудников правоохранительных органов.

В перспективе следует ожидать расширение практики применения ИИ в деятельности органов внутренних дел. В МВД России проводятся научно-исследовательские работы по подготовке датасетов для обучения и тестирования нейросетевых моделей, разрабатываются системы на базе ИИ, с помощью которых можно будет качественно и оперативно определять подделку видеоизображений, прогнозировать возникновение и развитие особенностей чрезвычайных ситуаций и моделировать варианты эффективного реагирования на них. Для реализации этих планов в МВД России подразделениях создаются специальные отделы для моделирования и управления данными [4].

В разработке информационных систем с искусственным интеллектом приходится учитывать ряд сложностей, связанных с решением вопросов методологического и нормативно-правового обеспечения, создания алгоритмов обработки информации, программно-аппаратного обеспечения.

В заключение отметим, что развиваемые и внедряемые в системе МВД России технологии искусственного интеллекта являются одним из определяющих факторов проводимой цифровой трансформации. Их использование имеет большие перспективы. Практика показывает, что уже сейчас внедрение ИИ способно повысить эффективность деятельности сотрудников органов внутренних дел в решении ими государственных задач в сфере борьбы с преступностью и обеспечения безопасности граждан.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гелиг А.Х., Матвеев А.С. Введение в математическую теорию обучаемых распознающих систем и нейронных сетей: учебное пособие. – Москва: СПбГУ, 2014. – 225 с.

2. Искусственный интеллект выходит на борьбу с преступностью в России. Правонарушителей будут искать хитрые нейросети [Электронный ресурс]. – URL: https://corp.cnews.ru/news/top/2024-01-11_iskusstvennyj_intellekt (дата обращения: 14.05.2024).

3. Николенко С.Т. Глубокое обучение. Погружение в мир нейронных сетей: руководство. – Москва: АСТ, 2023. – 328 с.

4. Меняйло Д.В., Барсова Е.Р. Применение информационных технологий в сфере противодействия коррупции / Информационные технологии в деятельности органов внутренних дел: сборник научных статей Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2023. – С. 222–226.

БИБЛИОТЕКА КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПОЛЬЗОВАТЕЛЯ

Дунаев Р.А.,
кандидат философских наук, доцент
(Белгородский государственный институт искусств и культуры)

Аннотация: современная библиотека – активный участник происходящих трансформаций – выступает сегодня в различных качествах и как социальное пространство, и как информационный центр, при этом являясь неотъемлемой частью культуры, предоставляя доступ к накопленному наследию. Библиотеки используют информационно-коммуникационные технологии, становясь элементом информационного пространства любого пользователя, поддерживая его информационные, социально-культурные потребности. В статье отмечается, что в информационном пространстве пользователя библиотека должна выступать как ключевой элемент, позволяя получать доступ к актуальной и достоверной информации.

Ключевые слова: библиотека, роль библиотеки, информационное пространство, информация, сеть.

LIBRARY AS A KEY ELEMENT OF THE USER'S INFORMATION SPACE

Dunaev R.A.,
Candidate of Philosophical Sciences, Associate Professor
(Belgorod State Institute of Arts and Culture)

Abstract: the modern library is an active participant in the ongoing transformations, acting today in various capacities both as a social space and as an information center. At the same time, it is an integral part of culture, providing access to the accumulated heritage. Libraries use information and communication technologies, becoming part of the information space of any user, supporting his information, socio-cultural needs.

Keywords: library, the role of the library, information space, information, network.

Сегодня сложно представить масштабы трансформации мира в связи с развитием современных информационных технологий, когда Интернет стал неотъемлемой частью нашей жизни, позволяя получать доступ к огромному количеству информации, покупать товары и услуги, общаться между собой, работать и учится дистанционно. Информация пронизывает все социальное пространство, влияет на общество, институты и человека. Сам термин «информационное пространство» [7] имеет, скорее, техническое наполнение и не отвечает на вопросы о возможностях и реальном использовании информации, также недооценена роль субъектов коммуникации, находящихся в данном простран-

стве. Современное информационное пространство (киберпространство) является огромным и сложным миром, в котором существует множество данных, информации и взаимосвязей между ними. По данным наблюдений statista.com, за 2023 год 66,04% населения земного шара регулярно пользуется Интернетом, более половины людей имеют подключение к интернет-сервисам. Соответственно, для того чтобы успешно учиться и работать, необходимо иметь минимальные знания в области информационного поиска, оценки контента и понимания основных рисков. Библиотека при этом не всегда рассматривается источником информации, обладая существенными базами данных электронных коллекций.

В отечественных работах отмечается новая роль информационного пространства и значительное влияние на различные сферы жизни человека [5; 6]. В 2010 году тогда старший научный сотрудник лаборатории компьютерных наук и искусственного интеллекта (МТИ) Дэвид Кларк в одной из своих работ [8] предположил, что нарождающееся киберпространство является «новым социальным пространством», которое влияет на жизнь и общество в целом. Киберпространство не является просто «технологическим инструментом», но также имеет социальные, политические и экономические компоненты и должно рассматриваться как новый вид общественного пространства, где люди могут взаимодействовать, обмениваться информацией и создавать новые формы социальной организации, также важна безопасность, которая должна быть встроена в саму архитектуру, чтобы защитить пользователей от угроз.

При этом стоит отметить уменьшение роли традиционных библиотек как основных источников информации, дальнейшее успешное развитие которых требует ряда изменений [4]. Конечно, библиотека в информационном обеспечении сотрудников организации/фирмы играет определенную роль, предоставляя доступ к литературе для решения различных задач, в том числе для проведения исследований. Сотрудники библиотеки могут осуществлять подбор истокников проводить разнообразные мероприятия по информационной грамотности, выступать центром обмена знаниями – центрами реальных встреч и живой коммуникаций. Но технологизация и формирование поведения современного пользователя позволяет ему при помощи гаджета и поисковых систем использовать Сеть как источник информации, не посещая традиционную библиотеку. Пользователь при помощи технологий может получить практически любую (насколько достоверную?) информацию почти мгновенно.

Кроме того, киберпространство позволяет перенести многие виды деятельности в онлайн-режим, что сокращает временные и материальные затраты. Однако все это имеет и свои недостатки: утечка информации, взлом систем безопасности и других преступлений. Помимо этого, киберпространство также может стать местом распространения дезинформации, разнообразного негативного и противозаконного контента. Для обеспечения безопасности при работе в Сети необходимо реализовывать определенные практики с учетом некоторых базовых правил, рассмотрение которых не предусмотрено рамками нашей работы.

Информационное пространство имеет сложную структуру, но тесно связано с социальным аспектом [2]. Также необходимо отметить, что новые информационные технологии дали возможность создания виртуальной «действительности», в которой находится пользователь, и она становится приближенной к реальной среде. Формируется личное виртуальное пространство, складываются определенные модели пользовательского поведения, способы поиска информации – и библиотека (в полном понимании как пространство) не всегда выступает ключевым элементом информационного пространства. Конечно, легче использовать бесконечную информационную ленту из устройства, которое всегда под рукой. Смеем предположить, что в складывающейся ситуации, когда наблюдается бурный рост развития технологий, роль библиотеки с учетом необходимых изменений должна оставаться ключевой в информационном пространстве любого пользователя и тому есть объяснения. Отметим тезисно некоторые из них.

Библиотека выступает хранилищем знаний, предоставляя возможность доступа к обширным и разнообразным ресурсам – печатным и электронным. Все эти источники систематизированы, размещены в библиотечных каталогаг по отраслям знаний в соответствии с определенной системой классификации. Библиотека обладает физическими коллекциями, часть из которых не оцифрована и представляет исследовательский интерес, что важно в поддержке научных исследований и необходимости получения углубленного обучения и непрерывного образования.

Современная библиотека представляет собой информационный центр, специалисты которого предоставляют в том числе услуги справочного обслуживания. Оказывается всесторонняя помощь и поддержка пользователей. Библиотекари помогают в поиске нужной информации, осуществляют подбор литературы по теме, организовывают разнообразные обучающие мероприятия: обучение навыкам информационной грамотности и цифровой компетентности; организация лекций и встреч для обмена опытом и знаниями и проч. Сами сотрудники библиотеки постоянно делятся опытом между собой, участвуют в конференциях, тренингах и семинарах, что способствует коллективному обучению и развитию.

Библиотека является социальным пространством, в котором проводятся тематические встречи с различными людьми,а также используется для обучения, общения и отдыха. Активно участвует в поддержке социальных инициатив, вовлекает различные возрастные категории граждан в досуговую деятельность.

Библиотека является полноправным участником и информационного пространства. Постоянно проводится работа по оцифровке фондов, расширяется цифровая коллекция и ассортимент предоставляемых услуг. Ежедневно ведется работа по интеграции библиотеки с другими цифровыми платформами, всевозможными базами данных.

Библиотеки вузов уже выступают ведущим звеном в информационном образовательном пространстве, выполняя своего рода интегративную функцию. Понятно, что есть ряд вопросов, которые мы поднимали и ранее [1, с. 110–118], на предмет того каким образом популяризовать библиотечный ресурс среди молодежи и формировать понимание библиотеки прежде всего как культурного

института в связке поколений. Тем более что в деле сохранения ценностей библиотека обладает всеми результатами, включая и борьбу с дезинформацией, и разумное использование «цифры» при сохранении традиционных форм доступа.

Таким образом, современная библиотека играет не только важную роль в обеспечении доступа к достоверной информации и знаниям, но и является неотъемлемым элементом информационного пространства любого пользователя, поддерживая его информационные, социально-культурные потребности. Безусловно, библиотека должна адаптироваться к меняющемуся информационному ландшафту, оставаясь современной, актуальной и доступной для пользователя в любом удобном ему коммуникационном канале.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бидоленко Л.А., Дунаев Р.А. Библиотека в пространстве преобразований Документ в социокультурном пространстве: теории и цифровые трансформации: материалы VI Междунар. науч.-практ. конф. (18 мая 2023 г.) / науч. ред.: Л.Е. Савич, А.Р. Мансурова; сост. Г.В. Матвеева, Ю.Н. Галковская. – Казань, 2023. – 524 с.
2. Игнатов В.С., Пименова Д.В. Информационное пространство. Структура и функции // Известия вузов. Поволжский регион. Общественные науки. – 2007. – № 3.
3. Мигулева М.В. Киберпространство как социальный институт: признаки, функции, характеристики // Научный журнал «Дискурс-Пи». – 2020. – № 4 (41). С. 199–212.
4. Мелентьева Ю.П. Роль и место традиционной библиотеки в условиях цифровизации общества // Культура: теория и практика. – 2019. – № 1 (28).
5. Пронина Л.А. Современная информационная среда как новая форма бытия человека // Аналитика культурологии. – 2005. – № 4.
6. Судоргин О.А. Новая роль информационного пространства в XXI веке // Власть. – 2009. – № 1.
7. Толковый словарь Глоссарий.ру [Электронный ресурс]. – URL: http://www.glossary.ru/cgi-bin/gl_find.cgi? (дата обращения: 01.04.2024).
8. Clark D.D. (2010). Characterizing cyberspace: Past, present and future (ECIR Working Paper No. 2010-3). MIT Political Science Department [Электронный ресурс]. – URL: https://dspace.mit.edu/bitstream/handle/ (дата обращения: 11.04.2024)

К ВОПРОСУ ПОЛУЧЕНИЯ ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Емельянова О.В.,
Симонова В.Д.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: статья посвящена анализу проблемы получения информации, необходимой для расследования преступлений в сети Интернет. Рассмотрены проблемы, возникающие на разных площадках сети, и пути их решения. Предложено создание единой системы для оперативного информирования сотрудников.

Ключевые слова: информационные технологии, сотрудники полиции, Интернет, киберпространство.

ON THE ISSUE OF OBTAINING OPERATIONALLY SIGNIFICANT INFORMATION ON THE INTERNET: PROBLEMS AND WAYS FOR THEIR SOLUTIONS

Emelyanova O.V.,
Simonova V.D.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: the article is devoted to the analysis of the problem of obtaining information necessary for investigating crimes on the Internet. The problems that arise on different network sites and ways to solve them are considered. It is proposed to create a unified system for promptly informing employees.

Keywords: information technology, police officers, Internet, cyberspace.

Информационные технологии занимают одно из центральныхе мест в жизни общества, которая строится на цифровизации и использовании различных электронных ресурсов. Ввиду таких изменений происшествия все чаще стали случаться на информационных площадках: злоумышленники находят способы обмануть людей, сделать это становится в некоторых случаях проще из-за кодификации информационных систем. Стремительное внедрение информационно-коммуникационных технологий во все сферы общественной жизни значительно изменили характер, методы и способы информационной деятельности государственных структур и вооруженных сил наиболее развитых государств [2].

Преступления, совершаемые с использованием информационно-коммуникационных технологий являются в настоящее время наиболее распространенными. По данным статистики МВД России, за прошедший год зафикси-

ровано рекордное количество преступлений, совершаемых в Интернете. Их численность составляет 677 тыс, что является 34,8% от всех преступлений, зарегистрированных в 2023 году. Стоит отметить, что более половины данных преступлений относятся к категории тяжких и особо тяжких. Таким образом, статистика показывает, что преступления с использованием Интернета занимают лидирующее положение, за ними следует мошенничество с использованием телефонной связи (вишинг) и кражей данных банковских карт.

С развитием информационных технологий деятельность подразделений полиции плавно перешла на информационные платформы. Преступления совершаются на площадках сети Интернет (маркет-плейсы, сайты интернет-магазинов и банков), социальных сетей и в наиболее опасном секторе информационной сети – DarkNet. Ввиду развития технологий следует отметить, что данные виды противоправных деяний являются наиболее сложными, т.к. злоумышленникам проще скрывать свои следы, и требуют быстрого реагирования в связи с названным фактором. Данное явление связано с тем, что в России Интернет является открытым источником, абсолютно каждый человек может свободно им пользоваться: размещать информацию, работать, совершать покупки, обучаться и т.п. В силу такой открытости информационного поля существуют угрозы информационной безопасности. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.11.2016 № 646 выделяет следующие сферы защиты: 1) экономическая сфера; 2) внешнеполитическая; 3) внутриполитическая; 4) область образования, науки и технологий; 5) духовная; 6) судебная и правоохранительная. В деятельность органов внутренних дел входит обеспечение информационной безопасности. Подразделения информационной безопасности осуществляют надзор в части целостности, доступности информации путем обеспечения защищенности каналов связи, бесперебойной работы информационно-телекоммуникационных систем.

Изучая следственно-судебную практику деятельности правоохранительных органов, можно выявить некоторые причины, которые негативно сказываются на их работе: 1) отсутствие нормативного закрепления норм, предусматривающих проведение оперативно-разыскных мероприятий поискового характера в сети Интернет в Федеральном законе от 12.09.1995 № 144-ФЗ «Об оперативно-разыскной деятельности»; 2) низкая квалифицированность сотрудников в сфере прикладных технологий; 3) сложность деанонимизации пользователя сети Интернет.

Несмотря на данные проблемы, правоохранительные органы адаптируют основные методы полицейской деятельности к особенностям киберпространства. Рассмотрим три зоны работы подразделений полиции в информационной среде: сайты сети Интернет, DarkNet и использование искусственного интеллекта.

Наиболее распространенной проблемой, согласно статистике, является мошенничество в Интернете. Оно достаточно обширно и имеет самые разные проявления. Кроме того, из года в год растет количество успешных кибератак, что не является положительной характеристикой. Кроме потери финансовых составляющих, происходят неблагоприятные социальные изменения, а именно

«утечки» личных данных пользователей, нарушаются их законные права на личную безопасность. В качестве ярких примеров можно привести ситуации с «Ренессанс страхованием» и с МТС Банком, когда из-за кибератак пострадали личные данные пользователей. Стоит отметить, что за подготовку и проведение кибератак наступает уголовная ответственность.

Особую угрозу составляет искусственный интеллект. С его помощью совершают преступления вишинга, а именно подделка голосов и т.п. Однако главное – искусственный интеллект служит помощником в «изобретении» новых моделей преступного бизнеса и вредоносного программного обеспечения и создании сложновыявляемого фальсифицированного контента. Поэтому требуется более четкая регламентация специальных программных средств, способных обеспечить оперативный доступ к компьютерным данным, представляющим интерес для раскрытия преступлений.

Еще одним направлением в сети Интернет является DarkNet. Опасность данной Сети состоит в том, что на нее нет прямого входа, для этого используется программа TOR, суть работы которой заключается в многоуровневом шифровании данных. Особенность веб-адресов в этой Сети заключается в том, что их доменное имя позволяет пользователю скрыть свои данные от интернет-провайдера и получить абсолютную анонимность. За счет данной специфики шифрования информации в DarkNet´ часто совершаются противоправные деяния. На данном сервере происходит незаконная продажа оружия и наркотических средств, публикуются подробные инструкции по изготовлению взрывных устройств, осуществляются террористические агитации, а также другие склонения лиц к совершению преступлений. Обычная блокировка сайтов не поможет в решении данной проблемы, т.к. пользователи используют «мосты», «зеркала», VPN-серверы. Для успешной обработки информации, позволяющей раскрыть преступление, необходимо выполнение следующего ряда задач: 1) изучение сайтов-аналогов TOR; 2) упорядочивание законодательного оформления информации, полученной из теневого интернета; 3) ориентирование сотрудников в первую очередь на открытые сети, т.к. чаще всего люди получают необходимую информацию там, а затем за более подробной информацией направляются в теневой Интернет.

Таким образом, можно выделить следующие основные методы добывания необходимой информации для расследования преступлений:

- Взаимодействие подразделений полиции с различными службами, такими как операторы сотовой связи, почтовые сервисы, поисковые системы, облачные хранилища и т.п. При направлении запроса в соответствующую службу можно получить необходимую информацию.
- Применение специальной техники, позволяющей снимать информацию с используемых преступниками каналов связи.
- Внимательное изучение информации из открытых источников. Переходы на страницы сайтов, чтение статей определенных личностей, подписки на группы в социальных сетях – все это при детальном изучении позволяет составить пласт необходимых сведений для расследования преступления.

При столкновении полиции с делами, связанными с сервисом DarkNet, необходимо использовать библиотеки WebRTC, предназначенные для обмена сетевыми данными между браузерами без промежуточных браузеров. Данная программа позволяет установить реальный IP-адрес, как при использовании человеком VPN-сервисы, так и без него. Таким образом в данной среде можно применить классический способ добывания информации, а именно, посредством наблюдения и проведения тайных операций, отслеживать онлайн-рынки, по поступающим денежным потокам для последующего их закрытия [1].

Для упорядочивания работы органов правопорядка необходимо восполнить существующие пробелы и неточности в законодательстве Российской Федерации. Для успешного разрешения проблем, возникающих в информационном секторе государства, необходимо составить единую справочную систему информирования. Необходимость такой системы состоит в том, что, как описывалось выше, преступления в IT-сфере охватывают сразу несколько отраслей деятельности органов внутренних дел и происходят на разных платформах интернета [3]. Также не стоит забывать, что в настоящее время общество и его процессы стремительно меняются и развиваются. Именно поэтому стоит своевременно повышать квалификацию сотрудников и углубляться в более узкие направления новых видов преступлений. Для эффективного раскрытия информационных преступлений необходимо иметь кооперацию со всеми подразделениями МВД России, а также развивать информационный сектор безопасности, который в настоящее время является неотъемлемой частью любой сферы жизни общества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. – 2019. – № 5. – С. 97–101.

2. Осипенко А.Л. Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. – 2021. – № 1 (75).

3. Пучнин А.В., Горбова А.В. Аппаратно-программные и технические средства фиксации преступной деятельности, осуществляемой в сети Интернет // Охрана, безопасность, связь. – 2018. – Т. 1. – № 3 (3). – С. 209–217.

4. Куриленко Ю.А., Едигарева Ю.Г., Ле Тхи Ван Обеспечение информационной безопасности при утечке, разглашении и торговле персональными данными // Криминологический журнал. – 2023. – № 2. – С. 216–221.

5. Комардина А.А., Меняйло Д.В., Меняйло Л.Н. Применение информационных технологий и возможностей цифровизации в деятельности сотрудника ОВД / Экономическая безопасность: правовые, экономические, экологические аспекты: сборник научных трудов 6-й Международной научно-практической конференции, Курск, 9 апреля 2021 года. – Курск, 2021. – С. 184–187.

6. Страхов А.А., Дубинина Н.М. Об утечке данных и DLP-системах // Криминологический журнал. – 2022. – № 4. – С. 226–232.

УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ: КЛАССИФИКАЦИЯ И МЕТОДЫ ЗАЩИТЫ

Ермолова С.В.,
Капусткин Н.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в данной работе рассмотрены уязвимости информационных систем: классификация и методы защиты.

Ключевые слова: информационные системы, уязвимости, угрозы, защита информации.

VULNERABILITIES OF INFORMATION SYSTEMS: CLASSIFICATION AND METHODS OF PROTECTION

Ermolova S.V.,
Kapustkin N.A.
(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: in this paper the vulnerabilities of information systems are considered: classification and methods of protection.

Keywords: information systems, vulnerabilities, threats, information protection.

В настоящее время сложно представить мир без информационных технологий, присутствующих во всех сферах нашей жизни. Однако наряду с этими преимуществами информационные технологии несут угрозы, одной из которых являются уязвимости информационных систем (далее – ИС).

Угрозы и уязвимости – это два важных понятия в области информационной безопасности, но они имеют разные значения и роли.

Угроза представляет собой потенциальную возможность события или действия, которое может нанести ущерб информационной системе, данным или ресурсам. Примерами угроз являются вирусы, хакерские атаки, природные катастрофы и человеческие ошибки, которые влекут. нарушения, доступности и конфиденциальности [2].

Число уязвимостей не ограничено и со временем их становится только больше.

Уязвимость – это слабое место или недостаток в системе, который может быть использован злоумышленником для нарушения безопасности или проведения атаки. Уязвимость может проявляться в виде программных ошибок, недостатков конфигурации, отсутствия обновлений или недостаточных мер защиты.

Для обеспечения информационной безопасности необходимо не только идентифицировать угрозы и уязвимости, но и принимать меры по их устранению или уменьшению для уменьшения потенциальных рисков и защиты системы от возможных угроз.

Уязвимости, в контексте информационных систем, регламентируются по ГОСТу Р 56546-2015 «Защита информации. Уязвимости информационных систем». В данном стандарте дается одно глобальное определение уязвимости и пять узких определений: уязвимость кода, уязвимость конфигурации, уязвимость архитектуры, организационная уязвимость, многофакторные уязвимости [3]. В широком смысле уязвимость – это недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Понимание разнообразных видов уязвимостей и методов их обнаружения и защиты становится ключевой задачей для организаций, государственных учреждений и даже обычных пользователей. Эта тема обретает особую актуальность в условиях, когда угрозы информационной безопасности становятся все более сложными и изощренными. В стандарте 56546-2015 дается классификация уязвимостей информационных систем по следующим классификационным признакам:

- область происхождения уязвимости ИС;
- типы недостатков ИС;
- место возникновения (проявления) уязвимости ИС.

Согласно ГОСТу Р 56546-2015 года уязвимости ИС по области происхождения подразделяются на следующие виды:

– уязвимости кода, появившиеся в процессе разработки программного обеспечения;

– уязвимость архитектуры, появившиеся в процессе проектирования ИС;

– уязвимость конфигурации, появившиеся в процессе задания конфигурации програмного обеспечения и технических средств ИС;

Организационная уязвимость – уязвимость, появившаяся в связи с отсутствием организационных мер защиты информации в ИС и несоблюдением правил эксплуатации системы защиты информации ИС, требований организационно-распорядительных документов по защите информации и несвоевременном выполнении соответствующих действий должностным лицом или подразделением, ответственным за защиту информации;

Многофакторная уязвимость – уязвимость, появившаяся в результате наличия нескольких различных типов [1].

Для того чтобы защититься от данных типов уязвимостей, необходимо применять следующие меры:

1. *Тестирование кода.* Проведение тщательного тестирования программного кода на наличие уязвимостей, такие как SQL-инъекции, XSS и другие. Помимо этого существует база данных эксплоитов (программный код или набор инструкций, который используется для активации и использования

уязвимости в компьютерной программе, операционной системе, сетевом протоколе или устройстве.).

2. *Статический анализ кода.* – Это метод исследования программного кода, который выполняется без его фактического выполнения. Данный вид анализа помогает выявить потенциальные проблемы, ошибки и уязвимости в коде до его запуска. Для выполнения данной задачи специалисты используют различные инструменты, среди них наиболее популярны: ESLint, Pylint, Checkstyle, Cppcheck, SonarQube.

3. *Обучение разработчиков*. Мера, направленная на обучение разработчиков лучшим практикам безопасной разработки и контролю качества кода.

4. *Проведение архитектурного анализа*. Оценка архитектуры информационной системы на предмет безопасности и применение соответствующих архитектурных шаблонов и практик.

5. *Применение принципов обеспечения безопасности в архитектуре*. Учет принципов безопасной архитектуры, таких как принцип наименьших привилегий при проектировании системы;

6. *Проводение аудита конфигурации*. – Это важная практика для обеспечения безопасности, эффективности и соответствия систем определенным стандартам и требованиям. Существует множество инструментов, которые могут быть использованы для аудита конфигурации, например Nessus, OpenVAS, Lynis.

7. *Автоматизированное управление конфигурацией*. Использование инструментов автоматизации для управления конфигурациями и обеспечения их соответствия стандартам безопасности для устранения ошибок из-за человеческого фактора.

8. *Политики и процедуры безопасности*. Разработка внедрение политики и процедуры безопасности, которые охватывают организационные аспекты безопасности информации, включая правила эксплуатации и обучение сотрудников.

9. *Интегрированный подход*. Применение комбинированных методов и мер защиты, для борьбы с многофакторными уязвимостями.

10. *Мониторинг и реагирование*. Регулярная проверка системы и реагирование на аномалии или инциденты, которые могли возникнуть из-за многофакторных уязвимостей.

Для удобства отслеживания уязвимостей и угроз, которые они в себе несут, существуют CVE (Common Vulnerabilities and Exposures) и CVSS (Common Vulnerability Scoring System) – стандарты и системы классификации уязвимостей и оценки их серьезности в компьютерной безопасности.

CVE – это система идентификации и наименования уязвимостей в компьютерной безопасности. Каждая уязвимость, подверженная атаке, получает уникальный идентификатор в формате CVE-год-номер, например CVE-2022-12345. Таким образом, строится база уязвимостей с уникальным стандартным идентификатором, что позволяет разработчикам, администраторам и исследователям программного обеспечения эффективнее обмениваться инфор-

мацией о конкретных уязвимостях и сосредотачиваться на их исправлении и искоренении.

CVSS – это система оценки серьезности уязвимости, которая предоставляет числовую оценку для характеристик уязвимости, таких как доступность, воздействие и сложность эксплуатации. Она оценивает уязвимости по шкале от 0 до 10, где 10 означает максимальную опасность. Система позволяет администраторам и разработчикам определить, насколько критична уязвимость, и принять соответствующие меры по ее устранению или уменьшению рисков.

Использование этих систем обеспечивает стандартизацию и более точную оценку уязвимостей в информационной безопасности. Организации и эксперты по информационной безопасности используют для более эффективного управления и реагирования на уязвимости.

Информационная безопасность является критически важным аспектом в современном мире, где множество угроз и уязвимостей могут подвергнуть риску конфиденциальность, целостность и доступность данных информационных систем.

Существует множество различных типов уязвимостей, включая уязвимости кода, архитектуры, конфигурации, организационные и многофакторные уязвимости. Каждый тип требует своих методов и мер безопасности для защиты.

Меры защиты от уязвимостей включают в себя технические, архитектурные, организационные меры. Эффективный подход к безопасности требует комплексного подхода и интеграции всех этих мер.

Стандарты и системы, такие как CVE и CVSS, играют важную роль в классификации, идентификации и оценке уязвимостей. Они обеспечивают стандартизацию и обмен информацией о уязвимостях, что помогает более эффективно управлять безопасностью информационных систем.

Важно подчеркнуть, что безопасность информационных систем требует постоянного мониторинга и обновления, а также соблюдения лучших практик в области безопасности, чтобы минимизировать риски и обеспечить защиту информации и ресурсов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Введение. 2015-08-19. – Москва: Стандартинформ, 2015. – 17 с.

2. Системы классификации и оценки уязвимостей и угроз информационных систем: какие они бывают и зачем нужны [Электронный ресурс]. – URL: https://habr.com/ru/companies/bastion/articles/706884/.

3. Зубарев И.В. [и др.] Уязвимости информационных систем // Информационные и математические технологии в науке и управлении. – 2016. – № 3. – С. 174–182.

ЧАТ-БОТ КАК ИННОВАЦИОННЫЙ ИНСТРУМЕНТ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ

Жмурко Д.Ю.,
кандидат экономических наук, доцент
(Краснодарский университет МВД России);
Лаптев С.В.,
кандидат физико-математических наук, доцент
(Кубанский государственный аграрный университет имени И.Т. Трубилина);
Шарпан М.В.,
кандидат физико-математических наук, доцент
(Краснодарский университет МВД России)

Аннотация: статья посвящена использованию инновационного инструмента – чат-бота при дистанционном обучении.

Ключевые слова: чат-бот, дистанционное образование, инновационный инструмент.

CHATBOT AS AN INNOVATIVE TOOL FOR DISTANCE LEARNING

Zhmurko D.Yu.,
Candidate of Economic Sciences, Associate Professor
(Krasnodar University of the Ministry of the Interior of Russia);
Laptev S.V.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Kuban State Agrarian University named after I.T. Trubilin);
Sharpan M.V.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Krasnodar University of Ministry of the Interior of Russia)

Abstract: the article is devoted to the use of an innovative chatbot tool in distance learning.

Keywords: chatbot, distance education, innovative tool.

Рост популярности дистанционного образования ставит перед образовательными учреждениями новые вызовы, среди которых – обеспечение качественного взаимодействия между преподавателями и слушателями в виртуальном пространстве. Чат-боты представляют собой инновационное решение, способное значительно улучшить эту взаимосвязь. Они обеспечивают непрерывное взаимодействие 24/7, доступ в любое время из любой точки мира, а также объективность оценки знаний слушателей. В контексте современного рынка образовательных услуг применение чат-ботов становится не только актуальным, но

и необходимым шагом для поддержания конкурентоспособности образовательных программ.

В нашем случае создание этого инновационного инструмента было направлено на решение весьма актуальной задачи – автоматизации процесса проведения зачета по дисциплине «Информационные технологии и кибербезопасность органов внутренних дел Российской Федерации».

Чат-бот представляет собой первый шаг на пути цифровизации учебного процесса не только в образовательной системе МВД России, но и во всей строне в данной области. На момент его создания аналогов данному решению в нашей стране не существовало, что делает его пионером в области образовательных технологий для органов внутренних дел.

Удобный инструмент не просто автоматизирует прием зачета, он призван облегчить и оптимизировать процесс обучения и проверки знаний слушателей. С помощью этого инструмента слушатели смогут подготовиться к зачету более основательно, в любое время суток и из любой точки, где есть доступ в Интернет.

Важнейшей особенностью нашего чат-бота является то, что он был создан с использованием платформы Manybot, что подразумевает под собой технологии no-code. Это значит, что для создания и настройки чат-бота не требуется глубоких знаний в программировании. Благодаря интуитивно понятному интерфейсу Manybot разработка становится доступна каждому, и даже без специальных технических навыков преподаватели могут самостоятельно разрабатывать пошаговые сценарии для различных образовательных задач.

Это открывает поразительные возможности для адаптации под конкретные учебные программы и курсы. Каждый преподаватель в силах создать чат-бот, который будет настроен на определенную дисциплину, тему или даже зачет, – и все это без необходимости вникать в сложности кода, что традиционно было уделом исключительно IT-специалистов.

Такой подход значительно повышает эффективность учебного процесса, делает его более гибким и индивидуализированным. Мы уверены, что внедрение таких чат-ботов сможет положительно отразиться на качестве подготовки специалистов для органов внутренних дел, сделав этот процесс более современным, интерактивным и доступным каждому.

Кроме того, чат-бот включает в себя аналитическую функцию, позволяющую преподавателям оценивать успеваемость и выявлять общие тенденции в знаниях слушателей, что является важным компонентом при формировании методических и образовательных стратегий.

Чат-боты – это программные агенты, способные имитировать письменное или устное общение с человеком, используя искусственный интеллект и машинное обучение. В зависимости от классификационного признака чат-боты можно классифицировать по-разному. Так например, примитивные могут работают по заранее определенным правилам и не способны учиться на ходу; саморазвивающиеся используют сложные алгоритмы для обучения и адаптации к пользовательским запросам; гибридные сочетают элементы обоих предыдущих типов для оптимальной эффективности.

Основные функции чат-ботов включают обработку и интерпретацию пользовательских вопросов, предоставление ответов и решений, а также выполнение определенных задач, таких как вызов, действие (наступление события) или ведение диалога.

В качестве очевидных преимуществ можно выделить то, что чат-боты позволяют автоматизировать несложные однообразные задачи, могут обращаться с большим объемом запросов одновременно, доступны в любое время дня и ночи без перерывов и выходных, обеспечивая поддержку слушателей, находящихся в разных часовых поясах.

Эти преимущества делают чат-ботов важным инструментом в модернизации и оптимизации образовательных процессов, в том числе и процедур проведения зачетов в условиях дистанционного обучения.

Рассмотрим пример использования чат-бота в работе факультета переподготовки и повышения квалификации.

Основной целью обучения на ФПиПК является укрепление профессиональных компетенций и адаптация к новым требованиям служебной деятельности, по возможности без отрыва от своей профессиональной деятельности. Для достижения этой цели применяются смешанные образовательные форматы, включая очные и дистанционные занятия, практические курсы, и вебинары от ведущих преподавателей вуза.

Для того чтобы дистанционное образование было эффективным, необходимо соблюдать ряд требований: 1) использование передовых образовательных технологий; 2) высокий уровень взаимодействия между слушателями и преподавателями посредством различных средств связи; 3) доступность в любое удобное время, что требует гибкости в планировании учебных программ и наполнении курсов.

Всем указанным выше требованиям в полной мере соответствует чат-бот.

Он представляет собой технологию, базирующуюся на искусственном интеллекте, которая позволяет автоматизировать процесс взаимодействия со слушателями факультета переподготовки и повышения квалификации в условиях дистанционного обучения (приема/сдачи зачета). Наш чат-бот оснащен функциями естественного языкового взаимодействия, что позволяет слушателям задавать вопросы и получать на них инструкции или ответы в режиме реального времени – таким образом, чат-бот может выступать в качестве виртуального преподавателя или экзаменатора.

Основные функциональные возможности и преимущества заключаются в реализации стандартизированных процедур проведения зачетов без необходимости постоянного присутствия преподавателей; одновременное проведение зачетов для большого числа слушателей без потери качества взаимодействия; возможность адаптировать вопросы и темы зачетов под конкретного слушателя на основе предварительного анализа входных данных об обучении и предпочтениях пользователя.

Инновация способствует не только улучшению административных (контролирующих) аспектов образования, но и обогащает педагогический процесс,

внося элементы интерактивности, доступности и адаптивности, что крайне важно для современного образовательного пространства.

Таким образом, внедрение чат-бота как инновационного инструмента для проведения зачетов открывает новые горизонты для повышения качества и доступности обучения на Факультете переподготовки и повышения квалификации и адаптации к требованиям современного информационного общества.

Представленная инновация обладает потенциалом радикально трансформировать образовательное пространство. Она может внести существенные изменения в методы обучения, делая их более интерактивными и персонализированными. Это поможет обучающимся не только лучше усваивать материал, но и развивать критическое мышление и творческие способности. Также стоит отметить возможность интеграции данной технологии с существующими образовательными системами, что облегчит ее адаптацию и повысит эффективность обучения в целом.

Таким образом, внедрение данной инновации может стать значимым шагом на пути к современному, динамичному и инклюзивному образовательному процессу.

Следует подчеркнуть, что эиап проект – это лишь вершина айсберга в деле внедрения цифровых технологий в учебный процесс, и мы полны решимости продолжать развитие в этом направлении.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Смирнова Е. Трудно быть ботом: как сделать чат-бота с помощью DeepPavlov [Электронный ресурс]. – URL: https://sysblok.ru/nlp/trudnobyt-botom-kak-sdelat-chatbota-s-pomoshhju-deeppavlov/.

2. Ураев Д.А. Классификация и методы создания чат-бот приложений // International scientific review. 2019. № LXIV [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/klassifikatsiya-i-metody-sozdaniya-chat-botprilozheniy.

3. Борисенко А.В. Особенности использования программного интерфейса приложения / Математические методы и информационно-технические средства: материалы XIX Международной научно-практической конференции. – Краснодар, 2023. С. 33–36.

4. Эволюция чат-ботов [Электронный ресурс]. – URL: https://habr.com/ru/post/402013/.

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ПОЖАРНО-СПАСАТЕЛЬНЫХ ПОДРАЗДЕЛЕНИЙ МЧС РОССИИ

Жукова П.Н.,
доктор физико-математических наук, доцент
(Санкт-Петербургский университет ГПС МЧС России
имени Героя Российской Федерации генерала армии Е.Н. Зиничева);
Прокопенко А.Н.,
кандидат технических наук, доцент
(Академия Государственной противопожарной службы МЧС России);
Страхов А.А.,
доцент
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в работе рассмотрены возможности использования технологий искусственного интеллекта при интеллектуальном сопровождении ликвидации пожаров пожарно-спасательными подразделениями. Модель оперативного управления организацией пожаротушения основана на структурно-функциональных компонентах подсистемы интеллектуальной поддержки анализа и контроля оперативной обстановки при пожаротушении. Предлагается использовать визуализацию данных для облегчения анализа поступающей оперативной информации на месте ликвидации пожара.

Ключевые слова: искусственный интеллект, визуализация, пожаротушение, ликвидация пожаров, расстановка сил и средств.

PROSPECTS OF CREATION OF AN INTELLECTUAL SYSTEM OF ANALYSIS OF THE OPERATIONAL SITUATION AT THE FIRE ELIMINATION SITE USING ARTIFICIAL INTELLIGENCE METHODS

Zhukova P.N.,
Doctor of Physical and Mathematical Sciences, Associate Professor,
(St. Petersburg State University of the Ministry of Emergency Situations of Russia
named after Hero of the Russian Federation, Army General E.N. Zinichev);
Prokopenko A.N.,
Candidate of Technical Sciences, Associate Professor
(Academy of the State Fire Service of the Ministry of Emergency Situations of Russia);
Strakhov A.A.,
Associate Professor
(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: the article considers possibilities of using artificial intelligence technologies in the intellectual support of fire and rescue departments. The model of operational management of fire extinguishing organization is based on structural and

functional components of the subsystem of intelligent support of analysis and control of operational situation during fire extinguishing. It is proposed to use data visualization to facilitate the analysis of incoming operational information at the scene of the fire.

Keywords: artificial intelligence, visualization, fire extinguishing, alignment of forces and means.

Информационно-аналитическое обеспечение организации системы поддержки принятия решений по управлению действиями пожарно-спасательных подразделений (далее – ПСП) при пожаротушении остается одним из главных направлений совершенствования системы управления МЧС России [1, 2]. Особый интерес представляет возможность использования методов искусственного интеллекта (далее – ИИ) в деятельности ПСП с учетом ограниченности использования электронно-вычислительных средств во время тушения пожара.

В этой связи перед анализом возможности внедрения ИИ необходимо рассмотреть направления действий, в соответствии с которыми использование сил и средств ПСП в данный момент времени обеспечивает наиболее эффективные условия для ликвидации пожара.

Алгоритм действий ПСП состоит из известных этапов [3]:

– прием и обработка сообщения о пожаре (оценка полученной информации, принятие решения о привлечении сил и средств; получение документов предварительного планирования действий по тушению пожара и административной информации об объекте);

– выезд и следование к месту пожара;

– разведка места пожара (сбор информации о пожаре для оценки обстановки и принятия решений по организации действий ПСП);

– аварийно-спасательные работы по тушению пожара;

– развертывание сил и средств;

– ликвидация горения;

– специальные работы;

– сбор и возвращение к месту дислокации.

Документы предварительного планирования действий ПСП на месте пожара (планы и карточки тушения пожара) передаются руководителю тушения пожара (далее – РТП) на бумажном носителе. Первичное ознакомление с указанными документами ограничено временем прибытия на объект вызова и ликвидации пожара. Последующая детализированная информация поступает из данных разведки.

Разведка в основном проводится личным составом, задействованным в процессе ликвидации чрезвычайной ситуации, и ведется непрерывно с момента сообщения о пожаре и до его полной ликвидации. На настоящий момент наиболее полное представление об оперативной обстановке для последующего анализа и принятия решений РТП поступает именно из данных источников.

Таким образом, принятие и реализация решений РТП в ситуации корректного прогнозирования процесса развития пожара требует постоянного информационного сопровождения.

Отметим, что с учетом нижеперечисленных факторов необходимо обратить внимание на потенциальную неприменимость автоматизированного интеллектуального сопровождения (объем информационных потоков, технических средств и т.п.) действий ПСП или РТП:

– временных ограничений принятия решений при ликвидации пожара;

– невозможности одновременного использования цифровых устройств и пожарного оборудования;

– опасных условий и факторов использования цифровой техники.

Широко известно [4, 5], что визуализация (графическое представление) реальных и абстрактных данных облегчает восприятие человеком информации, что позволяет наглядно представить ключевые положения и выводы.

В этой связи представляется наиболее приемлемым использование цифровых устройств визуального представления статической и динамической информации об объекте пожаротушения, расстановке и использовании сил и средств при ликвидации пожара при принятии решений РТП и оперативных штабов на месте тушения пожара (далее – ОШТП).

Ниже представлена схема использования статических (паспорт пожаротушения) и динамических данных для визуализации привлечения и расстановки сил и средств при ликвидации пожаров (см. рис.1).

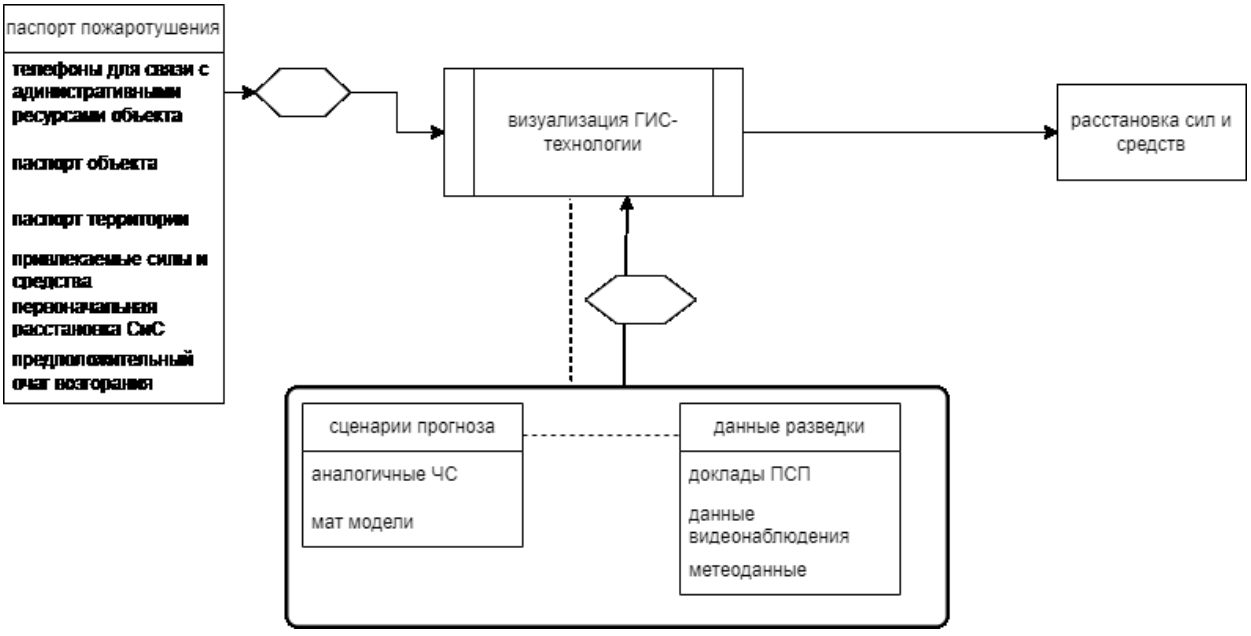


Рисунок 1. Структурно-функциональные компоненты
динамической подсистемы интеллектуальной поддержки анализа и контроля
оперативной обстановки пожаров

Анализ методов искусственного интеллекта, позволяет сделать вывод о возможности внедрения структуры ИИ в систему поддержки принятия решений РТП и ОШТП, например [6].

Общая классификация методов ИИ представлена на рисунке 2.

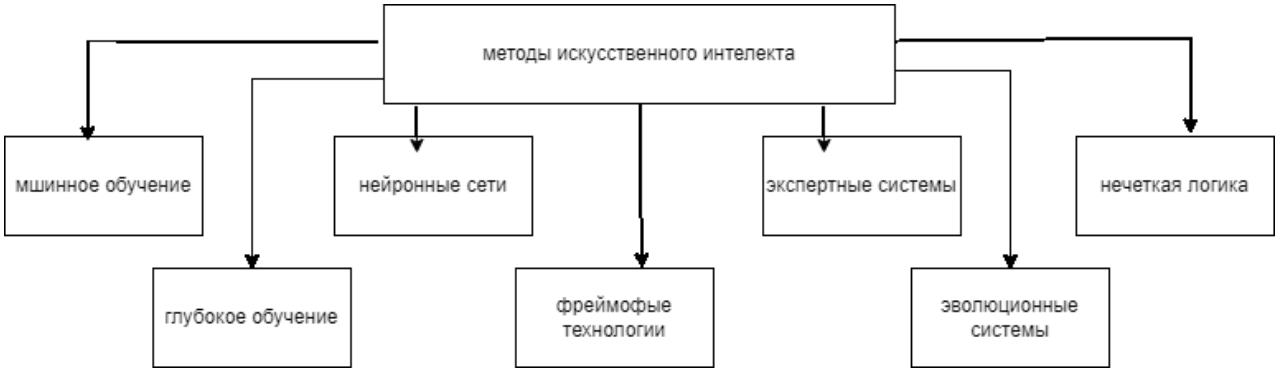


Рисунок 2. Общая классификация методов искусственного интеллекта

Данные созданной экспертной системы могут быть применимы при анализе аналогичных ситуаций.

Методы использования машинного обучения и построения искусственных нейросетей:

– математическая модель прогноза развития пожара. Например, использование вероятностных графических моделей (Байесовская сеть);

– преобразование текста в изображение – визуализация первичной статической информации об объекте пожаротушения;

– распознавание речи (создание сети речевых дескрипторов, причем количество объектов датасета ограничено профессиональной терминологией). Кроме того, требуется обработка коротких речевых сегментов, что облегчает задачу распознавания;

– преобразование речи в изображение. Визуализация донесений разведки на месте пожаротушения, команд РТП, данные с дронов, в случае задействования и т.п.

Ниже представлена модель реализации визуализации речевой информации.

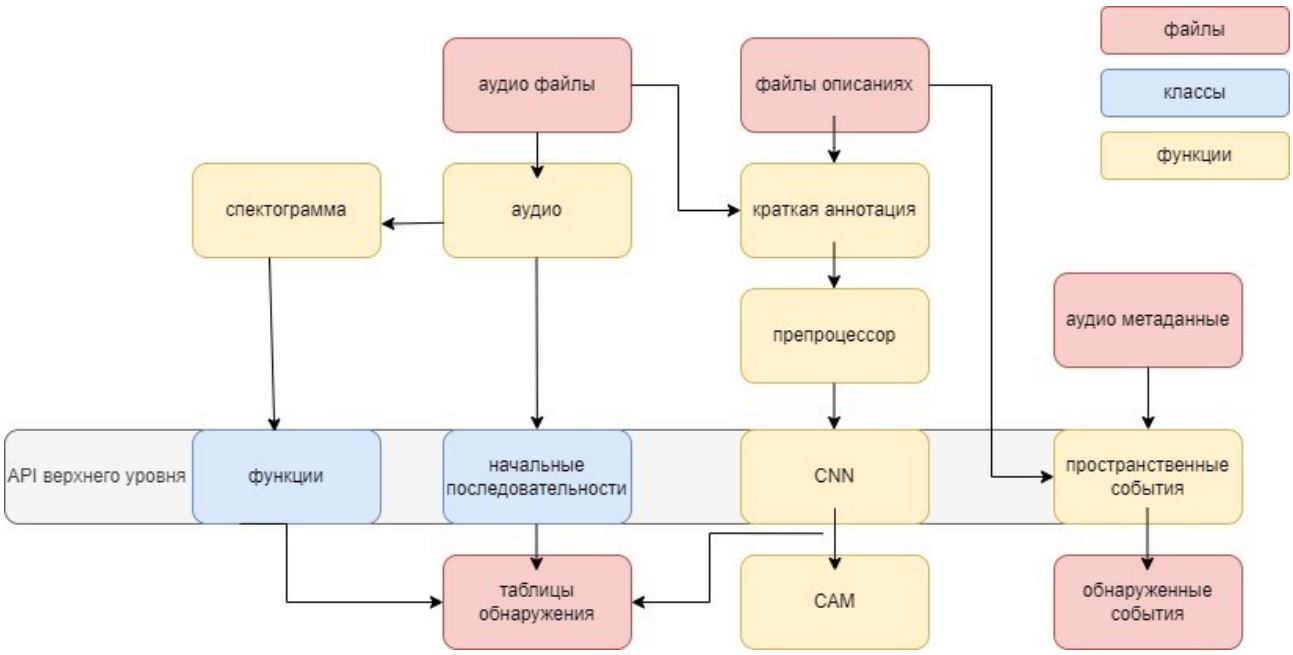


Рисунок 3. Модель реализации визуализации речевой информации

Классы и функции обеспечивают обнаружение звуков во времени и пространстве. Стрелки на диаграмме представляют поток информации от входов к выходам.

Классы и методы API верхнего уровня (серый прямоугольник) можно вызывать напрямую, чтобы использовать основные функции, не зная других частей API.

API, интерфейс прикладного программирования; CAM – карты активации классов; CNN – сверточная нейронная сеть.

Реализовать рассмотренную модель визуализации можно с помощью аналитеческой панели, которая позволит объединить данные и обобщить основную информацию по различным параметрам в режиме реального времени, что поможет отслеживать тенденции для разных временных отрезков ликвидации пожара. Информация может быть представлена в виде инфографики, метеоданных, графического представления оперативной обстановки, отчетов. Панель индикаторов возможно изменять, меняя анализируемые данные или подгружая их в реальном времени.

Возможности визуализации процесса пожаротушения и средства аналитики позволят максимально быстро учитывать изменения последовательных характеристик, изменений ситуации при пожарах, что , в свою очередь сократит время на принятие решений, влияющих на выполнение оперативно-тактических задач и характер их выполнения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Степанов О.И. Информационно-аналитическое обеспечение управления пожарными подразделениями при тушении пожаров в жилом секторе: дис. … канд. техн. наук. – Москва, 2019. – 192 с.

2 Степанов О.И., Худякова С.А. Применение моделей систем информационно-аналитического обеспечения пожарно-спасательных подразделений при пожаротушении // Вестник Дагестанского государственного технического университета. Технические науки. – 2019. – № 46 (2). – С. 108–117.

3. Денисов А.Н., Степанов О.И. Структура системы управления пожарно-спасательными подразделениями на начальном этапе пожаротушения // Технологии техносферной безопасности. – 2017. – № 3 (73). – С. 3–7.

4. Бразговка О.В., Микова О.П. Визуальное представление информации // Решетневские чтения. – 2014. – № 18.

5. Вашунина И.В. Особенности визуального способа представления информации // Вестник УРАО. – 2008. – № 3.

6. Симанков В.С., Теплоухов С.В. Аналитическое исследование методов и алгоритмов искусственного интеллекта // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – № 3 (266).

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КРИМИНАЛЬНОЙ ВЕБКАМ-ИНДУСТРИИ

Задохина Н.В.,
кандидат педагогических наук;
Карелова П.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: статья посвящена анализу сущности вебкам – индустрии, как преступному феномену цифрового мира, а также разработке уголовно-правовых мер, способствующих активному противодействию данному криминальному явлению. Актуальность темы проведенного исследования обусловлена тем, что сфера вебкам индустрии влечет за собой проблемы не только юридического или психологического характера, но и демографического, так как молодежь получает искаженное представление о семье, семейных отношениях и семейных ценностях.

Ключевые слова: феномен вебкам**,** вебкам-модель, вебкам-студия, правовое противодействие.

FEATURES OF COUNTERING CRIMINAL WEBCAM INDUSTRY

Zadokhina N.V.,
Candidate of Pedagogical Sciences;
Karelova P.A.
(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: the article is devoted to the analysis of the essence of the webcam industry as a criminal phenomenon of the digital world, as well as the development of criminal legal measures that contribute to the active counteraction to this criminal phenomenon. The relevance of the topic of the study is due to the fact that the webcam industry entails problems not only of a legal or psychological nature, but also of a demographic nature, since young people receive a distorted idea of the family, family relationships and family values.

Keywords: webcam phenomenon, webcam model, webcam studio, legal opposition.

С уверенностью можно утверждать, что вебкам – индустрия – это принципиально новая форма предоставления услуг интимного содержания (эротического или порнографического). Детальное рассмотрение феномена вебкам позволяет определить его сущность как коммерческое оказание онлайн услуг интимного содержания в киберпространстве [2, с. 486].

Обычно основными действующими элементами вебкам являются: вебкам-модель – лицо, оказывающее онлайн-услуги интимного содержания с целью получения прибыли; клиент – пользователь услуг вебкам-модели; вебкам-студия – организация, в компетентности которой находятся: поиск вебкам-моделей, предоставление помещения для видеотрансляции и специализированного оборудования, обеспечение минимального риска идентификации личности вебкам-моделей (блокировка работы программ захвата изображения, шифрование трафика и др.); специальные сайты вебкама; электронные платежные системы, обеспечивающие оплату услуг.

Кроме того, современные информационные технологии дают возможность организовать видеосвязь между моделью и клиентом на основе конфиденциальности. Считается, что это основное условие в анализируемой индустрии, которое переживает эксцесс своего развития, так как в настоящее время достаточно большая аудитория способна онлайн потреблять разнохарактерный интимный контент. Социологи утверждают, что такие онлайн-трансляции сильно влияют на человека, так как дают возможность реализации девиантным формам воздействия друг на друга, искажая истинные социальные связи. Пользователь как бы погружается в особую среду с созданным для него продуктом, где увеличивается психологический контакт с моделью. Все это негативно влияет на общественную нравственность, и прежде всего, на психику несовершеннолетних лиц, которые без проблем могут воспользоваться вебкамом (по причине открытости контента), скрывая данные о себе через VPN-технологии. Как только несовершеннолетнее лицо обращается к анализируемым услугам, начинается развращение

неокрепшей психики, что в будущем затрудняет процессы социализации, определения правильных представлений о добре и зле, о жизни в целом.

Кроме того, нравственная, социальная обусловленность запрета вебкам контента сопряжена с быстротой, простотой производства, распространения и его потребления. Самое главное, что на такой контент существует повышенный спрос. Доступность пользователей при получении интимных услуг через Интернет, анонимность влечет за собой демографические проблемы, так как рождаемость снижается; молодежь не видит смысла в знакомствах, общении, создании семьи. Когда человек обращается единично к онлайн-услугам интимного характера, чтобы получить новый опыт в общении, и когда такое общение становится нормой, приводя к извращенным желаниям.

Впрочем, нельзя также забывать об угрозах, при которых дети и подростки сами становятся жертвами сексуального насилия при трансляциях.

Указанные выше угрозы – самые распространенные на данный момент, но не исчерпывающие.

Очевидно, что одним из наиболее эффективных методов противодействия криминальной вебкам-индустрии остается правовой метод.

Контроль со стороны общества посредством назначения уголовно-правовых запретов в области общественной нравственности – это не новшество для законодательства России. С учетом таких положений сегодня приходится криминализовать гибридные формы совершения преступлений путем изменения подхода к анализу норм уголовного права.

На данный момент в России практика работы вебкам не урегулирована в рамках норм уголовного или какого-то другого законодательства. Трудность в плане квалификации подобных деяний обуславливается тем, что применяются средства анонимности в Интернете, а также инструменты онлайн-трансляций, что не предполагает создания предмета преступления: порнографических материалов или предметов, однако оборот и изготовление такого контента онлайн все же осуществляется [3, с. 78]. Как было указано выше, вебкам-студия обладает значимым функционалом, который обосновывает сходство деятельности руководящего звена в индустрии вебкам с деятельностью при организации проституции. Анализируя позиции правоведов, следует констатировать, что указанное сходство требует уголовно-правового регулирования путем дополнения Уголовного кодекса Российской Федерации новой нормой следующего содержания [3, с. 79]: статья 242.3 Уголовного кодекса Российской Федерации «Организация онлайн-услуг интимного (эротического или порнографического) характера посредством специальных онлайн-площадок в сети Интернет»:

1. Организация публичной онлайн-демонстрации материалов интимного (эротического или порнографического) характера, а равно систематическое предоставление помещений для оказания онлайн-услуг интимного (эротического или порнографического) характера посредством специальных онлайн-площадок в сети Интернет наказываются … ;

2. Те же деяния, совершенные с использованием лиц, не достигших четырнадцатилетнего возраста, наказываются … .

Известно, что вебкам-модель может работать в вебкам-студии, которая обеспечивает не только техническую базу, но и материальную стабильную поддержку, или на индивидуальной основе. Индивидуальная работа модели не дает возможность привлечь ее к ответственности по ст. 242.3 Уголовного кодекса Российской Федерации, что делает необходимым дальнейшую корректировку правовых норм.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.02.2024) // СПС «КонсультантПлюс».
2. Берсенев Е.В. Отношение уголовного закона Российской Федерации к явлению «вебкам» // Вопросы российской юстиции. – 2021. – № 15. – С. 485–491.
3. Борисенко А.В. Человеческий фактор в системе кибербезопасности // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 10-й Всероссийской научно-практической конференции. – Белгород, 2023. С. 27–31.
4. Куфлева В.Н., Литовченко А.И. Вебкам-индустрия – новая угроза общественной нравственности // Общество: политика, экономика, право. – 2022. – № 7 (108). – С. 75–81.

ПРИМЕНЕНИЕ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В ОБУЧЕНИИ СОТРУДНИКОВ ПОЛИЦИИ ТАКТИКЕ ВЕДЕНИЯ ПЕРЕГОВОРОВ С ПРЕСТУПНИКАМИ

Захаров Д.С.,
Огурцова К.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в данной научной статье рассматривается вопрос применения виртуальной реальности в обучении сотрудников полиции тактике ведения переговоров с преступниками. Актуальность темы обусловлена необходимостью повышения профессиональной подготовки работников правоохранительных органов с учетом активной цифровизации информационного пространства и постоянным развитием современных технологий. Авторы обращаются к порядку проведения переговоров с преступниками в реальной ситуации, а также анализируют преимущества внедрения VR-технологий в данный процесс. Также в статье также приводится зарубежный опыт использования виртуальной реальности в образовательной деятельности полицейских.

Ключевые слова: виртуальная реальность, тактика ведения переговоров, сотрудники полиции, преступники, стрессовые ситуации, симулятор.

APPLICATION OF VIRTUAL REALITY IN TRAINING POLICE EMPLOYEES IN NEGOTIATION TACTICS WITH CRIMINALS

Zakharov D.S.,
Ogurtsova K.A.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: this scientific article examines the issue of using virtual reality in training police officers in negotiation tactics with criminals. The relevance of the topic is due to the need to improve the professional training of law enforcement officers, taking into account the active digitalization of the information space and the constant development of modern technologies. The author addresses the procedure for conducting negotiations with criminals in a real situation, and also analyzes the advantages of introducing VR technologies into this process. The article also provides foreign experience in the use of virtual reality in the educational activities of police officers.

Keywords: virtual reality, negotiation tactics, police officers, criminals, stressful situations, simulator.

В современных условиях правоохранительные органы ежедневно сталкиваются с вызовами, требующими использования инновационных технологий для подготовки высококвалифицированных специалистов. Так, одной из актуальных задач, для реализации которой необходимо применение информационных ресурсов, является обучение сотрудников полиции тактике ведения переговоров с преступниками в целях обеспечения общественной безопасности и охраны общественного порядка.

Стоит отметить, что переговоры представляют собой способ организации диалога с преступником с целью предотвращения совершения им дальнейших противоправных действий [1, с. 833–834]. Так, в начале взаимодействия происходит установление первичного контакта сотрудника полиции с преступным лицом: изучение обстоятельств конкретной ситуации или дела в целом, выявление риска проявления негативного поведения со стороны виновного лица и др. Как правило, на данной стадии переговоров сотрудник правоохранительных органов стремится достичь принятия преступником требований прекратить противоправное поведение, а также старается узнать цели, задачи и особенности реализации незаконной деятельности. В свою очередь, виновное лицо тоже может выдвинуть некие условия. При этом, как показывает практика, оно отказывается выполнять законные распоряжения сотрудников полиции.

Кроме того, многие преступники могут оказывать психологическое давление, тем самым усугубляя ситуацию, делая ее более стрессовой и напряженной [2, с. 144]. Таким образом, переговоры представляют собой не просто ведение диалога с виновным лицом, а сложный последовательный процесс в оперативно-тактической деятельности, требующий от сотрудников полиции определенной подготовки.

В настоящее время для обучения профессиональных служащих тактике ведения переговоров с преступниками, как правило, проводятся лекционные и семинарские занятия, что не всегда в полной мере позволяет воссоздать реальные ситуации и продемонстрировать новым сотрудникам выполнение конкретных действий на практике. В связи с этим использование технологий виртуальной реальности, которые нашли широкое применение в современном мире, позволят модернизировать образовательный процесс и повысить уровень профессиональной подготовки сотрудников полиции.

Также, стоит отметить, что в настоящее время отсутствует нормативное закрепление рассматриваемого вопроса. В связи с этим при проведении переговоров должностное лицо либо использует предыдущий опыт, либо действует ситуативно [3, с. 197–198]. Так как тактика проведения рассматриваемой части оперативной деятельности интуитивно в большинстве случаев не является эффективной, обучение сотрудников действиям в различных ситуациях просто необходимо (в том числе при использовании инновационных информационных технологий). Так, благодаря VR-моделям могут быть разработаны максимально приближенные к реальности сценарии, что позволит работникам правоохранительных органов практиковаться в принятии решений и развивать навыки коммуникации и противодействия стрессовым ситуациям в цифровой среде.

Стоит отметить, что обучение сотрудников полиции тактике ведения переговоров с помощью VR-технологий способствует снижению рисков для здоровья, которые могут возникнуть при неадекватном поведении преступника в условиях реальных тренировок [4, с. 227–228]. Применение специального оборудования способствует полному погружению в виртуальное цифровое пространство, не ухудшая уровень подготовки. Немаловажно то, что VR-модели позволяют адаптировать сценарии и уровень их сложности под определенного обучающегося, тем самым способствуя более эффективному усвоению материала.

Кроме того, виртуальная среда обучения позволяет производить повтор различных ситуаций столько раз, сколько необходимо конкретному сотруднику для развития его профессиональных качеств. При повторении уже известной ситуации, сотрудник полиции способен лучше в ней ориентироваться, тем самым демонстрируя более высокий уровень своей подготовленности.

Необходимость внедрения виртуальной реальности в обучение сотрудников полиции обусловлена положительным опытом зарубежных стран. Например, в США компания Axon разработала симулятор, позволяющий внедрить в образовательный процесс должностных лиц возможности искусственного интеллекта [5]. Так, представителями данной организации было сформировано реалистичное виртуальное пространство со своими специальными персонажами. В рамках различных сценариев данные герои демонстрируют реакции на слова и действия своего оппонента по взаимодействию. Кроме того, возможности искусственного интеллекта обеспечивают естественное и неожиданное поведение преступников, что придает ситуациям еще большую реалистичность. Как правило, персонажи симулятора демонстрируют негативные эмоции, подвергая испытуемого воздействию стресса и иных психологических трудностей. Таким образом, данная программа учит сотрудника справляться со своим

стрессом, что позволяет ему строить грамотный диалог с собеседником и корректно отвечать на любые провокации. Исследования показали, что благодаря работе на симуляторе люди хорошо запоминают нужную модель поведения, что способствует удачному ведению переговоров в реальности.

В заключение стоит отметить, что внедрение искусственного интеллекта в деятельность правоохранительных органов может существенно поднять уровень профессионализма сотрудников, а также будет способствовать более эффективному решению сложных вопросов, касающихся взаимодействия с гражданами. Действительно, воспроизведение реальных ситуаций, которые могут возникнуть при проведении переговоров, на VR-симуляторах может помочь сотруднику проанализировать поведение преступников в специально выстроенном пространстве, а также оценить грамотность и результативность собственного поведения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Теория оперативно-разыскной деятельности / Ю.С. Блинов, О.А. Вагин, А.С. Вандышев [и др.]. – Москва: Инфра-М, 2006. – С. 832–837.

2. Никитина Л.Н., Смирнова М.И. Психолого-педагогические аспекты переговорной деятельности сотрудников органов внутренних дел // Проблемы современного педагогического образования. – 2022. – № 76-2. – С. 143–146.

3. Вахнина В.В., Стенюшкина Э.А. К вопросу ведения переговоров сотрудниками органов внутренних дел // Академическая мысль. – 2022. – № 2(19). – С. 195–200.

4. Внедрение облачных технологий в образовательный процесс образовательных организаций системы МВД России / А.Н. Прокопенко, П.Н. Жукова., С.Е. Савотченко [и др.]: учебно-методическое пособие. – Белгород, 2017.

5. Никитина Л.Н. Психологические аспекты ведения переговоров сотрудниками органов внутренних дел // Проблемы современного педагогического образования. – 2023. – № 80-1. – С. 225–228.

6. Axon VR Training/Axon [Электронный ресурс]. – URL: https://www.axon.com/products/vr (дата обращения 19.04.2024).

7. Худяков В.В., Ермакова А.С. Применение информационно-телекоммуникационных технологий при реализации образовательных программ высшего образования / Информационные технологии в системе военного образования России: проблемы и пути решения: сборник научных статей Всероссийской научно-практической конференции, Саратов, 20 декабря 2022 года. – Саратов: Саратовский военный ордена Жукова Краснознаменный институт войск национальной гвардии Российской Федерации, 2023. – С. 116–121.

МАШИННОЕ ОБУЧЕНИЕ КАК ИННОВАЦИОННОЕ СРЕДСТВО РАЗВИТИЯ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Иванов И.П.,
кандидат педагогических наук, доцент;
Епифанцева В.А.
(Краснодарский университет МВД России)

Аннотация: в статье рассматриваются возможности машинного обучения и его роль в персонализации процесса обучения. Приведены примеры использования обучающих информационных платформ. Авторы отмечают, что эти технологии уже нашли свое применение в других науках, например широко используются при изучении математики. Технологии МО могут способствовать демократизации доступа к качественному образованию, устраняя географические и социальные барьеры. Введение адаптивных систем обучения способно радикально изменить подход к обучению, делая его более эффективным и инклюзивным. Дальнейшее интегрирование МО в образовательные платформы несомненно увеличит эффективность обучения.

Ключевые слова: машинное обучение, образовательная среда, искусственный интеллект, персонализация обучения, адаптивные системы обучения, большие данные, виртуальная реальность.

MACHINE LEARNING AS AN INNOVATIVE MEANS OF DEVELOPING THE EDUCATIONAL ENVIRONMENT

Ivanov I.P.,
Candidate of Pedagogical Sciences, Associate Professor;
Epifantseva V.A.
(Krasnodar University of the Ministry of the Interior of Russia)

Abstract: the article discusses the possibilities of machine learning and its role in personalizing the learning process. Examples of the use of educational information platforms are given. The authors note that these technologies have already found their application in other sciences, for example, they are widely used in the study of mathematics. Machine learning technologies can help democratize access to quality education by removing geographical and social barriers. The introduction of adaptive learning systems can radically change the approach to learning, making it more effective and inclusive. Further integration of machine learning into educational platforms will undoubtedly increase the effectiveness of training.

Keywords: machine learning, educational environment, artificial intelligence, personalization of learning, adaptive learning systems, big data, virtual reality.

Машинное обучение (далее – МО) – это подраздел искусственного интеллекта (далее – ИИ), который фокусируется на разработке алгоритмов, позволяющих компьютерным программам обучаться на основе данных и строить прогнозы или принимать решения без явного программирования. В последние годы благодаря увеличению объемов данных и развитию вычислительных технологий машинное обучение стало неотъемлемой частью многих индустрий: – экономики, науки, здравоохранения, транспорта и многих других сферы жизнедеятельности человека.

МО применяется в самых разнообразных областях – от автоматического распознавания речи и обработки естественного языка до предсказательной аналитики и управления автономными транспортными средствами. В образовании машинное обучение начинает играть ключевую роль при персонализации учебного процесса, предоставляя преподавателю и обучающимся инструменты для создания персонализированных образовательных материалов. Данные системы могут анализировать успеваемость обучающихся в реальном времени и предлагать рекомендации для улучшения результатов.

Основной целью статьи является исследование возможностей и применения машинного обучения в рамках развития образовательной среды. В данной статье рассказано, как МО может трансформировать традиционные подходы к обучению и администрированию в образовательных учреждениях.

Задачами статьи являются:

– анализ текущих примеров успешного внедрения МО в образовательные процессы;

– оценка потенциалов и вызовов, связанных с интеграцией МО в образование;

– предложение направлений для будущих исследований и разработок в данной области.

Поставленные цели и задачи позволят выделить возможности детального рассмотрения механизмов машинного обучения и их воздействия на образовательную сферу.

Теоретические основы машинного обучения

Машинное обучение делется на три основных типа в зависимости от характера обучения и входных данных:

1. Обучение с учителем (Supervised Learning) используется, когда есть размеченные данные. Цель данного типа обучения состоит в том, чтобы найти функцию, которая наилучшим образом связывает входные данные с выходными метками на основе регрессии и классификации.

2. Обучение без учителя (Unsupervised Learning). В данном случае происходит работа с неразмеченными данными. Итог обучения заключается в выявлении скрытых структур в данных.

3. Обучение с подкреплением (Reinforcement Learning). В этом случае алгоритм самообучается, принимая решения из последовательностей действий и наблюдений, получая награды или наказания. Используется для автоматического принятия решений.

Важные модели и алгоритмы

1. Нейронные сети: основаны на математических моделях и функционируют аналогично человеческому мозгу. Применимы в задачах, где необходимо обрабатывать большие объемы данных и распознавать сложные паттерны. Нейронные сети используются для создания адаптивных обучающих систем, которые модифицируют учебный контент в соответствии с потребностями и возможностями обучающегося.

2. Решающие деревья: алгоритмы, которые строят модели принятия решений в форме дерева. Широко используются в статистическом анализе и машинном обучении для прогнозирования. Применяются для анализа успеваемости обучающихся, позволяя преподавателям видеть, какие факторы влияют лучше на учебный процесс.

3. Алгоритмы кластеризации, используются для группировки набора объектов так, чтобы объекты в одной группе (или кластере) были более похожи (в одном или нескольких смыслах) друг на друга, чем на объекты в других группах. Алгоритмы кластеризации могут быть использованы для группировки обучающихся по уровню знаний для более эффективного подбора групп и программ обучения.

Перечисленные методы и модели машинного обучения позволяют создавать более гибкие и эффективные образовательные системы, адаптированные под конкретные потребности каждого обучаемого, что способствует более эффективному усвоению знаний, развитию навыков и повышению общего уровня образования в целом.

Применение машинного обучения в образовании

Машинное обучение играет ключевую роль в адаптации учебных материалов и методик для индивидуальных нужд каждого обучающегося. Системы, использующие машинное обучение, могут анализировать прошлую успеваемость, стили обучения, предпочтения, чтобы предложить наиболее подходящие учебные материалы. Это не только повышает эффективность обучения, но и увеличивает мотивацию обучающихся.

Машинное обучение также применяется для автоматизации рутинных административных задач в образовательных учреждениях. Это включает в себя учет успеваемости, планирование расписания, а также организацию и проведение тестирований. Применение МО в этом направлении помогает сократить время на обработку данных и повысить точность учета информации.

С появлением машинного обучения обучающие платформы становятся более интерактивными. Использование игровых элементов и система наград способствует увеличению вовлеченности обучающихся в учебный процесс. Кроме того, такие платформы предоставляют обратную связь в реальном времени, что позволяет обучающимся узнать свои ошибки и немедленно работать над их исправлением.

Один из ярких примеров внедрения машинного обучения в образование – это система Khan Academy, которая использует данные для персонализации обучения. Платформа анализирует ответы обучающихся для определения их

сильных и слабых сторон, а затем адаптирует учебные материалы для максимальной эффективности обучения. Данная система разрабатывает обучающие материалы по всем направлениям, но по информатике пока ограничивается методами шифрования. Платформа содержит познавательные материалы, которые вызывают интерес из-за простоты интерпретации и восприятия.

Другой пример – это платформа Coursera, которая использует машинное обучение для создания адаптивных тестов, что позволяет более точно оценить знания обучающихся и предложить им дополнительные материалы для изучения в зависимости от их потребностей.

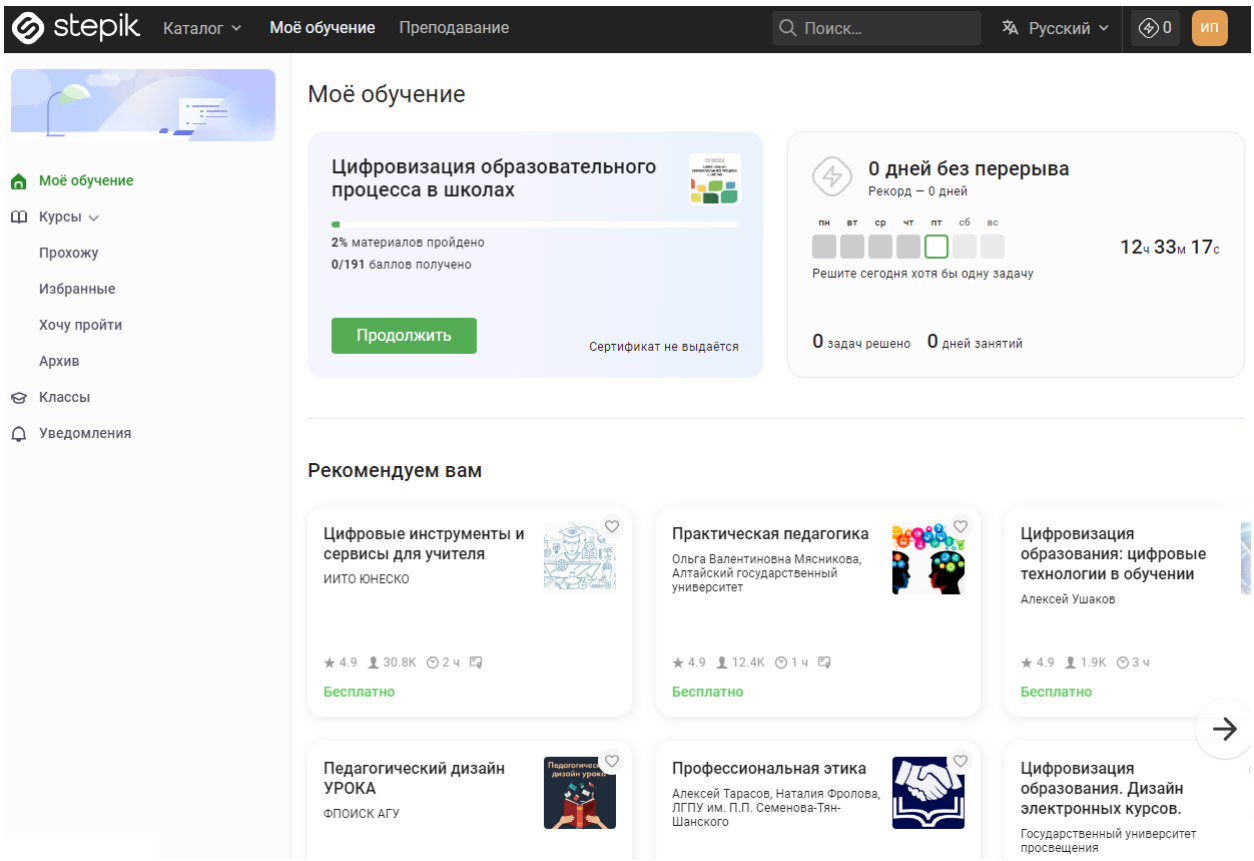


Рисунок 1. Stepik – образовательная платформа и конструктор онлайн-курсов

Эти примеры демонстрируют, как машинное обучение может радикально трансформировать традиционные методы обучения и управления образовательным процессом, делая его более персонализированным и эффективным.

Вызовы и ограничения машинного обучения в образовании

Машинное обучение зависит от достоверности и объема входных данных. Если данные неточные или предвзятые, это может привести к ошибочным выводам и рекомендациям. В образовательной сфере данный факт негативно скажется на обучении и оценке обучающихся. Сбор и анализ больших объемов данных об обучающихся ставит под угрозу их личную приватную информацию о поведении или успеваемости, но, с другой стороны, позволяет верно квалифицировать разработку обучающего материала.

В настоящее время процесс интеграции современного программного обеспечения в существующие образовательные системы по–прежнему сложен по двум причинам:

1. Технологические препятствия. Многие образовательные организации работают на устаревшем оборудовании, что затрудняет внедрение новейших технологий машинного обучения.

2. Подготовка преподавателей. Преподавателям необходимо приобретать и совершенствовать дополнительные знания и навыки для эффективного использования систем на базе ИИ. Для реализации данного направления требуются временные и/или финансовые вложения в обучение и профессиональное развитие.

Во время применения искусственного интеллекта в образовании возникают этические вопросы. Существует риск, что алгоритмы могут проявлять предвзятость против определенных групп обучающихся, что может усугубить уже существующие неравенства. Внедрение ИИ в образовательные процессы должно сопровождаться обеспечением обучающихся возможностью выбора и контроля над тем, как их данные используются. Кроме этого, существует опасность чрезмерной зависимости от технологических решений в образовании, что может ухудшить качество образования при технических сбоях или неадекватном программном обеспечении. Реализация решений в данном направлении должна приниматься преподавателем совместно с обучающимися для выработки верных стратегий эффективного и этичного использования машинного обучения в образовательном процессе.

Прогнозируя развитие современных информационных технологий, основывающихся на применении машинного обучения и оказываемого влияния на образовательный процесс, можно предположить, что для адаптивного обучения необходимо разрабатывать полностью персонализированные учебные планы, подстраивающиеся под уникальные потребности каждого обучающегося.

Продвижения в области аналитики больших данных позволят образовательным учреждениям эффективнее оценивать и оптимизировать учебные процессы.

Технологии VR (виртуальной реальности) и AR (дополненной реальности) будут интегрироваться в обучающие программы для приобретения виртуального опыта обучения.

Разработка нейроадаптивных систем, поможет синхронизироваться с нейронной активностью обучающихся, чтобы оптимизировать время и методы обучения в соответствии с их психологическими и физическими состояниями.

Продвинутые чат-боты на основе искусственного интеллекта смогут оказывать помощь обучающимся круглосуточно, отвечая на возникающие вопросы и предоставляя настраиваемые объяснения сложных концепций.

Исследования в области педагогической эффективности ИИ должны сосредоточиться на проблеме наилучшего внедрения ИИ в учебные программы, чтобы максимизировать педагогическую ценность и избежать потенциальных рисков.

Таким образом, будущее машинного обучения в образовании обещает быть революционным, предоставляя новые возможности для персонализации обучения и улучшения образовательных результатов на глобальном уровне.

Машинное обучение уже демонстрирует значительные успехи в трансформации образовательных процессов. Применение алгоритмов МО позволяет адаптировать учебные материалы под индивидуальные потребности обучающихся, предлагая персонализированные учебные пути и методы оценки. Благодаря анализу больших данных, системы МО способны предсказывать учебные трудности обучающихся и предлагать корректирующие меры до того, как проблемы станут критичными, что существенно повышает качество и доступность обучения.

Перспективы использования МО в образовании остаются весьма обнадеживающими. Технологии МО могут способствовать демократизации доступа к качественному образованию, устраняя географические и социальные барьеры. Введение адаптивных систем обучения способно радикально изменить подход к обучению, делая его более эффективным и инклюзивным. Дальнейшее интегрирование МО в образовательные платформы, несомненно, увеличит эффективность обучения и позволит образовательным заведениям лучше соответствовать требованиям рынка труда.

Машинное обучение, безусловно, продолжит оказывать значительное влияние на развитие образовательной среды, делая ее более адаптивной, эффективной и доступной для всех слоев населения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галаев А.Х. Технологии и наставничество: новые горизонты и возможности / Технопарк универсальных педагогических компетенций: материалы III Всерос. науч.-практ. конф. (Чебоксары, 15 декабря 2023 г.). – Чебоксары: Среда, 2023. – С. 125–127.

2. Савенко А.Г., Кукалев Н.А., Савенко А.Г. Виртуальная реальность как способ получения и доставки учебного контента / Высшее техническое образование: проблемы и пути развития: материалы IX Междунар. науч.-метод. конф., Минск, 1–2 ноября 2018 г. – Минск: БГУИР, 2018. – С. 394–397.

3. Константинова Л.С. Искусственный интеллект в образовании: перспективы и вызовы. – Новосибирск: Наука Сибири, 2021. – С. 73–74.

4. Колыхматов В.И. Профессиональное развитие педагога в условиях цифровизации образования: учебно-методическое пособие. – Санкт-Петербург: ЛОИРО, 2020. – 135 с.

5. Yusov K. Best Machine Learning Applications with Examples [Электронный ресурс]. – URL: https://jelvix.com/blog/machine-learning-use-cases, свободный (дата обращения: 25.04.2024).

6. Борисенко А.В. Особенности использования программного интерфейса приложения / Математические методы и информационно-технические средства: материалы XIX Международной научно-практической конференции. – Краснодар, 2023. С. 33–36.

7. The Role of AI and Machine Learning in Modern Education [Электронный ресурс]. – URL: https://www.coursera.org/lecture/machine-learning-role-education, свободный (дата обращения: 25.04.2024).

ПОДГОТОВКА СОТРУДНИКОВ МВД РОССИИ В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ивануха И.С.
(Омская академия МВД России)

Аннотация: анализ ситуации с преступлениями, совершаемыми с применением информационных технологий, в современном обществе. Постановка приоритетных задач по обучение и повышению квалификации сотрудников, способных раскрывать преступления совершаемыми с применением информационных технологий.

Ключевые слова: киберпреступность, кибербезопасность, информационные технологии, обучение, повышению квалификации.

TRAINING OF EMPLOYEES OF THE MINISTRY OF INTERNAL AFFAIRS IN THE FIGHT AGAINST CRIMES IN THE FIELD OF INFORMATION TECHNOLOGI

Ivanukha I.S.
(Omsk Academy of the Ministry of the Interior of Russia)

Abstract: analysis of the situation with crimes committed with the use of information technologies in modern society. Setting priority tasks for training and advanced training of employees capable of solving crimes committed using information technology.

Keywords: cybercrime, cybersecurity, information technology, training, advanced training.

Информационные (цифровые) технологии оказывают существенное влияние на общество и государство во всем мире. В современном обществе повседневные транзакции осуществляются с помощью различных интернет-сервисов, используются системы онлайн-платежей, а государственные услуги все чаще предоставляются в электронном виде.

Стратегией развития информационного общества Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, было определено, что в последние годы глобальная цифровизация стала одной из главных тенденций в современной жизни российского общества.

Стоит отметить, что такие преступления, как хищения, мошенничество, преступления, связанные с незаконным оборотом наркотиков, а также преступные посягательства на безопасность и государственную власть сегодня в боль-

шинстве случаев совершаются дистанционно с использованием информационных технологий.

Согласно статистическим данным, приведенным 22 мая 2023 года руководителем Криминального центра Следственного комитета при прокуратуре Российской Федерации Темираном Салиховым, в 2022 году в России было совершено около 510 000 преступлений с использованием информационных технологий против 10 000 в 2014 году. Таким образом, количество преступлений в сфере информационных технологий увеличилось более чем в 50 раз. По его словам, в большинстве случаев киберпреступники используют искусственный интеллект для создания фишинговых сайтов и генерирования текста, похожего на сообщения от определенных организаций или группировок.

20 марта 2023 года Президент Российской Федерации Владимир Путин сообщил на расширенном заседании МВД, что в 2022 году преступления в сфере информационных технологий составим четверть всех преступлений в России, превысив 500 тыс. случаев. Глава государства добавил, что борьба с преступлениями, совершаемыми с использованием информационных технологий, является одним из безусловных приоритетов Министерства внутренних дел Российской Федерации.

Развитие информационных технологий сопровождается ростом ИТ-преступности (киберпреступности), а причиняемый ею имущественный ущерб превышает ущерб от традиционной преступности.

Перед правоохранительными органами стоит непростая задача раскрытия новых видов преступлений, совершаемых в киберпространстве.

Система органов внутренних дел Российской Федерации занимает центральное место в борьбе с киберпреступностью и обеспечивает выявление, раскрытие и расследование этих преступлений. Для выполнения поставленых задач сотрудники службы предварительного расследования, оперативного управления и уголовного розыска должны не только «идти в ногу со временем», но и «быть на шаг впереди»: обладать современными знаниями, навыками и умениями для расследования преступлений, совершенных с применением информационных технологий (например, знать, как совершаются такие преступления, уметь собирать инкриминирующую информацию быстрее, чем преступник успеет ее сфальсифицировать или полностью удалить).

Перед подразделениями Министерства внутренних дел Российской Федерации, работающими над раскрытием преступлений, совершенных с применением информационных технологий, стоят следующие основные задачи:

1) создание системы электронного документирования правонарушителей и преступлений, включая создание единого каталога и системы классификации;

2) обучение сотрудников «кибертехнологиям» на специальных курсах для сотрудников полиции;

3) объединение в общую сеть подразделений полиции, судов, исправительных учреждений и совершенствование информационных технологий;

4) соблюдение прав граждан, неприкосновенности частной жизни и кибербезопасности.

Мы считаем, что это одна из основных задач, стоящих перед государством.

В условиях роста преступности в сфере информационных технологий правоохранительным органам необходимо наращивать свой технологический потенциал и создавать специализированные подразделения. Однако существуют и факторы, препятствующие оперативному расследованию таких преступлений.

Сегодня, например, высокая скорость передачи информации среди подразделений министерства внутренних дел Российской Федерации и банками, операторами мобильной связи и провайдерами Интернета может весьма сильно влиять на эффективность расследования такого рода преступлений и своевременное установление личности преступников. В наши дни механизмы получения информации (например, о движении средств на банковском счете мошенника, телефонных соединениях и т.д.) чрезвычайно сложны для следователей, расследующих кражи из удаленных мест, а в случае многоэтапных схем хищений расследование может затянуться на несколько месяцев. При раскрытии дел и проведении расследований в современной цифровой и быстро меняющейся среде правоохранительные органы должны получить доступ к необходимой им информации как можно быстрее, желательно в режиме онлайн. Например, сегодня центральному банку требуется три дня, чтобы обнаружить и закрыть так называемый фишинговый сайт, но этого все равно недостаточно. Для своевременного пресечения незаконной деятельности мошенников обмен информацией и реагирование должны быть чрезвычайно оперативными.

Современное общество и государство все чаще сталкивается с преступлениями, совершенными с использованием информационных технологий, которые остаются нераскрытыми. Этим обусловлена актуальная потребность в специалистах, умеющих обращаться с современным оборудованием, вырабатывать и использовать новейшие технологические решения. Другим приоритетом является необходимость подготовки техников, инженеров и ИТ-специалистов, способных развивать информационное общество и государство. Также необходима подготовка и переподготовка сотрудников правоохранительных органов, которые в будущем смогут использовать свои знания для предупреждения, контроля, раскрытия и расследования преступлений в области информационных технологий.

На заседании коллегии Министерства внутренних дел Российской Федерации 1 ноября 2019 года были приняты следующие решения по организации работы по выявлению, раскрытию и расследованию преступлений, связанных с использованием современных информационных технологий:

1) создание структурного подразделения, специализирующегося на борьбе с преступлениями, связанными с использованием информационных технологий;

2) расширение штатной численности подразделения Бюро специальных технических технических мероприятий МВД России;

3) создание информационно-поисковой базы данных;

4) создание в МВД России нового подразделения по борьбе с преступлениями с использованием информационных технологий;

5) подготовка кадров для вновь создаваемых подразделений МВД России.

Таким образом, одной из основных задач, стоящих в настоящее время перед правоохранительными органами, является необходимость их реформирования и подготовки компетентных кадров для «полиции будущего». Речь идет не только о переподготовке кадров, и подготовке специалистов, способных расследовать преступления с использованием информационных технологий, но и о повышении уровня знаний, навыков и компетенции действующих сотрудников полиции.

При этом меры по борьбе с киберпреступностью иногда требуют привлечения экспертов различных научных специальностей. Однако для достижения поставленных целей сотрудникам полиции в раскрытии и расследовании преступлений необходимо обладать знаниями и навыками, позволяющими использовать новейшие достижения науки и техники.

Конечно же, такая подготовка требует определенного подхода и должна готовить специалистов, способных принимать участие в раскрытии и расследовании преступлений, совершаемых с помощью информационных технологий.

Основная задача, стоящая перед учебными заведениями, – обеспечить большинство сотрудников МВД России необходимыми знаниями, навыками и умениями. Не разрушая базовую структуру системы образования, вузы модернизируются по трем основным направлениям: разработка и внедрение методик обучения, позволяющих вооружить сотрудников внутренней службы необходимыми знаниями в период обучения в образовательной организации; повышение квалификации профессорско-преподавательского состава образовательной организации; повышение квалификации сотрудников образовательных организаций. Стоит отметить, что все эти направления связаны друг с другом.

Одним из ведущих учебных вузов страны является Омская академия МВД России, имеющая значительный опыт подготовки кадров по борьбе с преступлениями, совершаемыми с применением информационных технологий.

Образовательная организация ежегодно направляет сотрудников академии из числа профессорско-преподавательского состава, среди которых есть как юристы, так и инженеры, на курсы повышения квалификации и стажировку в оперативные подразделения Министерства внутренних дел Российской Федерации, занимающихся раскрытием преступлений, совершаемых с применением информационных технологий.

В Омской академии МВД России в программу обучения курсантов и слушателей по первоначальной подготовке сотрудников органов внутренних дел введено специальное направление «Основы кибербезопасности», способствующее формированию соответствующих компетенций, предусмотренных национальными стандартами.

Будущие следователи, дознаватели и оперативники также приобретают навыки выявления, раскрытия и расследования преступлений, совершаемые с применением информационных технологий. Учебные полигоны действуют на всех учебных корпусах академии, и одной из основных задач является формирование навыков и умений по изъятию информации, содержащейся на электронных носителях информации.

В Академии предварительного следствия практические занятия проводятся в условиях имитации банковского офиса. На этой учебной площадке будущие оперативники и следователи обучаются проведению оперативно-разыскных мероприятий, изъятию информации в электронном виде, грамотному взаимодействию с представителями организаций финансово-кредитной сферы.

Также на базе Омской академии МВД России проводится повышение квалификации действующих сотрудников органов внутренних дел, что является весьма важным направлением в подготовке сотрудников. Созданная в Омской академии многогранная инфраструктура, информационная среда, функционирующая на всех учебных площадках, позволяет проводить предварительное следствие, оперативно-разыскные мероприятия и специализированные уголовные расследования, повышая квалификацию сотрудников, работающих в различных регионах. Таким образом, одной из основных задач в борьбе с преступностью с применением информационных технологий является обучение и повышение квалификации сотрудников органов внутренних дел, способных эффективно предупреждать, выявлять, регистрировать и расследовать преступления, совершаемые с применением информационных технологий.

В процессе обучения сотрудников органов внутренних дел необходимо обеспечить их знаниями законодательства, выработать у них навыки и компетенцию применения законодательства при проведении оперативно-разыскных мероприятий. Также необходимо развивать у каждого сотрудника способность к самостоятельному обучению и постоянному совершенствованию своих профессиональных знаний, навыков и компетенции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Овчинский В.С., Жданов Ю.Н. Полиция будущего. – Москва, 2018. IRA. – 165 с.

2. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – Москва: Норма, 2017. – 528 с.

3. Калиниченко И.А. О приоритетных направлениях подготовки кадров для органов внутренних дел Российской Федерации в условиях информатизации общества // Вестник Московского университета МВД России. – 2020. – № 3. – С. 11–14.

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ МВД РОССИИ

Калашникова А.А.,
Фомичев Е.С.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматриваются вопросы эффективности применения геоинформационных систем в деятельности органов внутренних дел, так как именно они позволяют сотрудникам оптимизировать процесс использования возможностей программно-технического комплекса, повысить уровень информационно-аналитического обеспечения правоохранительной деятельности, обеспечить своевременное и действенное реагирование на возникающие угрозы общественного порядка и общественной безопасности. В связи с этим, становится актуален вопрос анализа эффективности использования геоинформационных систем в деятельности сотрудников органов внутренних дел, выявления наиболее проблемных аспектов по данной теме с дальнейшей разработкой мер по их устранению.

Ключевые слова: органы внутренних дел, геоинформационные системы, преступления, правонарушения, геоинформационные услуги, Единая система информационно-аналитического обеспечения деятельности МВД России.

APPLICATION OF GEOINFORMATION TECHNOLOGIES IN THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Kalashnikova A.A.;
Fomichev E.S.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: the author of the article considers the issues of the effectiveness of the use of geoinformation systems in the activities of internal affairs bodies, since they allow employees to optimize the process of using the capabilities of the software and hardware complex, increase the level of information and analytical support for law enforcement, ensure timely and effective response to emerging threats to public order and public safety. In this regard, the issue of analyzing the effectiveness of the use of geoinformation systems in the activities of police officers, identifying the most problematic aspects on this topic with further development of measures to eliminate them becomes relevant.

Keywords: internal affairs agencies, geoinformation systems, crimes, offenses, geoinformation services, a unified system of information and analytical support for the activities of the Ministry of Internal Affairs of Russia.

В последние годы наблюдается рост уровня преступности в Российской Федерации, что требует от правоохранительных органов разработки новых эффективных методов борьбы с ней. Особое место в такой борьбе занимают геоинформационные системы, так как в современном мире преступники стали активно использовать новые технологии и преступные схемы в сети Интернет для совершения преступлений. Поэтому деятельность сотрудников органо внутренних дел (далее – ОВД) должна соответствовать этим изменениям и обеспечивать эффективное получение информации о преступлениях и их участниках. Для противодействия современной преступности сотрудникам ОВД необходимо располагать достоверной и актуальной информацией о преступных проявлениях. Для этого им необходимо располагать современными информационными технологиями, которые позволяют сотрудникам ОВД собирать, обрабатывать и анализировать информацию более эффективно и оперативно. Для всех перечисленных целей сотрудники ОВД используют геоинформационные систем МВД России.

Сегорня применение геоинформационных технологий в системе МВД России позволяет получить ответы на ряд вопросов:

1. Что на исследуемой территории находится?
2. Какие изменения мы можем наблюдать в период с … по …?
3. Что существует в данной местности?
4. Какая взаимосвязь изменений объекта А и объекта Б?

Получение ответов на конкретные вопросы позволяет собрать необходимую информацию о местоположении на геоинформационной платформе, провести анализ такой территории и предпринять соответствующие меры по реализации целей деятельности сотрудников ОВД. Так, данная информация позволит разработать план проведения оперативно-разыскных или следственных мероприятий, смоделировать ситуацию перехвата преступников, выбрать место для организации оперативного штаба и многое другое.

Наравне с изучаемой системой в МВД России существуют и иные специальные системы, которые, в свою очередь, используются в конкретных подразделениях и решают вопросы деятельности ОВД в определенных сферах деятельности. Например, в Главном управлении по борьбе с контрабандой Государственного таможенного комитета Российской Федерации создана информационно-поисковая система «БК-ИНФОРМ» с целью информационной поддержки расследований по делам о нарушении таможенных правил, производства дознания по уголовным делам, проведения оперативно-разыскной деятельности [5]. Созданная информационно-поисковая система «БК-ИНФОРМ» имеет ряд задач, которые свойственны именно тем целях, которые реализуют сотрудники подразделений по борьбе с контрабандой.

Исследуемые системы выполняют ряд функций, которые были нами обозначены на рисунке 1. Отметим, что представленный перечень не является исчерпывающим, что связано с постоянным развитием геоинформационных систем и появлением новых возможностей применения таких систем в деятельности ОВД.

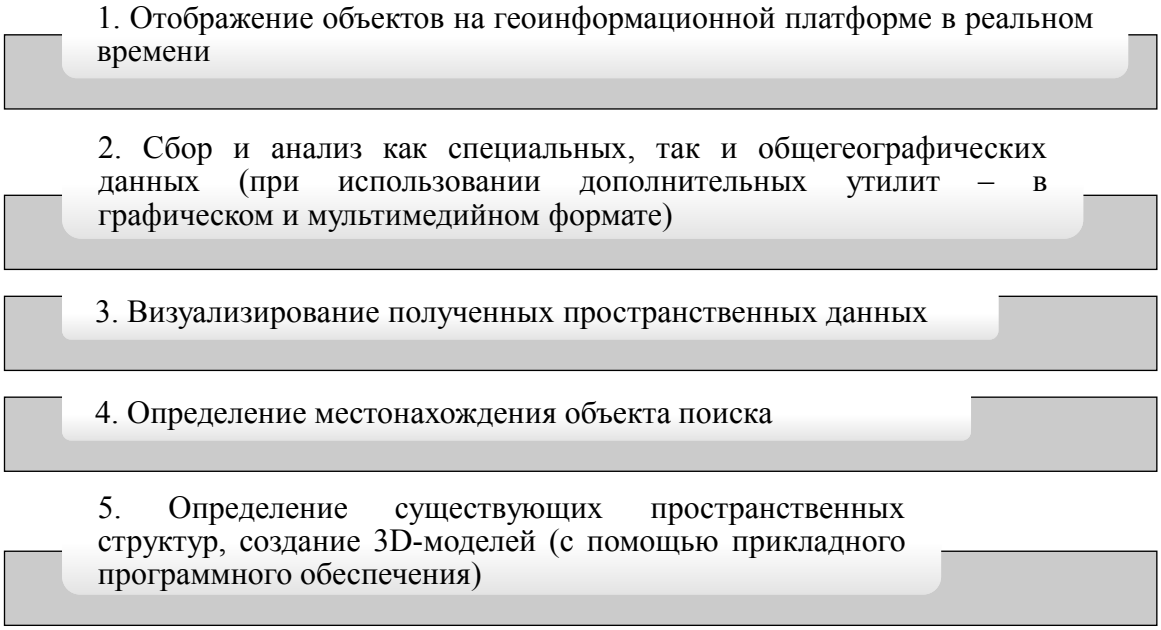


Рисунок 1. Функции геоинформационных систем ОВД

Далее отметим, что геоинформационная система ОВД основывается на следующих принципах:

1. Законности – информационное обеспечение деятельности ОВД должно осуществляться в соответствии с действующим законодательством Российской Федерации.

2. Достоверности – информация, полученная из геоинформационных систем, должна быть объективной и не содержать искажений.

3. Полноты – информация, используемая в информационном обеспечении, должна быть полной и охватывать все необходимые аспекты предмета исследования.

4. Своевременности – информация должна быть актуальной и своевременно доводиться до сотрудников ОВД.

5. Системности – информационное обеспечение деятельности ОВД должно осуществляться в рамках единой системы.

Отметим, что в целях более быстрого и качественного определения геопространственных данных, сотрудникам ОВД необходимо использовать геоинформационные системы в практической деятельности. Такие системы в свою очередь позволяют сотрудникам ОВД своевременно выявлять, предупреждать, пресекать и раскрывать преступления, а также выявлять и устанавливать лица, совершающие или совершившие преступления на определенной территории.

На данный момент в деятельности ОВД, согласно Указу Президента Российской Федерации № 638«Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации», используется только оборудование Глобальной Навигационной Спутниковой Системы (далее – ГЛОНАСС) – российской спутнико-

вой системы навигации или совмещенное ГЛОНАСС/GPS [1]. К сожалению, существует проблема недостаточного нормативного регулирования работы государственных органов и ОВД России с оборудованием ГЛОНАСС, а также отсутствуют методологические рекомендации по использованию оборудования и информации ГЛОНАСС. По нашему мнению, необходимо реализовать ряд мероприятий, направленных на создание минимальной нормативно-правовой базы использования ГЛОНАСС, так как полученную информацию сотрудники ОВД могут использовать в процессе доказывания вины преступников, в рамках проведения оперативно разыскных мероприятий и в множестве иных аспектов.

Отметим, что на сегодняшний день развитием данной системы занимается российская государственная корпорация «Роскосмос», а также ряд министерств (в том числе МВД России). В рамках разработки проекта ГЛОНАСС сотрудникам ОВД необходимо вносить предложения по методическим и правовым основам применения такой системы в деятельности ОВД. Для упрощения внедрения нововведений, создания методической основы и контроля использования системы ГЛОНАСС предлагается внедрить ее функционал в уже существующую Единую систему информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России). Такое внедрение позволит сотрудникам ОВД ограничить доступ посторонних лиц к системе ГЛОНАСС и как итог – будет организована адаптация исследуемой системы для целей деятельности сотрудников ОВД.

В заключение следует отметить, что стремительное развитие информационных технологий обусловливает появление новых возможностей и способов подготовки и совершения преступлений, поэтому вопросы, связанные с информационным обеспечением деятельности сотрудников ОВД, являются одними из ключевых и требуют особого внимания как со стороны руководства ОВД, так и со стороны руководства Российской Федерации. Отметим, что вопросы эффективности использования геоинформационных систем в деятельности ОВД становятся особо актуальны, так как именно они позволяют сотрудникам оптимизировать процесс использования возможностей программно-технического комплекса, повышать уровень информационно-аналитического обеспечения правоохранительной деятельности, обеспечивать своевременное и эффективное реагирование на возникающие угрозы общественного порядка и общественной безопасности, а также многое другое.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 17 мая 2007 г. № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации» // СПС «КонсультантПлюс».

2. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс».

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

4. Альховская А.В., Худяков В.В., Воробьева Т.И. Применение геоинформационных технологий в профессиональной деятельности сотрудников полиции // Международный журнал гуманитарных и естественных наук. – 2022. – № 3-1 (66). – С. 85–89.

5. Федосеев А.Э., Михайликов В.Л. Современные возможности анонимизации в сети Интернет / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 8-й Всероссийской научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2021. – С. 187–190.

6. Котляров Д.И. Информационные технологии оперативно-разыскной деятельности // Символ науки. – 2022. – № 12-2. – С. 66–69.

ЗАЩИТА ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОЙ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Казачкина В.С.,
Емельянова О.В.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: правоохранительные органы являются составляющей частью в структуре государственного управления, поэтому эффективность деятельности данных лиц напрямую зависит от обеспечения защиты информации, которую они используют, выполняя возложенные на них обязанности. В настоящее время информационные технологии не стоят на месте, происходит постоянное их развитие, что позволяет людям получать больше данных в сети Интернет, а также внедряться в различные сферы общества, что создает угрозу мошенничества, утечки данных, повешения количества уголовных преступлений. Так как деятельность правоохранительных органов напрямую связана с защитой прав и свобод человека и гражданина, следовательно, обеспечение защиты информации, которую они используют в своей работе, влияет на эффективность деятельности, уровень безопасности государственного управления, степень защищенности граждан, а также лиц, имеющих доступ к государственной тайне.

Ключевые слова: информация, информационная безопасность, защищенность, деятельность правоохранительных органов.

INFORMATION PROTECTION TO ENSURE EFFECTIVE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Kazachkina V.S.,
Emelyanova O.V.
(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: law enforcement agencies are an integral part of the structure of public administration, therefore the effectiveness of the activities of these individuals directly depends on ensuring the protection of the information that they use while performing their duties. Currently, information technologies do not stand still; they are constantly developing, which allows people to obtain more data on the Internet, as well as penetrate into various spheres of society, which creates the threat of fraud, data leakage, and an increase in the number of criminal offenses. Since the activities of law enforcement agencies are directly related to the protection of human and civil rights and freedoms, therefore, ensuring the protection of information that they use in their work affects the effectiveness of their activities, the level of security of public administration, the degree of protection of citizens, as well as persons with access to government secret.

Keywords: information, information security, security, activities of law enforcement agencies.

В XXI веке информационная инфраструктура достигла высокого уровня развития, появились новые средства передачи и использования информации: люди знакомятся с новыми методами реализации своих навыков и умений через сеть Интернет, правоохранительные органы могут своевременно получать актуальные сведения, необходимые для выполнения возложенных на них обязанностей. Это, конечно, положительно сказывается на показателе уровня развития государства, но вместе с тем и повышает показатели киберпреступлений: использование информации, несанкционированное ее распространение может нанести ущерб правам и свободам гражданам государства и интересам национальной безопасности.

Развитие информационных и телекоммуникационных технологий приводит к тому, что возрастает роль правоохранительных органов в части информационной безопасности. Рост цифровизации приводит к увеличению рисков утечки конфиденциальных сведений, поэтому важно обеспечить государственную службу теми средствами, которые создадут безопасность их деятельности. Прежде всего информационная безопасность – это состояние защищенности государственных органов, их интересов для более эффективного выполнения возложенных на них обязанностей, раскрытия преступных деяний, которые нарушают спокойствие граждан страны.

По данным статистики Министерства внутренних дел Российской Федерации, за январь – март 2024 года количество преступлений с использованием информационно-телекоммуникационных технологий увеличилось на 17,6% по сравнению с январем и мартом прошлого года [3]. Исходя из этого, можно сде-

лать вывод, что сейчас главной задачей правоохранительных органов является обеспечение информационной безопасности.

Угрозы информационной безопасности правоохранительных органов. Деятельность государственных служащих напрямую зависит от внешних угроз. Для того чтобы обеспечить результативность работы различных подразделений правоохранительных органов, нужно знать и учитывать угрозы, которые приходят извне, и стараться их предотвратить. Если рассматривать подобные угоры, то это прежде всего деятельность иностранных организаций, подразделений, международных преступных сообществ, использующих все средства и методы для проникновения в структуру государственного управления для завладения нужной для них информацией, для сбора сведений, раскрывающих задачи и методы деятельности, места дислокации различных подразделений.

Говоря о внутренних угрозах к ним можно отнести недостаточно компетентных лиц, которые стоят у руля защиты данных, сведений и имеют доступ к государственной тайне. Также это и нарушение сбора, обработки, использования и хранения информации, содержатся в различных банках данных для использования в раскрытии преступлений. Недостатки в нормативной базе также сказываются на обеспечении информационной безопасности. Правильный разработанный регламент использования информации и ее защиты нужен для отграничения доступа различных лиц к тем сведениям, завладение и распространение которых может негативно сказаться на государственной защите в сфере информатизации. Зачастую различные сбои программного обеспечения в информационных системах влияют на эффективность выполнения сотрудниками правоохранительных органов своих функций и обязанностей. Следовательно, такая угроза также может существовать в сфере обеспечения информационной безопасности.

Методы и средства обеспечения защиты информации в правоохранительных органах. Сталкиваясь с различными угрозами важно создать и разработать концепцию по созданию методов и средств для предотвращения угроз жизни общества. Главным таким методом является проведение комплексного контроля над выполнением нормативно-правовых актов как органами государственной власти, в том числе правоохранительными органами, так и населением России ведь при соблюдении законов, устанавливается свобода и справедливость, степень защищенности населения, происходит повышение эффективности деятельности государственного управления.

Другой метод – это совершенствование взаимодействия головных и подчиненных подразделений через телекоммуникационные связи. Оснащение программными, программно-аппаратными средствами защиты информации позволяет организовать защиту сведений, передаваемых между различными подразделениями государственного аппарата. Переход на отечественные программно-аппаратные платформы также является методом повышения информационной безопасности, поскольку отграничение зарубежных платформ позволяет снизить вмешательство иностранных фирм и организаций во внутригосударственные отношения, максимально повысить возможный уровнень обеспечения защиты информации и тем самым достичь сбалансированности системы [2]. Повы-

шение защиты информации от утечки является главной задачей, которая стоит перед правоохранительными органами. Это в том числе и использование различных систем шифрования, авторизации и аутентификации. Для того чтобы качественно применять такие средства, важно организовать подбор квалифицированных кадров при приеме на работу. Ведь зачастую ошибки, связанные с использованием конфиденциальных сведений, происходят по причине невнимательности, неквалифицированности работников. Поэтому необходимо организовать обучение сотрудников в поддержании безопасности данных [4].

Иногда киберпреступления совершаются из-за недостатка сведений, у граждан по поводу деятельности правоохранительных органов. Следовательно, еще одним методом для обеспечения информационной безопасности является повышение информирования граждан о том, чем занимаются государственные служащие, какие преступления и правонарушения совершаются в стране, какие средства применяются при расследовании противоправных деяний.

Таким образом, можно сделать вывод, что защита информации в настоящее время является главной составляющей в эффективности работы правоохранительных органов. Сведений, используемых сотрудниками различных ведомственных подразделений, позволяет сохранить секретность оперативно-разыскной деятельности, а также обеспечить защиту интересов как государства, так и граждан. Развитие инфраструктуры информационно-телекоммуникационных технологий, программного обеспечения, информационных коммуникаций повышают роль деятельности правоохранительных органов в сфере обеспечения информационной безопасности для эффективности их деятельности [1].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баторов Б.О. Некоторые проблемы нормативно-правового регулирования защиты информации в органах внутренних дел Российской Федерации и пути их разрешения // Труды Академии управления МВД России. – 2022. – № 2.

2. Завгородный Е.Н. Развитие системы обеспечения информационной безопасности в органах внутренних дел // StudNet. – 2021. – № 7.

3. Краткая характеристика состояния преступности в Российской Федерации за январь–март 2024 года [Электронный ресурс]. – URL: https://мвд.рф/reports/item/49477631/ (дата обращения: 09.04.2024).

4. Терновенко А.П. Информационная безопасность в правоохранительных органах // Аллея Науки. 2023. № 5 [Электронный ресурс]. – URL: https://alleyscience.ru (дата обращения: 09.05.2024).

5. Основы кибербезопасности в деятельности сотрудников правоохранительных органов / Прокопенко А.Н., Страхов А.А., Ковалева Е.Г. [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. – 153 с.

6. Худяков В.В., Альховская А.В. К вопросу об обеспечении кибербезопасности деятельности сотрудников полиции / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей IX Всероссийской научно-практической конференции. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2022. – С. 175–181.

О ВОЗМОЖНОСТЯХ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОВД С ЦЕЛЬЮ ПРОФИЛАКТИКИ И КОНТРОЛЯ ЗА ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ

Мельникова С.Д.,
Калашникова А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: технологии искусственного интеллекта на сегодняшний день играют важную роль в жизни социально-правового государства. Изучение вопросов использования технологий искусственного интеллекта приходится на многие сферы и области жизнедеятельности, в том числе науку и юриспруденцию. Актуальность данной темы состоит в том, что во многих странах, в частности и в России, происходит изменение системы общественных отношений за счет внедрения информационно-коммуникационных технологий, что способствует формированию отраслей и подотраслей права, и это уже получило свое название – цифровое право. Усовершенствование технологий искусственного интеллекта позволяет систематизировать расширенный поиск информации про наркотические средства, а также способствует укреплению профилактических мер для пресечения попытки употребления или внедрения противозаконных препаратов на территории нашей страны. В данной статье рассмотрены такие вопросы, как: Что из себя представляет оборот наркотических средств? Каковы тенденции развития технологий искусственного интеллекта с целью профилактики ограничения движения наркотических средств? Какие существуют возможности применения цифровых технологий для пресечения оборота наркотических средств? Проанализирован вопрос о наиболее важных направлениях регулирования технологий искусственного интеллекта, которые необходимы для профилактики и контроля за оборотом наркотических средств, а также устойчивого развития государства в целом.

Ключевые слова: технологии искусственного интеллекта, наркотики, правовое регулирование, оборот наркотических средств, информационное законодательство, государство, профилактические меры, контроль, направления развития.

ABOUT THE POSSIBILITIES OF USING INFORMATION TECHNOLOGY IN ATS FOR THE PURPOSE OF PREVENTION AND CONTROL OF DRUG TRAVEL

Melnikova S.D.;
Kalashnikova A.A.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: artificial intelligence technologies today play an important role in the life of a social and legal state. The study of the use of artificial intelligence tech-

nologies covers many spheres and areas of life, including science and law. The relevance of this topic lies in the fact that in many countries, in particular in Russia, the system of social relations is changing due to the introduction of information and communication technologies, which contributes to the formation of branches and subsectors of law and this has already received its name digital law. Improving artificial intelligence technologies makes it possible to systematize an expanded search for information about narcotic drugs, and helps to strengthen preventive measures to suppress attempts to use or introduce illegal drugs into the territory of our country. This article addresses questions, such as: What is drug trafficking? What are the trends in the development of artificial intelligence technologies for preventing restrictions on the movement of narcotic drugs? What opportunities exist for using digital technologies to curb drug trafficking? The issue of the most important areas of regulation of artificial intelligence technologies, which are necessary for the prevention and control of drug trafficking, as well as the sustainable development of the state as a whole, alsoare analyzed.

Keywords: artificial intelligence technologies, drugs, legal regulation, drug trafficking, information legislation, state, preventive measures, control, development directions.

Сегодня в нашей стране происходит ускоренное вовлечение технологий искусственного интеллекта в общественную жизнь государства. Данный процесс оказывает свое влияние почти на каждую сферу жизнедеятельности людей, будь то экономика, политика или социология, а также воздействует на все отрасли российского права, в частности на уголовное право. Это явление не обошло и юриспруденцию, так как развитие новых IT-технологий и внедрение их в повседневную жизнь требуют усовершенствования правового регулирования и соответствующего закрепления в законодательстве страны. Рассмотрим возможность использования информационных технологий в целях профилактики пресечения оборота наркотических средств на территории Российской федерации.

Что же такое оборот наркотиков, что он из себя представляет? Данное понятие представлено в Федеральном законе от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» – оборот наркотических средств, психотропных веществ – разработка, производство, изготовление, переработка, хранение, перевозка, пересылка, отпуск, реализация, распределение, приобретение, использование, ввоз на территорию Российской Федерации, вывоз с территории Российской Федерации, уничтожение наркотических средств, психотропных веществ, разрешенные и контролируемые в соответствии с законодательством Российской Федерации [1]. В свою очередь мы проанализируем процесс незаконного оборота наркотиков, который прямо противоположен вышеприведенному определению. Данный процесс заключается в скрытной, незаконной реализации наркотических средств на территории государства, без наличия на то должного разрешения.

На сегодняшний день число преступлений, связанных с незаконным оборотом наркотических средств, только увеличивается, так как большинство таких преступлений совершается посредством сети Интернет. Данное явление объясняется тем, что в информационной сети присутствуют как открытые для пользователя сведения о составе наркотических и психотропных веществ, способе их приготовления и их видов, так и присутствуют закрытые источники, содержащие сведения о покупке и продаже наркотических средств, личные сведения продавцов и их контакты. Государственной антинаркотической политикой Российской Федерации была разработана Стратегия, содержащая меры по предупреждению совершения преступлений, связанных с наркотиками. В данный перечень мер входят:

1. Осуществление совершенствования государственного управления и законодательства в сфере оборота наркотиков.
2. Создание государственной системы мониторинга наркоситуации в Российской Федерации.
3. Оптимизирование работы сотрудников правоохранительных органов для улучшения показателя раскрываемости преступлений, связанных с незаконным оборотом наркотических средств.
4. Формирование механизмов выявления потребления наркотических средст и др.

Мы живем в современном постиндустриальном мире, где информация – это и есть главное оружие, защита и нападение, а, следовательно, бороться с какими-либо правонарушениями и преступлениями необходимо также с использованием глобальной сети Интернет, поэтому для полного и всестороннего изучения вопроса незаконного оборота наркотических средств, необходимо создание информационных технологий, которые позволят систематизировать массив данных о всей системе такого оборота.

Именно для этого по Указу Президента Российской Федерации [2] была разработана и внедрена система мониторинга наркоситуации в России. Под мониторингом в данном случае следует понимать систему наблюдения за развитием ситуации в сфере оборота наркотических и психотропных веществ, а также их прекурсоров.

Процесс изучения вопроса незаконного оборота наркотиков осуществляется Государственным антинаркотическим комитетом, антинаркотическими комиссиями в субъектах Российской Федерации, а также органами исполнительной власти и общественными объединениями. Такого рода контроль осуществляется в целях определения состояния наркоситуации, выявления и пресечения преступлений в этой сфере, оценки имеющихся способов и методов раскрытия преступлений и др.

Мониторинг наркоситуации осуществляется с использованием единого банка данных и в целом предусматривает систематическое проведение исследований по установлению причин незаконного оборота наркотиков с целью пресечения таких действий и эффективной борьбы.

Помимо изучения и последующего анализа данных о состоянии оборота наркотических средств на территории Российской Федерации сотрудниками органов внутренних дел и иными подразделениями на постоянной основе должна проводиться работа на предмет обнаружения на различных сайтах и в мессенджерах подозрительной деятельности в данной сфере (вербование, сбыт, покупка, реклама и т.д.). Кроме того, анализу подлежат различные электронные платежные системы, с помощью которых производятся скрытые расчеты в сети Интернет.

Сложность проведения такого рода анализа и выявления фактов незаконного оборота наркотических средств заключается в анонимности наркоторговцев, осуществляющих свою преступную деятельность, посредством интернет ресурсов, а именно: наркоторговцами используются современные технологии, которые позволяют сбывать наркотические вещества бесконтактным способомс помощью так называемых «тайников-закладок». Кроме того, существует возможность создания интернет-магазинов посредством теневого сектора DarkNet, позволяющий в условиях анонимности совершать сделки онлайн, не раскрывая своих личных данных. Также анонимность обеспечивается за счет обезличенных криптосчетов, используемых для проведения расчетных операций. Поэтому для эффективной реализации мероприятий по пресечению незаконного оборота наркотиков сотрудники правоохранительных органов, несомненно, должны обладать специальными знаниями в сфере IT-технологий, устройств, приложений.

Профилактика и контроль со стороны органов внутренних дел в системе предупреждения незаконного оборота наркотиков имеет важное значение, поскольку данный вид деятельности направлен на устранение и нейтрализацию криминогенных факторов, способствующих совершению преступлений, а также пресечение такого рода преступлений.

Борьба с наркопреступностью является актуальным и повседневным вопросом в России. С этой целью необходимо совершенствовать имеющиеся и разрабатывать новые оперативно-тактические методы и приемы по противодействию незаконному обороту наркотиков.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» [Электронный ресурс] // СПС «КонсультантПлюс».

2. Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» (с изм. и доп.) [Электронный ресурс] // СПС «КонсультантПлюс».

3. Положение о государственной системе мониторинга наркоситуации в Российской Федерации, утвержденное постановлением Правительства Российской Федерации от 20.06.2011 № 485 [Электронный ресурс] // СПС «КонсультантПлюс».

4. Воронцов А.В., Михайлов Б.П., Хазов Е.Н. Современные проблемы организации оперативно-разыскной профилактики и пути их решения // Вестник экономической безопасности. – 2017. – № 3. – С. 137–140.

5. Кузина Л.С. Предупреждение вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов. – Краснодар, 2020. – 258 с.

6. Кустов А.В. Криминалистическая концепция механизма преступления // Вестник МФЮА. – 2016. – № 2. – С. 164–169.

7. Лебедева С.Я. Предупреждение преступлений и административных правонарушений органами внутренних дел: учебник для студентов, обучающихся по направлениям подготовки «Юриспруденция» и «Правоохранительная деятельность». – 3-е изд. – Москва: ЮНИТИ-ДАНА, 2017. – 639 с.

8. Меняйло Д.В., Семенюк А.Ф. Использование информационных технологий при профилактике наркомании / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 5-й Международной научно-практической конференции, Белгород, 12 октября 2018 года. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2019. – С. 153–156.

9. Михайлов Б.П., Тузов Л.Л., Чварков М.А. К вопросу о проведении специальных оперативно-разыскных операций по противодействию незаконному обороту наркотиков // Вестник Московского университета МВД России. – 2021. – № 1. – С. 199–204.

10. Степаненко Д.А., Рудых А.А Цифровые технологии в криминалистическом обеспечении процесса доказывания / Криминалистика: теория и практика: материалы VII Международной научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2019. – С. 317–322.

ПРОБЛЕМЫ МЕЖДУНАРОДНОГО ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Карпика А.Г.,
кандидат технических наук, доцент
(Ростовский юридический институт МВД России)

Аннотация: статья посвящена анализу проблем международного взаимодействия правоохранительных органов в области противодействия киберпреступности. Содержит результаты анализа и предложения, направленные на повышение эффективности взаимодействия.

Ключевые слова: киберпреступность, правоохранительная деятельность, международное сотрудничество, уголовное преследование, гармонизация национальных законодательств, международный потенциал.

PROBLEMS OF INTERNATIONAL COUNTERACTING CYBERCRIME

Karpika A.G.,
Candidate of Technical Sciences, Associate Professor
(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article is devoted to the analysis of the problems of international interaction between law enforcement agencies in the field of counteracting cybercrime. Contains the results of analysis and sentences aimed at improving the effectiveness of interaction.

Keywords: cybercrime, law enforcement, international cooperation, criminal prosecution, harmonization of national legislation, international potential.

Современное состояние киберпреступности и тенденции ее дальнейшего развития позволяют сделать вывод о том, что проблема эффективности деятельности правоохранительных органов в этой области требует серьезного рассмотрения на российском и международном уровне. Актуальность решения этой проблемы состоит в активизации деятельности киберпреступников различного уровня и специализации во всех областях деятельности физических лиц и организаций.

Анализ открытых источников [1; 2; 3] позволил выявить некоторые наиболее показательные примеры деятельности правоохранительных органов различных стран в области борьбы с киберпреступностью. Так, в марте 2021 года Европол, агентство по сотрудничеству в правоохранительных органах Европейского Союза, объявило об аресте подозреваемого лидера преступной группировки, которая проводила акции в отношении более 100 финансовых учреждений в более чем 40 странах, что привело к убыткам свыше 1 миллиарда евро. Начиная с 2013 года эта организованная криминальная группа использо-

вала вредоносное программное обеспечение, нацеленное на финансовые переводы и сети банкоматов финансовых систем по всему миру. Лидер группы был арестован в Испании после многолетнего расследования, координированного Центром киберпреступности Европола. Арест, проведенный испанской национальной полицией, включал в себя поддержку Федерального бюро расследований США, правоохранительных органов в Румынии, Молдове, Беларуси, Тайване и ряда частных компаний, специализирующихся в области кибербезопасности.

В августе 2022 года Министерство юстиции США объявило о том, что трое украинских граждан, являвшихся членами преступной организации FIN7, были арестованы в Польше, Германии и Испании. Им было предъявлено обвинение в развертывании вредоносного программного обеспечения с целью воздействия на более чем 100 американских компаний и краже более 15 миллионов записей карт клиентов. Привлечение к ответственности лишь некоторых из этих киберпреступников включало сотрудничество многочисленных правоохранительных органов, каждый из которых внес свой вклад в транснациональное исследование. Эти факты являются яркими примерами глобального сотрудничества, необходимого для достижения прогресса в выявлении и привлечении к ответственности киберпреступников.

Киберпреступность остается постоянной и трансграничной угрозой, которая продолжает расти в глобальном масштабе, затрагивая страны, независимо от уровня развития. Распространение технологий и плотность подключения к сети Интернет по всему миру в сочетании с технологиями ананимизации обеспечили киберпреступность сравнительно низким уровнем риска и сделали ее высокодоходным предприятием, оказывающим влияние на граждан, государственные институты, гражданское общество и предприятия. Этот тезис подтверждают многочисленные примеры: ограбление Центрального банка Бангладеша в 2016 году примерно на 101 миллион долларов США; атака Samsam Wareware 2018 года, которая парализовала американский город Атланту, и другие государственные и частные предприятия США.

Основным последствием атак на государственные организации в 2023 г. в отличие от 2022-го, стало нарушение основной деятельности, что соответствует тренду 2023 г. на атаки с разрушительными последствиями. Так, например, городской совет муниципалитета Дуранго (Испания) был «полностью парализован» из-за кибератаки. Местные СМИ сообщили, что «взлом был серьезным», а системы городского совета парализованы «на несколько недель»: все компьютеры совета и учетные записи корпоративной электронной почты не работали, ввиду чего сотрудники были вынуждены перейти на бумажный документооборот.

Подобные случаи происходили в России: сбои в Единой информационной системе таможенных органов России начались в 06:00 10 апреля 2023 г., о котором сообщила Федеральная таможенная служба (ФТС) в своем Telegram-канале. Из-за этих сбоев в ряде случаев было затруднено выполнение таможенных операций. Проблемы с ФТС возникли и у железнодорожных операторов. Представитель «Нефтетранссервиса» сообщил «Ведомостям», что отсутствие возможности проведения таможенных процедур «наблюдается во многих реги-

онах России». В результате, по его словам, груженые вагоны скапливались на железнодорожных станциях.

Компания Professional Services Accenture оценивает, что киберпреступность может стоить частному сектору 5,2 триллиона долларов в течение следующих пяти лет, так как лавинообразное расширение пользователей сети Интернет и сетевых устройств продолжает «обеспечивать» киберпреступникам предложение целей для преступлений. В то время как компании в области кибербезопасности продолжают разрабатывать инструменты для обеспечения безопасности пользователей, киберпреступники используют эти же технологии и основанные на них методы атак с целью уклониться от идентификации и облегчить проведение атак.

Киберпреступность влияет на страны по – разному в зависимости от их уровня развития. Развитие сетевых технологий в развивающемся мире увеличило плотность деятельности киберпреступников, но прибыль, извлеченная из этих преступлений, оказалась существенно ниже, чем в более развитых странах. Кроме того, киберпреступления совершаются разнообразными субъектами с различными мотивами. Так, угрозы могут исходить от организованных преступных групп, террористов, действующих лиц, работающих самостоятельно или по найму организаций, людьми, которые мотивированы финансово, идеологически, политически или по другим причинам.

Организованные уголовные группы, и во многих случаях независимые субъекты, как правило, чаще преследуют и финансовой выгоды, в то время как организации с более широкими мотивами больше нацелены на проведение разрушительных атак, направленных на уничтожение или сбор данных. Несмотря на различия в профилях преступников и мотивации, очевидно, что большинство актов киберагрессии носят транснациональный характер, что прямо или косвенно подтверждают данные правоохранительных органов. Так, киберинцидент может привести к многочисленным жертвам в разных странах независимо от местоположения преступников, из чего следует, что к расследованиям необходимо привлекать правоохранительные органы, прокуратуру и суды разных юрисдикций. Это осложняет проведение расследований, включающих вопросы, связанные с экстерриториальной юрисдикцией и обеспечением эффективности международных механизмов сотрудничества.

Проблемы, с которыми сталкиваются правоохранительные органы вследствие типичного транснационального характера угрозы киберпреступности, являются частью более широкого набора вопросов, препятствующих глобальному взаимодействию правоохранительных органов в достижении прогресса в противодействии подобного рода преступлениям. Анализ доступных данных показал, что в США менее 1% киберинцидентов приводят к фактическому аресту лиц, причастных к ним. К сожалению, отсутствие подобных данных по всем странам в открытой печати не позволяет сделать вывод о глобальных показателях.

Несомненно, ключевым фактором в решении проблемы противодействия киберпреступности является улучшение механизмов обмена информацией и сотрудничества между правоохранительными органами, пострадавшими или заинтересованными гражданами и юридическими лицами. Обеспечение любого

подхода, направленного на борьбу с угрозами, связанными с государственными и негосударственными субъектами со стороны киберпреступности, безусловно заслуживает внимания так же, как и установление четких и измеримых показателей для оценки динамики киберпреступности на национальном уровне и эффективности работы организаций, занимающихся правоохранительной деятельностью, с увязкой их полномочий в различных юрисдикциях и потенциальных возможностей, которые могут оказать влияние на способность сотрудничать со схожими органами по всему миру.

Понимание стимулов и проблем для эффективного обмена информацией между общественным и частными секторами экономики, установление четкой основы для оценки воздействия киберпреступности на экономический потенциал, например по сравнению с другими видами преступности, позволит определить приоритеты деятельности полиции в этой сфере. На стратегическом уровне определение тенденций киберпреступности и обеспечение достаточного количества человеческих и финансовых ресурсов для борьбы с угрозой может быть серьезной проблемой в случае отсутствия адекватных измеримых показателей.

В различных странах также существуют проблемы на стратегическом уровне в установлении четкого разграничения ролей различных государственных учреждений, работающих над вопросами кибербезопасности и межведомственной координации действий. Причиной этого является отсутствие эффективного центра координации, осведомленного о различных аспектах деятельности координируемых органов и организаций. Так, в Соединенных Штатах Америки существует множество правительственных учреждений и правоохранительных органов с полномочиями противодействия киберпреступлениям, которые часто имеют дубликативные и избыточные функции без единого центра или лица, ответственного за координацию. Вместе с этим имеется и положительный опыт подобной деятельности. Например, в 2016 году правительство Сингапура запустило стратегию кибербезопасности с соответствующим национальным планом действий, в котором говорится о том, что должны предпринимать отдельные организации для достижения своих целей. Ответственным был назначен министр кибербезопасности, функции которого заключаются в оказании помощи в координации реализации этой стратегии.

Данные о киберпреступности, как правило, опираются на отчеты о жертвах, которые, по мнению ряда авторов, содержат только «долю» совершенных преступлений. Даже в тех случаях, когда устанавливались механизмы отслеживания статистики по киберпреступности и кибербезопасности, эти механизмы часто недостаточны, фрагментированы и не допускают сравнения между различными областями в пределах как одного и того же государства, так и между различными государствами. Кроме этого, имеются известные трудности мотивирования жертв сообщать о киберпреступниках.

Формальное международное сотрудничество в области киберпреступности и получение цифровых доказательств закреплено в двусторонних и многосторонних соглашениях. Эти инструменты устанавливают параметры для процесса расследования иностранных правоохранительных органов, которые влияют на суверенитет национального государства. Наиболее распространенными

формальными методами сотрудничества в правоохранительных органах в области расследования киберпреступности являются соглашения о взаимной правовой помощи, а также экстрадиция и координация. Соглашения о взаимной правовой помощи теоретически могут помочь в содействии сотрудничеству по расследованию и судебным преследованиям в области киберпреступности, в том числе путем предоставления сбора и совместного использования доказательств в национальных границах. Соглашения, как правило, обязывают страны собирать документы и другие доказательства, оповещать свидетелей, исполнять запросы, согласовывать процессы, обрабатывать запросы по уголовным делам.

Инструменты, обычно вводящиеся в двусторонние или многосторонние соглашения, устанавливают процесс, посредством которого одна страна отправляет человека в другую страну для судебного преследования или наказания за преступления, совершенные в юрисдикции запрашивающей страны. Многие двусторонние соглашения об экстрадиции, подписанные в последние десятилетия, включали требование «двойное преступление», которое требует криминализированного поведения как в требовании, так и в запрошенных юрисдикциях для выполнения экстрадиции. Следовательно, без высококачественной гармонизации национальных законов о киберпреступности правоохранительные органы могут не иметь возможности выдавать обвиняемых и преследовать их в судебном порядке, если их поведение не будет криминализировано в обеих юрисдикциях.

В настоящее время Конвенция ООН против транснациональной организованной преступности является глобальным юридически обязательным инструментом, который поддерживает международное сотрудничество в предотвращении и борьбе с транснациональной организованной преступностью, а 190 стран сегодня являются участниками этого договора. В некоторых случаях он может использоваться для содействия сотрудничеству в случаях, связанных с киберпреступностью. Кроме того, созданы более неформальные методы международного сотрудничества, чтобы помочь полиции оптимизировать запросы, связанные с экстратерриториальными доказательствами в случаях киберпреступности. Вместе с этим нестабильный характер электронных доказательств и легкость, в которой они могут быть изменены, заблокированы или удалены, требует своевременных действий, навыков для поддержания цепочки защиты данных, например на базе технологии блокчейн, а также развития специализированных навыков для сбора, хранения и обмена такими доказательствами законным и допустимым образом [4]. Кроме того, требования к двойной криминализации для экстрадиции означают, что национальные законы должны быть согласованы, поэтому уголовное преступление в стране, делающее запрос, также является уголовным преступлением в запрошенной стране, что в настоящее время не всегда имеет место.

Отсутствие гармонизации национальных законодательств с двусторонними и многосторонними инструментами борьбы с киберпреступностью и обеспечением электронных доказательств или полное отсутствие этих законов является серьезным препятствием для сотрудничества. Кроме этого, существующая проблема соблюдения прав человека также может препятствовать сотрудничеству, так как правоохранительные органы не могут выполнить любые запросы

на экстрадицию или найти и временно арестовать подозреваемое лицо для ожидания его экстрадиции в том случае, если есть проблемы с правами человека по поводу контекста запроса или преступления, считающегося политическим по своей природе.

Еще одной проблемой является сотрудничество между правоохранительными органами и поставщиками услуг, что жизненно важно для предоставления и получения электронных доказательств киберпреступления. Поставщики услуг часто избегают сотрудничества, так как у них есть свои индивидуальные правила и политики, они руководствуются различными национальными законами, которые определяют то, как они сохраняют, получают и передают данные. Формальное сотрудничество между национальными правительствами, в отличие от непосредственного сотрудничества между правительствами и поставщиками услуг, также обычно необходимо для обеспечения того, чтобы такие доказательства могли быть допустимы в суде.

Попытаясь противодействовать этому, некоторые страны внесли ряд законодательных изменений с 2014 года для уменьшения длительные задержки в трансграничном разделении доказательств и обеспечения доступа к доказательствам непосредственно от поставщиков услуг по юрисдикциям. Например, в 2018 году Конгресс США принял «разъяснение Закона об использовании данных за рубежом» (Закон об облаке), чтобы облегчить процесс трансграничного обмена данными непосредственно между американскими технологическими компаниями и иностранными правительствами. Закон об облаке позволяет Соединенным Штатам заключать соглашения с другими странами для предоставления прямого доступа к данным технологических компаний, а также повышения стандартов гражданских свобод. Кроме того, Европейская комиссия предложила новый пакет E-Aevidence в апреле 2020 года, нацеленный на создание правовой базы для судебных приказов членов ЕС, которые должны быть направлены непосредственно поставщикам услуг или их юридическим представителям вместо добровольного сотрудничества.

Несмотря на достижение некоторого прогресса в укреплении международного сотрудничества по киберпреступности и определении правил поведения государства в киберпространстве на политическом уровне, эти усилия вряд ли серьезно повлияют на фактическое решение проблемы киберпреступности, так как правоохранительные органы не имеют технических возможностей применить данные правила на практике. В связи с этим для решения такой проблемы можно предположить, что наращивание договорного и технического международного потенциала как стратегически оправданный подход к противодействию киберпреступности является вполне рабочим инструментом. Наращивание потенциала может выполнить следующие задачи:

– обеспечить соблюдение национальных законов и международных договоров, а также гармонизацию законодательств в области противодействия киберпреступности;

– сместить акцент в преследовании киберпреступников из национальной юрисдикции в международную;

– способствовать актуальным потребностям защиты человека от преступных посягательств путем включения его в транснациональные программы обучения методам противодействия киберпреступникам и реабилитации жертв киберпреступлений;

– уменьшить цифровой разрыв в способностях между субъектами уголовного правосудия, находящихся в технологически развитых и технологически отсталых странах.

Примерами такого наращивания потенциала может стать поддержка разработки политики и стратегий в области киберпреступности; создание новых и/или обновленных законодательных рамок, обеспечивающих защиту отдельных граждан и организаций; создание систем отчетности по киберпреступности и показателям, связанным с правоприменением; укрепление специализированных полицейских подразлелений; расширение возможностей судебного преследования; разработка обучающих программ и программ тренингов правоохранительных органов, прокуратуры и судебных органов; создание механизмов сотрудничества правоохранительных органов и научных организаций для продвижения исследований киберпреступности.

Таким образом, комплексная стратегия борьбы с киберпреступностью должна стать первым шагом в оценке потребностей правоохранительных и правоприменительных органов в деле обнаружения и пресечения киберпреступлений. Использование уже разработанных национальных и международных правовых инструментов целесообразно для проведения оценки существующих угроз и имеющихся в распоряжении возможностей. В контексте сказанного важно отметить, что многие из них включают в себя акцент на важность включения межнационального сотрудничества в качестве аспекта национальных стратегий для обеспечения рассмотрения трансграничного характера затронутой в статье проблемы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Петерс А., Джордан А. Противодействие разрыву в киберправоприменении: укрепление глобального сотрудничества противодействия киберпреступности [Электронный ресурс]. – URL: http://thirdway.imgix.net/ (дата обращения: 01.04.2024).

2. Дж. Хинк, Т. Моро. Постоянное правоприменение: уголовные обвинения как реакция на злонамеренную киберактивность национального государства [Электронный ресурс]. – URL: http://thirdway.imgix.net/ (дата обращения: 01.04.2024).

3. Российские таможенные органы под атакой: масштабные сбои вызваны внешним воздействием [Электронный ресурс]. – URL: https://www.securitylab.ru/news/537510.php? (дата обращения: 01.04.2024).

4. Карпика А.Г. Анализ направлений применения искусственного интеллекта в правоохранительной деятельности // Юристъ-Правоведъ. 2023. № 1. С. 130–135.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ В ИНФОРМАЦИОННОЙ СФЕРЕ

Ковалева Е.Г.,
кандидат технических наук, доцент;
Струкова С.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной работе раскрыта уголовная ответственность за совершение преступлений в информационной сфере, а также представлены виды данной ответственности.

Ключевые слова: уголовная ответственность, информационная сфера, преступление.

CRIMINAL LIABILITY FOR COMMITTING CRIMES IN THE INFORMATION SPHERE

Kovaleva E.G.,
Candidate of Technical Sciences, Associate Professor;
Strukova S.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in this work criminal liability for committing crimes in the information sphere is disclosed, as well as the types of this responsibility are presented.

Keywords: criminal liability, information sphere, crime.

В настоящее время особо важное место в развитии государства занимает конкретно информационная сфера. Ее востребованность связана с появлением новейших тенденций, представляющих собой развитие компьютерных технологий.

В государстве информационная система представляет собой не только компьютеризацию, но также и обеспечение безопасности в экономической, политической и военных аспектах. При этом важно упомянуть и то, что информационные технологии существенно облегчили жизнь общества, так как теперь людям намного проще найти ту же информацию, быть в курсе новостей. Но, к сожалению, с развитием информационных технологий также развивается и преступность в этой сфере. Так называемые «хакеры», к примеру, – это люди, которые взламывают компьютеры, телефоны пользователей или же их социальные сети, вычисляя необходимую для них информацию.

В связи с появлением информационных технологий многие граждане теперь пользуются банковскими картами, на которые им приходит заработная плата и другие различные зачисления, в связи с этим появилось множество мошенников, которые звонят гражданам на мобильные телефоны, представляясь сотрудниками банка, и сообщбт о том, что у них хотят украсть деньги, просят

назвать код, благодаря которому они смогут произвести списание всех денежных средств на свои счета.

Именно поэтому данная тема исследования является актуальной и востребованной.

Если говорить конкретно про термин, то «преступления в области компьютерной информации – это опасные для общества деяния, осуществляемые по злому умыслу или по неосторожности, угрожающие безопасности компьютерной информации и способные причинить вред благам, охраняемым законом (правам личности, отношениям собственности и т.д.)» [3]. Данные преступления наносят вред обществу так же, как и преступления в остальных сферах.

Данные преступления подобно любым другим преступлениям, регламентируются Уголовным кодексом Российской Федерации (далее – УК РФ). Впервые ответственность за совершение данных преступлений была внесена в УК РФ в 1996 году. Они были закреплены в отдельной главе, которая и до сих пор имеет место быть, так как эти статьи не изменялись. Это 28 глава «Преступления в сфере компьютерной информации» [2].

Для привлечения к уголовной ответственности необходимо наступление одного из фактов совершения преступления, таких как:

– блокирование информации, то есть воздействие на информацию, после чего данная информация недоступна на неопределенный срок либо же вовсе навсегда;

– уничтожение информации – воздействие, которое приводит к полному удалению на цифровых носителях, приведение информации в непригодное для использования состояние;

– модификация состояния – внесение огромных изменений в информацию на компьютере, которые меняют ее суть;

– копирование информации – перенос информации на посторонние носители, которые впоследствии предоставят ее в открытый доступ, что нанесет ущерб государству, если, к примеру, эта информация является государственной тайной.

В главе 28 УК РФ закреплены статьи 272, 273, 274.1 и 274.2, все они делятся на пункты, которые определяют конкретное наказание за совершение преступления. Например, в п. 1 Ст. 272 закреплено, что «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок» [1]. Необходимо отметить, что совершенное преступление имеет несколько видов наказания, которые зависят от тяжести нанесенного ущерба, то есть, чем больше ущерба нанесено, тем больше будет наказание.

Ответственность за преступления, связанные с информационной сферой, но не напрямую, к примеру, кража мобильного телефона, ноутбука либо же той же банковской карты, будут уже относиться к другим главам и статьям, кото-

рые также закреплены в УК РФ, то есть, за данные деяния подозреваемый будет нести наказание, связанное с кражей.

Немаловажным фактом является и то, что уголовные преступления и уголовная ответственность в информационной сфере постоянно претерпевают изменения, которые связаны с постоянным развитием компьютерной информации. Поэтому государству, специалистам, которые занимаются уголовным правом, необходимо постоянно мониторить ситуацию и стадии развития информационных технологий, чтобы вносить измебнения в УК РФ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022) // СПС «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 23.03.2024) (с изм. и доп., вступ. в силу с 01.04.2024) // СПС «КонсультантПлюс».

3. Шарыпова Т.Н., Триба К.А. Уголовная ответственность за совершение преступлений в информационной сфере // Colloquium-journal. – 2020. – С. 232–235.

ЭЛЕМЕНТЫ ФОРЕНЗИКИ – СОСТАВЛЯЮЩАЯ ЦИФРОВОЙ ГРАМОТНОСТИ СОТРУДНИКА ОВД

Красноруцкая А.И.;
Федосеев А.Э.,
кандидат физико-математических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматривается актуальность обладания специальными знаниями сотрудниками правоохранительных органов в условиях роста киберпреступности. Описывается важность применения сотрудниками некриминалистических подразделений элементов форензики. Указывается на значимость цифровой грамотности в качестве элемента профессиональной подготовки.

Ключевые слова: киберпреступность, форензика, компьютерная криминалистика, цифровая грамотность.

FORMALIZATION OF THE APPROACH TO THE METHODOLOGY OF DIGITAL TRACES IDENTIFICATION AND FIXATION

Krasnorutskaya A.I.;
Fedoseev A.E.,
Candidate of Physical and Mathematical Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses the relevance of having special knowledge by law enforcement officers in the context of the growth of cybercrime. The importance of the use forensic elements by employees of non-criminalistic units is described. The significance of digital literacy as an element of professional training is pointed out.

Keywords: cybercrime, forensics, computer forensics, digital literacy.

Компьютеризация, пронзившая все стороны человеческой жизни, цифровая трансформация [1] как государственное направление в развитии общественных отношений – все это подтверждает повышение роли информационных технологий в жизни как каждого человека в отдельности, так и общества в целом. Положительные аспекты, вносимые технологиями, лежат в основе причин их повсеместного применения, а также неостанавливающегося развития. Но, к сожалению, достижения используются не только в созидательных целях. Инновации различных областей человеческой деятельности применяются против человека, против аспектов его деятельности, против государственного устройства. Обратная сторона прогресса – высокотехнологичная преступность. Деятельность правоохранительных органов нацелена на противодействие противоправным проявлениям. В том числе новым проявлениям, новым способам реализации, новым вариантам использования технологий.

В рамках расширенной коллегии Министерства внутренних дел Российской Федерации по итогам 2022 года В.В. Путин отметил наличие соответствующих знаний у граждан, в качестве одного из способов противодействия высокотехнологичной преступности: «…важно постоянно информировать граждан о новых разновидностях подобных преступлений, учить, как обезопасить себя от этих преступлений, в целом повышать цифровую грамотность людей…» [2].

Рост количества преступных проявлений в специфической форме способствует совершенствованию ответных мер. Правоохранительные органы в своей деятельности применяют обновленные тактические элементы и методики в противодействии видоизменяющимся преступлениям. Изменения коснулись составных частей расследования и оперативной составляющей, в том числе и криминалистики. Новые технологии пополняют и арсенал противодействия преступности применяемыми в разных отраслях инструментами OSINT и форензики. Сам термин имеет происхождение от *forensics* – сокращенной формы английского сочетания *forensic science*, интерпретируемого как судебная экспертиза или криминалистика. Несмотря на существование самостоятельного

термина *computer forensics*, в своем составе несущего определение «компьютерная», форензика без определения рассматривается как криминалистика, ориентированная именно на компьютерную сферу [3]. Форензика определяется как подраздел криминалистики [4], как прикладная наука, рассматривающая методы поиска, получения, закрепления и исследования цифровых доказательств. Зарубежная часть *computer forensics* относится непосредственно к криминалистическим исследованиям, связанным с локальными компьютерами: нахождению следов и артефактов в оперативной памяти, внешних сопряженных носителях, элементов журналирования программного обеспечения, реестра. Это один из элементов, присутствующих в классификации [5] направлений исследования. К другим компонентам классификации относят:

– Network forensics – рассматривает расследования в сегменте сетевого трафика информационных систем.

– Forensic data analysis – рассматривает направления анализа данных, получаемых в виде следов (для преступлений, инцидентов).

– Mobile device forensics – рассматривает мобильный сегмент с особенностями данных в системах Android, iOS и им подобных.

– Hardware forensic – рассматривает аппаратную составляющую, наиболее сложную по реализации, например, в виде анализа низкоуровневых данных микроконтроллеров, частот Wi-Fi-устройств или аппаратных закладок.

Помимо узких направлений внутри форензики ее практическая сфера применения охвачена не только криминалистической деятельностью в рамках расследования проявлений компьютерной преступности. Локализация и исследование цифровых следов используются также в гражданских правоотношениях, касающихся компьютерной информации или электронных доказательств в рамках разбирательств по гражданским делам. Разбирательства по нарушениям в сфере страхования, касающиеся компьютерной информации или информационных систем, тоже связаны с форензикой, как и процесс реагирования на инциденты информационной безопасности в компаниях и организациях. Элементы форензики применяются в рамках реализации информационного противодействия при решении задач даже военной или разведывательной направленности, а также на бытовом уровне организации гражданами защиты своих прав и частных интересов в отношении информации в электронном виде и электронных документов.

Форензика в органах внутренних дел по своей сути имеет непосредственное отношение к деятельности криминалистических подразделений. Одним из видов экспертиз, проводимых ими, являются компьютерно-технические экспертизы. Специалист, исследуя соответствующим образом изъятую технику, устанавливает наличие определенной следовой картины цифровой природы, исследует ее и документирует для возможности использования в качестве доказательной базы в судебном производстве. Вопросы, на которые необходимо ответить специалисту, формулирует следователь. Они носят юридический характер, так как полученная информация должна подтверждать факты нарушения определенных правовых норм и являться значимой в рамках рассматриваемого судом дела. Уголовно-процессуальное законодательство регламентирует экс-

перту указание в заключении «примененных методик» [6] наряду с результатами исследований. Эта сторона знаний носит уже технический характер. Таким образом, эксперт при реализации своей служебной деятельности должен опираться на разные области знаний.

С другой стороны, возможны ситуации формирования доказательной базы на основе цифровых следов, получаемых оперативным путем. Процесс документирования регламентируется нормативными документами, требующими соблюдения юридических норм, однако фактически сам процесс получения цифровой информации от смены должностного лица не изменился и также требует наличия знаний в области технических наук.

Еще одна норма федерального законодательства выражает обязанность полиции «…обеспечивать сохранность следов преступления, административного правонарушения, происшествия…» [7]. Это общее требование относится к сотрудникам полиции различных подразделений, т.е к представителям тех служб, которые будут реализовывать указанную функцию. Как правило, на место происшествия первым прибывает наряд патрульно-постовой службы или соответствующий участковый уполномоченный. Для реализации мероприятий по сохранению обстановки, следов и других вещественных доказательств на месте происшествия этим сотрудникам необходимо как минимум иметь представление о природе следов, их локализации и о действиях, способных повредить следы или даже уничтожить.

Природа цифрового следа как отличительная характеристика не позволяет однозначно определить его наличие или отсутствие органами человеческих чувств. Необходимо понимание сущности проявления этих специфических следов в виде, неотделимом от носителей, представление о носителях, реализованных в виде самостоятельных устройств, о способах формирования следов и, соответственно, способах их удаления (заметания), искажения и потери. Эти знания помогут качественно выполненять возложенные на полицию обязанности и в недопущении к искажению следовой картины по причине неквалифицированных действий, основанных на отсутствии знаний.

Глубина знаний о физических процессах не нужна для реализации указанной обязанности. Понимание того, что, наступив на отпечаток обуви на месте происшествия, можно исказить следовую картину или потерять вовсе, должно существовать в аналогии и для цифровых следов. Например, школьная информация о способности магнита намагнитить или размагнитить определенные материалы. Этот же принцип лежит в природе создания накопителей на жестких магнитных дисках (он же НЖМД, HDD, винчестер или жесткий диск). В совокупности эта информация сформирует знания о том, что поднесение магнита к такому носителю способно исказить или уничтожить информацию на нем, а, следовательно, и непосредственно цифровой след, что приведет к потере элементов доказательной базы. Или знания о том, что оперативная память является энергозависимой должны принести понимание того, что обесточивание компьютера на месте происшествия также способно уничтожить находящуюся в ней информацию (следовую картину).

Мы говорим о всепоглощении информатизацией всех сторон жизни, и, соответственно, наличии определенных знаний у человека для возможности использования этой информатизации в облегчении производственных процессов и для реализации цифровых благ в частной жизни. Почему же необходимость технической грамотности вменяют только специалисту? Глубокие знания – да, его прерогатива, но знаниями отдельных элементов форензики должен обладать значительно больший круг сотрудников, что подтверждают вышеуказанные примеры. Повышение уровня раскрываемости, в том числе высокотехнологичных преступлений, связывается с изменением уровня специальных знаний среди сотрудников [8].

При реализации основных профессиональных образовательных программ высшего образования, например, программ бакалавриата по направлению подготовки 40.03.02 Обеспечение законности и правопорядка, федеральный государственный образовательный стандарт высшего образования предписывает в качестве одной из общепрофессиональных компетенций сформировать у выпускника способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-12) [9]. Те самые элементы технических знаний, которые будут содействовать в служебной деятельности будущего сотрудника, получающего юридическое образование, учтены в базовом документе, предъявляющем требования к этому образованию. Подобные требования можно встретить в ряде других нормативных документов, касающихся и профессионального обучения сотрудников, впервые принимаемых на службу в органы внутренних дел, и дополнительных профессиональных программ повышения квалификации. В 2022 году в результате организационно-штатных мероприятий в системе МВД России создан новый главк по работе с личным составом. По словам Министра внутренних дел Российской Федерации генерала полиции Российской Федерации В.А. Колокольцева «Среди его функций – повышение качества подготовки сотрудников полиции к профессионально грамотным действиям в условиях любой оперативной обстановки».[2]

Систематическое развитие информационных технологий и их роли во всех областях деятельности человека, рост высокотехнологичной преступности – значимые социальные явления. Повышение роли информационной компетентности в профессиональных знаниях, ведомственный акцент на значимости качества подготовки сотрудников – закономерная реакция в вопросах противодействия новым противоправным проявлениям. Все в совокупности – взаимосвязанные проявления. Ведь новые технологии – это новые знания. Использование новых технологий, эффективное их применение, и тем более развитие не возможны без обладания знаниями. А раз мы говорим о новых этапах в развитии информационных технологий, то и знания должны быть именно из этой области. Из области информатики – в широком смысле, в узком – в виде навыков оператора прикладных программ или тех самых элементов компьютерной криминалистики.

Знания помогают не только использовать блага технологий, но и развивать их. В условиях тенденций роста количественной и качественной характеристик киберпреступности неоспоримы актуальность использования, а также

развития форензики как инструмента противодействия. Однако недостатки в уровне знаний из области информационных технологий не позволяют реализовать в правоохранительной деятельности весь потенциал, в том числе и компьютерной криминалистики. Это в очередной раз подтверждает важность реализации элементов цифровой грамотности при подготовке сотрудников органов внутренних дел.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Распоряжение Правительства Российской Федерации от 20 февраля 2021 г. № 431-р (ред. от 07.06.2021) «Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 года» // Собрание законодательства Российской Федерации. – 2021. – № 10. – Ст. 1634.
2. Расширенное заседание коллегии МВД России 20.03.2023 [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/events/president/transcripts/ (дата обращения: 28.03.2023).
3. Федотов Н.Н. Форензика – компьютерная криминалистика. – Москва: Юридический Мир, 2007. – 432 с.
4. Форензика [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Форензика (дата обращения: 28.03.2023).
5. Пискунов И. Искусство форензики. Теория, книги, курсы, полезные материалы [Электронный ресурс]. – Режим доступа: https://xakep.ru/2018/04/03/forensics-guide-1/ (дата обращения: 28.03.2023).
6. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 18.03.2023) (п. 9. ч. 1 ст. 204) // Собрание законодательства Российской Федерации. – 2001. – № 52. – Ч. 1. – Ст. 4921.
7. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 28.12.2022) «О полиции» // Собрание законодательства Российской Федерации – 2011. – № 7. – Ст. 900.
8. Архипцев И.Н., Федосеев А.Э., Шевцов Р.М. Кибербезопасность и компьютерная грамотность в правоохранительных органах // Пробелы в российском законодательстве. – 2021. – № 4. – С. 276–279.
9. Приказ Минобрнауки России от 27 июля 2021 г. № 677 «Об утверждении федерального государственного образовательного стандарта высшего образования бакалавриат по направлению подготовки 40.03.02 Обеспечение законности и правопорядка» (Зарегистрировано в Минюсте России 19.08.2021 № 64694) [Электронный ресурс] // СПС «КонсультантПлюс».

ДАРКНЕТ – УГРОЗА БЕЗОПАСНОСТИ: ПЛЮСЫ И МИНУСЫ

Куриленко Ю.А.,
кандидат юридических наук;
Князев П.И.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: новые цифровые технологии в настоящее время затрагивают все сферы жизнедеятельности. Каждый человек, у которого есть хотя бы один из видов связи: стационарный телефон, смартфон, компьютер, находящийся в сети, имеет широкий круг общения, возможность пользоваться различными услугами быстро и качественно, но в то же время в любой момент может стать жертвой кибермошенников. Многие пользователи сети Интернет сталкивались с понятием Даркнет, при этом не до конца понимая, что именно он собой представляет и какую возможную угрозу несет в себе. Авторами проведен анализ использования Даркнета, предложены некоторые правила безопасного поведения в сети и дополнительные меры для предотвращения кибер-преступлений.

Ключевые слова: даркнет, мошенничество, киберпреступность, кибербезопасность, личные данные.

DARKNET IS A SECURITY THREAT: PROS AND CONS

Kurilenko Y.A.,
Candidate of Law;
Knyazev P.I.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: new digital technologies currently affect all spheres of life. Every person who has at least one type of communication: landline phone, smartphone, computer, being in the network, has a wide range of communication, the ability to use various services quickly and qualitatively, but at the same time at any moment he can become a victim of cyber fraudsters. Many Internet users have encountered the concept of Darknet, while do not fully understand what exactly it is and what possible threat it poses. The authors have analyzed the use of the Darknet, proposed some rules of safe behavior in the network and additional measures to prevent cybercrime.

Keywords: Darknet, fraud, cybercrime, cybersecurity, personal data.

Если переводить слово «DarkNet» дословно, получаем: «темная сеть», «скрытая сеть», «теневая сеть». Чтобы понять, как устроен Даркнет, стоит разделить всю глобальную сеть на три слоя:

1. Видимая сеть. Каждый пользователь может посетить эти общедоступные ресурсы.

2. Углубленная сеть (глубокий Интернет). Самым простым примером может служить частное облачное хранилище (Private Cloud или Яндекс Диск).

3. Даркнет. Слой Интернета, скрытый от общего доступа.

Даркнет был создан военными США для выполнения специальных операций и засекречивания данных. В 2002 году компания Microsoft пролила свет на это скрытое сетевое пространство, именно после этого Даркнет стал довольно быстро развиваться. В России про Даркнет стали говорить относительно недавно шесть-семь лет назад.

Притягательность использования Даркнета заключается в том, что все пользователи засекречены. Это, с одной стороны, позволяет им анонимно совершать разные сделки, а с другой стороны, – развязывает киберпреступникам руки.

Стоит учитывать то, что серфинг Даркнета не является правонарушением, но при приобретении запрещенных товаров или услуг пользователь несет полную ответственность перед законом. На теневом рынке нет никаких государственных законов, но площадки устанавливают свои правила, за нарушение которых пользователь может быть заблокирован или, к примеру, потерять криптовалюту, которая лежала на данной площадке.

Самым простым примером Даркнета является TOR. Рассмотрим, каким образом пользователь в Даркнете остается анонимным. TOR Onion имеет логотип лука. Защита данных в TOR организована следующим образом. Зашифрованная информация перекидывается через несколько других компьютеров, что можно сравнить с продвинутой матрешкой. Отправитель шифрует данные так, что их может расшифровать только оператор, но затем они шифруются для посредника и только потом переходят оператору. Получается эффект луковицы: чтобы дойти до середины, нужно снять слой, а потом другой и так далее. Анонимность сети также основывается на осторожности пользователей и VPN.

Сделки на площадках лежат на плечах так называемого гаранта. Это третье независимое лицо или представитель площадки. Товары и услуги в Даркнете довольно разнообразны: начиная от взломанных программ и игр, заканчивая услугами на заказное убийство, наркотиками, торговлей оружием и еще многим, что нельзя найти в открытой сети. Следует отметить, что в Даркнете присутствует огромное количество мошенников, хакеров и двойников известных сайтов. Причем если киберпреступление будет совершено на просторах Даркнета (даже если вы являлись обычным пользователем), вернуть, к примеру, украденную криптовалюту или похищенные данные будет практически невозможно. Криптовалюта является весьма лакомым куском для киберпреступников, потому как она не обладает следующими атрибутами: указанием персональных данных, местонахождения пользователя и другой инфориации, что могло бы выдать человека, оплачивающего покупку с помощью банковской карты.

Большинство пользователей Даркнета используют его для покупки наркотиков (почти 70%), что в данный момент является одной из основных проблем борьбы с преступностью. Правоохранительные органы довольно активно борются с подобными преступлениями. Одним из самых известных способов являются подставные ресурсы, ссылки и форумы, при переходе на кото-

рые можно узнать IP-адрес преступника. Не так давно удалось закрыть площадку «Hydra». Основная часть серверов находилась в Германии, при этом обслуживалась вся Россия и часть стран в Европе.

Следует рассеять тот миф, что Даркнет содержит только преступную направленность. Многие опытные пользователи используют его в качестве дополнительной защиты, чтобы во время использования публичного Wi-Fi не потерять личные данные, которые могут украсть мошенники. На просторах Даркнета есть известные всем сайты BBC, The New York Times, ProPublica. BBC специально создали свой сайт в теневом пространстве, чтобы пользователи могли анонимно сообщать интересную информацию, тем самым не боясь расправы со стороны лиц, которым это невыгодно.

Подводя итог вышесказанному, отметим, что все же Даркнет представляет больше опасность как для общества, так и для всего государства. В России нет запрета на посещение сети Даркнет. Было бы правильно оградить обычных пользователей от возможных посягательств киберпреступников. А потому внесение предложений по изменению в уголовном законодательстве считаем актуальным. Необходимо ужесточение наказания за киберпреступления, в частности за создание сайтов для продажи незаконных товаров и услуг.

Сложность расследования киберпреступлений заключается в том, что преступник и пострадавший могут находиться в разных странах. Следовательно, нужно совершенствовать взаимодействие с другими странами в правовой сфере.

Кроме того, нужны обученные, квалифицированные эксперты в области информационной безопасности, ведь такая работа требует грандиозного количества знаний. Также возможно использование опыта других стран. Одним из основных современных примеров может служить «Золотой щит» в Китае. В России предложение сделать похожую систему безопасности для управления сетевым контентом появилось в 2022 году. Пока что предложение только рассматривается, и, безусловно, реализация данного предложения требует колоссальных ресурсов и временных затрат.

Профилактическая работа в молодежной среде является также немаловажным аспектом предотвращения кибепреступлений. Многими участниками судопроизводства по уголовным делам, связанным с киберпреступлениями, оказываются подростки, которые обладают низким уровнем правосознания. Проведение различных воспитательных работ в школах, в средних и высших учебных заведениях правоохранительными органами с примерами пресечения таких преступлений помогло бы повысить осознание опасности использования Даркнета.

Пользователям сетей следует воздержаться от посещения запрещенных площадок и сайтов, ведь именно они позволяют существовать теневой сети Даркнет.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мазур А.А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет [Электронный ресурс]. – URL: https://cyberleninka.ru/ (дата обращения: 20.04.2024).
2. Свищев А.В., Лаухина А.С. Darknet: полезный инструмент или источник угрозы [Электронный ресурс]. – URL**:** https://cyberleninka.ru/ (дата обращения: 20.04.2024).
3. Даркнет [Электронный ресурс]. – URL: https://ru.wikipedia.org/ (дата обращения: 20.04.2024).
4. Скобелев В. Что такое даркнет и насколько он безопасен [Электронный ресурс]. – URL: https://www.forbes.ru/ (дата обращения: 20.04.2024).
5. Прокопенко А.Н., Страхов А.А., Гусев Ю.М. Крупнейший наркорынок мира «Гидра»: история появления, причины и следствия разгрома / Противодействие незаконному обороту наркотиков в условиях цифровизации общества: сборник материалов Международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2023. – С. 124–131.

КИБЕРСКВОТТИНГ КАК РАЗНОВИДНОСТЬ КИБЕРПРЕСТУПЛЕНИЯ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Лемайкина С.В.
(Ростовский юридический институт МВД России)

Аннотация: настоящая статья изучает явление недобросовестного использования доменного имени в сети Интернет (киберсквоттинг), различные виды киберсквоттинга и возможные способы борьбы с ним и защиты от него.

Ключевые слова: интернет, доменное имя, киберсквоттинг, киберсквоттеры, тайпсквоттинг, кибепреступление, веб-сайт.

CYBERSQUATTING AS A TAPE OF CYBERCRIM: CURRENT STATE, PROBLEMS AND PROSPECTS

Lemaikina S.V.
(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: this article examines the phenomenon of unfair use of a domain name on the Internet (cybersquatting), various types of cybersquatting and possible ways to combat and protect against it.

Keywords: fhe Internet, domain name, cybersquatting, cybersquatters, typesquatting, cybercrime, website.

Стремительное развитие компьютерных технологий и Интернета оказало большое положительное влияние и привнесло в нашу жизнь множество удобств. Однако это также вызвало и проблемы, с которыми трудно справиться, такие как появление новых видов преступлений. Каждый день мы сталкиваемся с растущим числом и разнообразием киберпреступлений, поскольку эта технология представляет собой простой способ для преступников достичь своих целей. Кроме того, информационные технологии способствуют глобализации этих преступлений, стирая границы стран и значительно затрудняя мониторинг, обнаружение, предотвращение или поимку киберпреступников. С каждым днем объем цифровых данных, хранящихся и обрабатываемых на компьютерах и других вычислительных системах, растет в геометрической прогрессии, люди общаются, делятся информацией, работают, совершают покупки и социализируются с помощью компьютеров и Интернета. Языковые и национальные барьеры исчезли, а виртуальный мир стал более населенным, чем когда-либо. Большинство киберпреступлений, которые мы наблюдаем сегодня, просто представляют собой миграцию преступлений из реального мира в киберпространство, которое становится инструментом, используемым преступниками для совершения старых преступлений новыми способами.

Об этом свидетельствуют статистические отчеты Министерства внутренних дел Российской Федерации, а именно: в 2023 г. количество преступлений, совершенных и использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, составило 676 951, в 2022 г. – 52 2065 [1]. Это обусловлено такими факторами, как психология преступника: правонарушитель совершает противоправные действия, на которые не осмелился бы в реальном мире.

Среди популярных схем обмана людей последних лет в области киберпреступлений стал кибersквоттинг или иначе захват домена. Захват домена представляет собой регистрацию, незаконный оборот или использование доменного имени в Интернете исключительно с недобросовестным намерением: извлечь выгоду из репутации, создаваемой товарным знаком, который принадлежит кому-либо другому. Это относится к недобросовестной регистрации доменного имени с нарушением прав на товарный знак другого лица.

«В 2023 году на просторах Интернета специалисты зафиксировали 207,1 тыс. мошеннических сайтов. Это на 86% больше, чем в предыдущем году», – сообщил директор департамента анализа защищенности и противодействия мошенничеству Bi.Zone Евгений Волошин в беседе с «Известиями». По его словам, основные скачки роста количества таких ресурсов пришлись на март, сентябрь и октябрь. В этим месяцы было зафиксировано больше всего доменов, которые имитировали площадки для розыгрыша призов. [2]

Кибersквоттеры – это люди, занимающиеся регистрацией популярных доменных имен, созвучных с именами популярных брендов и организаций. Данная деятельность связана с получением прибыли, так как имена доменов перепродают по завышенным ценам.

Существуют различные типы кибersквоттинга. Две основные формы кибersквоттинга заключаются в хранении коллекции похожих доменных

имен, связанных с товарными знаками. Покупка в данном случае, совершается с расчетом продажи доменных имен владельцам товарных знаков, часто по сильно завышенной цене. Еще один вид мошенничества как определено выше, заключается в желании извлечь выгоду из использования доменного имени, похожего на имя другого домена, воспользоваться его деловой репутацией и товарным знаком. Из-за отсутствия ясности Всемирная организация интеллектуальной собственности (далее – ВОИС) определила этот термин как неправомерную регистрацию доменного имени. Кибersквоттеры обычно могут свободно регистрировать любые доменные имена, даже если доменное имя с аналогичным именем уже существует. Кибersквоттеры часто используют сочетание нелегальной и законной работы для получения денег.

Далее приведем примеры известных громких случев, когда компании пострадали от кибersквоттинга. В 2000 году Google.com: кибersквоттер зарегистрировал доменное имя «googledotcom.com» с намерением обмануть пользователей, стремящихся получить доступ к поисковой системе Google. Корпорация Майкрософт: кибersквоттер зарегистрировал множество доменов, используя орфографические ошибки в популярных продуктах Microsoft, таких как «windwosliveemail.com» и «offcie365online.com» в попытке перенаправить ничего не подозревающих посетителей.

Понятие «кибersквоттинг» не регламентируется в российском законодательстве, хотя подобные действия попадают под законы, защищающие интеллектуальную собственность.

Разновидность кибersковттинга – тайпсквоттинг, преднамеренное неправильное написание известного бренда с целью регистрации схожего с ним доменного имени [3]. Кибersквоттеры желают легкого заработка. Тайпсквоттеры заходят дальше, их цель – взломать компьютер пользователя, что делает его уязвимым для кражи личных данных и нарушений безопасности.

Виды тайпсквоттингаю

Использование поддельного веб-сайта, чтобы вынудить законных владельцев веб-сайтов покупать доменные имена для кибersквоттинга, генерировать больше веб-трафика и распространять вредоносное программное обеспечение. Например, Twitter.com, и Twittr.com.

Похитители личных данных крадут вашу личную информацию и создают на ее основе домены. Мошеннический веб-сайт выдается за подлинный, его внешний вид имитирует вид реального сайта. Например, при имитации сайта известного банка будет использован логотип, цветовая схема и макет страницы этого банка. Разработчики на Python столкнулись с заражением вредоносной программой. Киберпреступники воспользовались тайпсквоттингом. В итоге разработчики, искавшие files.pythonhosted.org, попадали на похожий сайт, находящийся под контролем хакеров [4].

Namejackers регистрируют доменное имя, связанное с именем известного человека, обычно знаменитости или общественного деятеля.

Все виды кибersквоттинга влекут за собой определенные негативные последствия. Они могут угрожать репутации бренда, правообладателя товарного знака, могут ослаблять индивидуализирующие свойства обозначения, препят-

ствовать регистрации доменного имени правообладателем товарного знака, ввести в заблуждение потребителя, повлечь финансовые потери. В зарубежных правопорядках уже существуют механизмы пресечения таких нарушений. В Соединенных Штатах действует Федеральный закон о защите потребителей от кибersквоттинга. Согласно данному закону кибersквоттинг заключается в регистрации, незаконном обороте или использовании доменного имени в Интернете с недобросовестным намерением извлечь выгоду из репутации товарного знака, принадлежащего кому-либо другому [5]. В России правовая база по этому вопросу пока недостаточно наработана.

Существуют программы, которые могут помочь справиться с кибersквоттингом. Программное обеспечение может находить нарушителей, программы также могут отслеживать поддельные веб-сайты, кибersквоттинг имени и принудительно удалять их. Программы могут выяснить, какую информацию они собрали, и какие действия они совершали, злонамеренно используя ваше имя. Они также могут сообщить вам, стали ли действия другого лица причиной того, что ваш IP-адрес был помечен как вредоносный, и как это исправить.

Можно с полной уверенностью сказать, что кибersквоттинг будет развиваться и дальше, и так до тех пор, пока не будет ужесточен контроль за доменными именами (введение искусственного интеллекта, который будет при помощи определенных алгоритмов сразу не давать возможности регистрации ранее зарегистрированного доменного имени или схожего до степени смешения) и урегулировано законодательство по данному вопросу.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр» // Состояние преступности в России за январь-декабрь 2022 г., с. 1–67 за январь–декабрь 2023 г. [Электронный ресурс]. – URL: https://мвд.рф/reports/item/ (дата ознакомления: 23.04.2024).

2. Число мошеннических сайтов выросло на 86% в 2023 году [Электронный ресурс]. – URL: https://ren.tv/news/v-rossii/1176205-chislo-moshennicheskikh-saitov-vyroslo-na-86-v-2023-godu (дата обращения: 23.04.2024).

3. Киберскооттинг и Тайпсквоттинг [Электронный ресурс]. – URL: https://telegra.ph/Kiberskvotting-and-Tajpskvotting (дата обращения: 23.04.2024).

4. Топовые Python-разработчики заразились инфорстилером в ходе сложной атаки [Электронный ресурс]. – URL: https://ic-cs.ru/new-main/tpost/ (дата обращения: 23.04.2024).

5. Сухарева А.Е., Туркин Р.Э. Сравнительное исследование механизмов защиты от кибersквоттинга в России и США // Журнал Суда по интеллектуальным правам. – 2017. – № 16. – С. 84–94.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ МИГРАЦИИ И ПРИОБРЕТЕНИЯ ГРАЖДАНСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Маматова А.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются такие институты права, как гражданство Российской Федерации, миграция и миграционная политика, информационные технологии.

При приобретении гражданства Российской Федерации иностранному гражданину разъясняются права, которые ему предоставлены как гражданину государства, и обязанности, которыми он наделен после вступления в гражданство Российской Федерации. От соблюдения прав и обязанностей зависит безопасность населения и государства в целом. В связи с изменением законодательства о гражданстве Российской Федерации, вступлением в силу ряда нормативных актов, в том числе Федерального закона от 28 апреля 2023 г. № 138-ФЗ «О гражданстве Российской Федерации», введен относительно новый для правоприменителя институт прекращения гражданства Российской Федерации. В целях проверки законности пребывания иностранных граждан на территории Российской Федерации, выявления фактов нарушений миграционного законодательства сотрудниками УМВД России и территориальных органов как самостоятельно, так и совместно с УФСБ России по Белгородской области, ПУ ФСБ России по Белгородской и Воронежской областям и представителями органов местного самоуправления, проводятся рейдовые мероприятия по отработке мест пребывания иностранных граждан и осуществления ими трудовой и иной деятельности.

Ключевые слова: информационные технологии, электронный паспорт, миграция, гражданство Российской Федерации, иностранные граждане, прекращение гражданства Российской Федерации, миграционное законодательство.

THE USE OF INFORMATION TECHNOLOGIES IN THE FIED OF MIGRATION AND ACGUISITION OF CITIZENSHIP OF THE RUSSIAN FEDERATION

Mamatova A.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article examines such an administrative and managerial procedure as termination of citizenship of the Russian Federation as one of the ways to make a positive decision in the field of public administration. Citizenship is a stable legal connection of a person with the Russian Federation, expressed in the totality of their mutual rights and obligations. When acquiring citizenship of the Russian Federation, a foreign citizen is explained the rights that are granted to him as a citizen of

the state, and the responsibilities that he has after acquiring citizenship. The security of the population and the state as a whole depends on the observance of rights and obligations. In connection with changes in the legislation on citizenship of the Russian Federation, the entry into force of a number of regulations, including Federal Law № 138 "On Citizenship of the Russian Federation," a relatively new institution for law enforcement officials to terminate citizenship of the Russian Federation has been introduced. Its novelty and peculiarity lies in the possibility of depriving a person of acquired citizenship of the Russian Federation for certain actions, including the commission of crimes provided for by the Criminal Code of the Russian Federation (the legislator provides specific compositions of articles of the Criminal Code of the Russian Federation). The article analyzes the relevance and feasibility of the newly introduced norms, examines some of the first practical cases of termination of citizenship of the Russian Federation, and identifies problematic aspects and ways to solve them.

Keywords: information technologies, electronic passport, migration, citizenship of the Russian Federation, foreign citizens, de termination of citizenship of the Russian Federation, migration legislation.

Согласно Федеральному закону от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», под предоставлением государственных и муниципальных услуг в электронной форме понимается предоставление государственных и муниципальных услуг с использованием информационно-телекоммуникационных технологий, включая использование Единого портала государственных и муниципальных услуг или региональных порталов государственных и муниципальных услуг, в том числе осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями. В целях предоставления государственных и муниципальных услуг в электронной форме могут использоваться другие средства информационно-телекоммуникационных технологий в случаях и порядке, которые определяются Правительством Российской Федерации [1].

Вопросам приобретения и прекращения гражданства Российской Федерации уделялось и уделяется повышенное внимание как со стороны государственных деятелей, так и ученых, занимающихся исследованиями в публично-правовой сфере.

Как справедливо отметили И.В. Игнатушко и М.А. Дроздова «вопросы правового регулирования гражданства в Российской Федерации в последнее время становятся особо актуальными. Сложная геополитическая обстановка, необходимость защитить интересы России на международной арене, необходимость сплочения общества на фоне ведения боевых действий актуализируют тему гражданства, ответственности граждан перед своей страной» [2, с. 28].

Одним из эффективных механизмов быстрого реагирования на изменяющиеся обстоятельства, в том числе в период специальной военной операции, как отмечает В.А. Марачева, являются указы Президента Российской Федерации, которые позволяют сократить срок внесения изменений в правовые нормы

с целью защиты прав русскоязычного населения и соотечественников за рубежом [3, с. 22].

Проводя анализ деятельности миграционных подразделений региональных органов МВД России в области предоставления государственных услуг через электронные каналы, обратим внимание на пути улучшения этих процессов.

Так, информационно-аналитические материалы об оперативно-служебной деятельности УВМ УМВД России по Белгородской области (далее УВМ УМВД) и подразделений по вопросам миграции территориальных органов МВД России по Белгородской области на районном уровне (далее – ПВМ территориальных органов) за 12 месяцев 2023 г. свидетельствуют, что доля граждан, использующих механизм получения государственных услуг в электронной форме, составила 80,05% от общего числа поданных заявлений по всем государственным услугам. Непосредственно в ПВМ территориальных органов поступило 84 708 заявления, из них 67 812 – в электронном виде.

По данным информационно-аналитической системы мониторинга качества государственных услуг (далее – ИАС МКГУ) уровень удовлетворенности составил 99,94%. Всеми ПВМ территориальных органов достигнуто плановое значение уровня удовлетворенности (не менее 90%).

В частности, Президент Российсклй Федерации Владимир Путин подписал Указ, который утверждает новые положения о порядке рассмотрения вопросов гражданства Российской Федерации и принесения присяги гражданина. Документ был подписан в соответствии с новым Федеральным законом «О гражданстве Российской Федерации», вступившим в силу 26 октября 2023 года.

В соответствии с новыми положениями полномочия президента Российской Федерации в сфере гражданства сужаются. Теперь глава государства имеет право выдавать гражданство в исключительном порядке, в остальном вопросы принятия в гражданство переходят к МВД и МИД РФ. Одновременно президент сможет определять категории лиц, которые имеют право на упрощенное приобретение гражданства Российской Федерации [4].

Кроме того, вводится институт прекращения гражданства Российской Федерации для тех категорий, кто приобрел его не по рождению. Основаниями для его лишения являются:

– совершение преступлений террористической направленности, тяжких преступлений против государства, а также преступлений в сфере оборота наркотических средств и психотропных веществ;

– подделка документов, удостоверяющих личность гражданина Российской Федерации;

– публичные призывы к действиям против территориальной целостности Российской Федерации, дискредитации Вооруженных сил Российской Федерации, участию в нежелательной иностранной или международной НПО;

– публичные призывы к экстремизму, посягательство на жизнь госслужащего, организация вооруженного мятежа в целях насильственного изменения конституционного строя Российской Федерации, совершение действий, создающих угрозу нацбезопасности России.

Также отметим, что нововведения упрощают получение российского гражданства для более чем 20 категорий лиц, среди которых:

– иностранцы и лица без гражданства, достигшие 70 лет или признанные инвалидами I группы, иностранцы, которые родились или постоянно проживали на территории РСФСР и были советскими гражданами, граждане, у которых родственники по прямой восходящей линии постоянно проживали на территории, относившейся к Российской империи или СССР (в пределах госграницы Российской Федерации) – они все освобождаются от предоставления документов, подтверждающих владение русским языком, знание истории России и основ закона;

– лица, у которых близкие родственники – граждане России, живущие в России, а также граждане бывшего СССР, которые сейчас имеют статус лиц без гражданства;

– ветераны Великой Отечественной войны – бывшие граждане Советского Союза. Аналогичный механизм действует для ветеранов боевых действий по ходатайству госоргана, выдавшего удостоверение ветерана боевых действий – это необходимо подтвердить документом, образцы которых были утверждены до 1 января 1992 года;

– если гражданин заключил контракт о прохождении службы в Вооруженных силах Российской Федерации, других войсках или воинских формированиях, то он будет вправе подать на гражданство без учета требования о постоянном проживании в Российской Федерации; при этом контракт должен быть заключен на срок не менее одного года. Эта норма будет распространяться на участников государственной программы по переселению соотечественников и членов их семей и на иностранцев или лиц без гражданства, которые проживают в Российской Федерации не менее одного года и признаны беженцами или получили политубежище.

Невозможно обойти вниманием и проблемы миграции, особенно в приграничных регионах. Так, подводя итоги деятельности и определяя задачи на предстоящий период, заместитель начальника УВМ УМВД России по Белгородской области в своем выступлении на тему «О результатах служебной деятельности УВМ УМВД и подразделений по вопросам миграции территориальных О(У)МВД России по Белгородской области на районном уровне в 2023 году и постановка задач на 1-й квартал 2024 года по линии контрольно-надзорной деятельности» указал, что оперативно-служебная деятельность подразделений по вопросам миграции территориальных органов МВД России по Белгородской области на районном уровне в 2023 году была направлена на исполнение требований Директивы МВД России и выполнение целей, принципов и задач, определенных Указом Президента Российской Федерации от 31октября 2018 г. № 622 «О концепции государственной миграционной политики Российской Федерации на 2019–2025 годы».

В части миграционной ситуации, за период 12 месяцев 2023 года через белгородский участок Государственной границы Российской Федерации и административной границы с Луганской Народной Республикой в обоих направлениях проследовали 382 492 иностранных гражданина (2022 – 534 285; –28,4%), при этом отмечается тенденция к уменьшению количества въехавших иностранных граждан – 175 919 (АППГ – 322 482; –45,5%) и сохранению коли-

чества выехавших иностранных граждан на уровне предыдущего года – 206 573 (АППГ – 211 803; –2,5%).

По состоянию на 01.01.2024 на территории области находилось 18 тыс. (18 060) иностранных граждан (АППГ – 28 574; -36,8%), большинство из которых состоят на миграционном учете как прибывшие на территорию региона на срок до 90 суток, работающие на основании патента либо обучающиеся в учебных заведениях области (10 038 или 55,6%) и около 8 тысяч (8 022) проживают по разрешению на временное проживание (1 314, 7,3%) и виду на жительство (6 708, 37,1%).

В текущем году УВМ УМВД приняты решения о предоставлении российского гражданства 9 401 иностранным гражданам (АППГ – 13 387; –29,8%), среди которых преобладают выходцы из Украины.

За отчетный период оформлено 4 199 патентов, что на 8,8% больше, чем АППГ (3 859). Иностранным гражданам, указавшим при подаче документов на осуществление трудовой деятельности у юридических лиц, оформлено 830 патентов, что на 14,4% меньше, чем АППГ (970), у физических лиц – 3 369 патентов АППГ (2 889; +16,6%).

Среди оформивших патенты преобладают граждане Узбекистана (3 104; 73,9%), Таджикистана (712; 16,9%), Азербайджана (292; 7%), Молдовы (91; 2,2%).

В 2023 году иностранными гражданами совершено 286 преступлений (АППГ – 215; +33%), указанные преступления совершены 164 иностранными гражданами, количество лиц, совершивших преступления, снизилось на 22,6% (АППГ – 212).

Учитывая, что регион является миграционно-привлекательным в первую очередь для граждан СНГ и Украины, количество которых превышает 80% от общего числа находящихся в области иностранных граждан, соответственно и количество преступлений, совершенных этой категорией лиц, значительно. Так, 54% преступлений (155) совершено гражданами Украины, лицами без гражданства – 40 (14%). Основными видами совершенных иностранцами преступлений являются:

– незаконный оборот наркотиков – 103;

– кражи – 69;

– мошенничества – 20.

Совершаемые иностранными гражданами преступления не оказывают существенного влияния на криминогенную ситуацию в области, поскольку составляют 1,78% от общего количества зарегистрированных преступлений (16 097).

В целях проверки законности пребывания иностранных граждан на территории Российской Федерации, выявления фактов нарушений миграционного законодательства сотрудниками УВМ УМВД и территориальных органов как самостоятельно, так и совместно с УФСБ России по Белгородской области, ПУ ФСБ России по Белгородской и Воронежской областям и представителями органов местного самоуправления проводятся рейдовые мероприятия по отработке мест пребывания иностранных граждан и осуществления ими трудовой и иной деятельности. За 12 месяцев 2023 года сотрудниками УМВД России про-

ведено 13 оперативно-профилактических мероприятий в сфере миграции (2022 – 16; –18,8%), в ходе которых проверено 3 387 объектов различных форм собственности (2022 – 3 393, –0,2%), в т.ч.:

– 3 334 проведено в пределах полномочий, предоставленных Федеральным законом от 07 февраля 2011 г. № 3-ФЗ «О полиции» (на объектах жилого сектора и индивидуального жилищного строительства – 3 304, на объектах юридических лиц – 30),

– 53 проведено (оконченных) в рамках осуществления федерального государственного контроля (надзора) в сфере миграции (46 – документарных, 7 – выездных).

Также, важно отметить, что Президент Российской Федерации Владимир Путин заявил о необходимости создания специального органа, который бы комплексно занимался темой трудовой миграции в России. Он, по мнению президента, мог бы учитывать потребность экономики в иностранной рабочей силе, заниматься подготовкой граждан других государств к работе и жизни в России, учитывая при этом интересы коренного населения страны. Проблему миграции президент в ходе итоговой прямой линии, совмещенной с пресс-конференцией, назвал непростой, но характерной для многих стран. «Несмотря на отсутствие безработицы в России (ее уровень составляет 2,9%), потребности в кадрах на рынке труда существуют», – сказал Путин. «Но это не значит, что мы любой ценой и в ущерб коренному населению России должны решать экономические вопросы и закрывать проблемы рынка труда», – отметил президент. «В России находится более 10 млн трудовых мигрантов», – сказал он. Отечественная экономика в первую очередь должна стремиться привлекать из других государств квалифицированных специалистов. «Без рабочей силы более низкой квалификации тоже, вроде как, не обойтись», – добавил он. При этом подготовку потенциальных иностранных работников, по мнению президента, следует начинать заблаговременно – еще в странах исхода и совместно с властями этих государств. Они только поддерживают эту инициативу. Объединять экономическое, социально-культурное, образовательное и другие направления могло бы отдельное ведомство. «Нужен специальный орган, не только МВД России, который занимается техническими и правовыми вопросами. Нужен орган, который смотрел бы на эту проблему [трудовой миграции] в комплексе и своевременно бы находил решения по каждому аспекту этой проблемы», – заявил президент. «Идея создания единого органа, который бы занимался всеми миграционными вопросами, не нова и обсуждается уже около пяти лет», – сказал «Ведомостям» эксперт по миграции, бывший заместитель директора ФМС России (ликвидирована в 2016 г.) Вячеслав Поставнин. По его мнению, тот факт, что тема была озвучена президентом, может говорить о том, что экспертное сообщество и власти пришли в этом вопросе к единому мнению. Специальное ведомство, по мнению Поставнина, должно решать стратегические задачи в сфере миграционной политики, объединяя на своей площадке экономистов, социологов, специалистов по трудовой миграции и др. «Сейчас мигрантами фактически никто не занимается: МВД России выполняет исключительно контрольно-надзорную функцию, а у Минтруда России, Федерального агентства по делам

национальностей России, Минпросвещения мигранты не в фокусе внимания», – сказал он.

Подводя итоги, отметим, что в миграционной политике назрел ряд проблем, требующих разрешения. Это, во-первых, создание специализированного органа исполнительной власти, курирующего данную сферу, решающего в перспективе и вопросы социальной адаптации мигрантов; во вторых, проблема слабого знания мигрантами русского языка и местной культуры, которую тоже сейчас никто не решает на глобальном уровне, МВД России не может и не должно за это отвечать. Третья острая ситуация связана с отношением самих россиян к мигрантам. При желании иностранного гражданина остаться в России и обзавестись семьей у него возникает вопрос о выборе такого места жительства, чтобы не вызывать негативного отношения со стороны местного населения. В некоторых, как правило бедных, районах возникает «некая переполненность национальностями».

Кроме того, создание системы многофункциональных центров, предоставляющих муниципальные услуги (МФЦ), является необходимым шагом в развитии системы предоставления услуг в сфере миграции. Разветвленная сеть таких центров позволяет гражданам оперативно предоставлять полный спектр услуг, включая консультации по миграционным вопросам. Несмотря на то, что современная система развития предоставляет услуги в сфере миграции в электронной форме, этот институт все еще требует дальнейшего развития, поскольку многие процессы все еще не соответствуют требованиям уровня эффективности и функционирования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства Российской Федерации. – 2010. – № 31. – Ст. 4179.

2.Игнатушко И.В., Дроздова М.А. К вопросу о прекращении гражданства Российской Федерации // Конституционное и муниципальное право. – 2023. – № 5. – С. 27–31.

3. Марачева В.А. Вопросы приобретения и прекращения гражданства в связи с принятием в Российскую Федерацию новых субъектов // Конституционное и муниципальное право. – 2023. – № 5. – С. 19–26.

4. Путин утвердил новое положение о рассмотрении вопросов гражданства России [Электронный ресурс]. – URL: https://www. Fontanka.ru/2023/11/23/.

НЕКОТОРЫЕ ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ В СЕТИ ИНТЕРНЕТ

Маслиенко М.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье затрагивается тема актуального состояния деятельности по предупреждению правонарушений, совершаемых в цифровом пространстве. Проанализирован вопрос совершенствования мер по предупреждению противоправных действий в сети Интернет, с учетом актуальных потребностей и особенностей внутриполитической и внешнеполитической обстановки в России. Автором предложены конкретные меры по совершенствованию законодательства в данной области.

Ключевые слова: цифровизация, сеть Интернет, специальная военная операция, дискредитация Вооруженных сил Российской Федерации, предупреждение, социальные сети, мониторинг.

SOME ISSUES OF PREVENTION OF ILLEGAL ACTIONS COMMITTED BY THE INTERNET

Maslienko M.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article touches upon the topic of the current state of activities for the prevention of offenses committed in the digital space. The issue of improving measures to prevent illegal actions committed on the Internet is analyzed, taking into account the current needs and peculiarities by the domestic and foreign policy situation in Russia. The author suggests specific measures to improve legislation in this area.

Keywords: digitalization, Internet network, special military operation, discrediting of the Armed Forces of the Russian Federation, warning, social networks, monitoring.

В современном мире процесс цифровизации интегрирован во все сферы: государственную, общественную и частную. Однако помимо эффективности и удобства использования возможностей сети Интернет, ее пользователи непосредственно сталкиваются с потенциальными и реальными угрозами цифрового пространства. Криминологические риски связаны с тем, что злоумышленниками осуществляется посягательство на чужое имущество, на неприкосновенность частной жизни, а также распространяются сведения, ставящие под угрозу общественную безопасность.

Стоит отметить, что в общей структуре цифровых преступлений в 2023 году чаще всего совершались преступления против собственности (487,7 тыс. преступлений – 72,1%), преступления, связанные с незаконным оборотом наркотических

средств и психотропных веществ (103,9 тыс. – 15,4%), а также преступления, предусмотренные ст. 207 УК РФ (17,5 тыс. – 2,6%) и ст. 272 УК РФ (36,7 тыс. – 5,4%). Всего же в 2023 году зарегистрировано 676 951 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [1].

Для сравнения необходимо отметить, что за 2022 год в этой сфере зарегистрировано на 29,7% меньше цифровых преступлений, при этом раскрыто в 2023 году на 21% больше преступлений в сфере информационно-телекоммуникационных технологий и сети Интернет [2]. Это позволяет сделать вывод о том, что правоохранительные органы стали лучше работать по раскрытию преступлений, но одновременно с этим рост количества противоправных действий, совершаемых в сети Интернет, свидетельствует о том, что в профилактической деятельности есть проблемы. При этом профилактика цифровых преступлений по-прежнему остается одной из важнейших задач органов внутренних дел.

Общесоциальной мерой предупреждения противоправных действий, совершаемых в сети Интернет, является осуществление блокировки сайтов, содержащих сведения, носящие противоправный характер. Обязанности по мониторингу контента в сети Интернет возложены на общественные организации и правоохранительные структуры, деятельность которых связана с контролем за распространением информации, ограниченной в обороте [3]. Так, в случае установления фактов распространения информации, нарушающей установленные нормы административного или уголовного законодательства, осуществляется направление сведений в Роскомнадзор, который производит блокировку сайтов или отдельных страниц в сети Интернет, содержащих противоправный контент.

Процедура блокировки сайта в случае обнаружения Роскомнадзором противоправного контента выглядит следующим образом: 1) принимается решение о внесении сайта или отдельной страницы в реестр запрещенных ресурсов; 2) направляется обращение к хостинг-провайдеру с требованием заблокировать сайт. После этого у хостинга и владельца сайта есть три месяца, чтобы обжаловать решение в судебном порядке [4]. В случае удаления противоправного контента или в случае наличия соответствующего постановления суда, Роскомнадзор должен исключить сайт из реестра.

Сайт Роскомнадзора (https://rkn.gov.ru/) предусматривает подачу официальных обращений граждан в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в разделе «Общественная электронная приемная Роскомнадзора» с указанием предложенной в перечне тематики обращения [5]. Таким образом, помимо должностных лиц правоохранительной системы подать обращение о блокировки сайта либо отдельных страниц в сети Интернет, содержащих противоправный контент, может каждый гражданин.

Роскомнадзор наделен правом самостоятельно блокировать сайты и отдельные страницы, содержащие деструктивный контент в сетевом пространстве, если он содержит следующие сведения:

– о суицидах;

– о детской порнографии;

– о пронаркотической деятельности;

– о незаконных азартных онлайн-играх;

– о незаконной продаже лекарственных препаратов;

– информацию, вовлекающую несовершеннолетних в противоправную деятельность;

– о незаконной продаже алкогольной продукции в сети Интернет;

– о пострадавших в результате противоправных действий несовершеннолетних;

– о взрывчатых веществах и оружии;

– об ЛГБТ, педофилии и смене пола;

– о средствах обхода блокировок [6].

Так, например, в декабре 2023 года наибольшее количество обращений было по поводу распространения сведений, связанных с пропагандой проституции, оказанием интим-услуг, продажей продукции, свободная реализация которой посредством сети Интернет запрещена, экстремизмом, а также способами совершения экономических преступлений [7]. Обобщенный анализ данных обращений позволяет сконцентрировать внимание правоохранительных органов на наиболее опасных противоправных явлениях в сети Интернет и в дальнейшем привлечь причастных лиц к установленной законом ответственности.

Одним из эффективных методов противодействия противоправным действиям, совершаемым в информационно-телекоммуникационных сетях, а также в сети Интернет является совершенствование правовых норм, содержащих в себе запрет распространения информации, оборот которой запрещен на территории Российской Федерации. В силу чего, вполне обоснованным является необходимость актуализации критериев признания информации запрещенной, приведение их в соответствии с актуальными угрозами, обусловленным распространением противоправных действий в сети Интернет [8].

В связи с началом специальной военной операции, направленной на денацификацию и демилитаризацию политического режима на Украине, в средствах массовой информации и информационно-телекоммуникационных сетях, в том числе в сети Интернет, фиксируются многочисленные факты распространения заведомо ложной либо дискредитирующей информации о действиях Вооруженных сил Российской Федерации. Эта проблема обозначила острую необходимость защиты имиджа военнослужащего и Вооруженных сил Российской Федерации, недопущения призывов к введению в отношении России дополнительных санкций со стороны других государств, а также в устранении условий, способствующих созданию нестабильной обстановки на территории нашей страны [9].

Таким образом, закономерной реакцией будет дополнение перечня указанных критериев путем включения в них следующей информации:

– направленной на дискредитацию использования Вооруженных сил Российской Федерации или исполнения государственными органами Российской Федерации своих полномочий в целях защиты интересов Российской Федерации и ее граждан, а также поддержания международного мира и безопасности;

– о призывах к введению мер ограничительного характера в отношении Российской Федерации, а также граждан Российской Федерации. Данные изменения упомянутого правового акта должны основываться на разработке универсальных положений, не только позволяющих оценивать имеющуюся информацию, но и предусматривающих новые виды подобной информации.

Мониторинг цифрового пространства является весьма результативным методом предупреждения распространения противоправного контента и совершения противоправных действий в информационно-телекоммуникационных сетях, а также сети Интернет. Чаще всего данные противоправные действия совершаются в социальных сетях и мессенджерах, что закономерно в связи с их широким распространением как основного средства опосредованной межличностной коммуникации. По данным Kepios, количество профилей пользователей социальных сетей превысило отметку в 5 миллиардов, что эквивалентно 62,3% населения мира. За 2023 год этот показатель увеличился на 266 миллионов, в результате чего рост пользователей составил 5,6%, при этом на начало 2024 года в социальных сетях насчитывалось более 5,04 миллиардов человек [10].

В вопросе криминализации социальных сетей как наиболее часто используемых при совершении противоправных действий стоит согласиться с мнением В.С. Соловьева, который в своей работе «Методики оценки криминогенного потенциала социальных сетей» справедливо отмечает: «Любое криминологическое исследование, касающееся вопросов криминализации социальных сетей, должно учитывать мнения пользователей, поскольку именно они в первую очередь сталкиваются с преступными проявлениями в социальных сетях» [11].

Большое значение в предупреждении противоправных действий, совершаемых в сети Интернет имеет распространение профилактического контента. С учетом постоянного обновления новых видов противоправных деяний, совершаемых в киберпространстве, профилактический контент, размещаемый на официальных информационных ресурсах, также должен быть актуальным, а для повышения эффективности его распространения необходимо уделять внимание технологиям его продвижения, которые позволяют обеспечить доставление информации до потенциального потребителя при помощи email- и смс-рассылок, контекстной и таргетированной рекламы и т.д.

При этом распространение профилактического контента необходимо организовать во взаимодействии с коммерческими организациями, оказывающими рекламные услуги в информационно-телекоммуникационных сетях и сети Интернет, в целях охвата большей аудитории. Данный вопрос также необходимо урегулировать правовыми нормами, что позволит в свою очередь результативно организовать взаимодействие между специализированными и неспециализированными субъектами профилактики.

Таким образом, вопрос дальнейшего преобразования законодательства в рассматриваемой сфере должен быть проработан с учетом оценки криминогенности сети Интернет и социальных сетей экспертами государственных, коммерческих и некоммерческих организаций, оказывающими помощь правоохранительным органам в вопросах проведения экспертной оценки противоправных явлений в цифровом пространстве.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Отчет ГИАЦ МВД России о результатах деятельности ОВД РФ по противодействию преступлениям, совершаемым с использованием ИТТ, а также результатах деятельности структурных подразделений ОВД РФ, специализирующихся на противодействии преступлениям данного вида (форма «ИТТ» код 280) // Сервис ведомственной правовой статистики МВД России.

2. Статистические сведения о состоянии преступности в 2023 году [Электронный ресурс]. – URL: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/ (дата обращения: 30.05.2024).

3. Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службу по надзору в сфере связи, информационных технологий и массовых коммуникаций» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс».

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12.12.2023) п. 6–11 ст. 15.1 «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс».

5. Роскомнадзор – Общественная электронная приемная Роскомнадзора [Электронный ресурс]. – URL: https://rkn.gov.ru/treatments/ask-question/ (дата обращения: 30.05.2024).

6. Роскомнадзор – Пресечение распространения противоправной информации [Электронный ресурс]. – URL: https://rkn.gov.ru/activity/electronic-communications/p1568/ (дата обращения: 30.05.2024).

7. Роскомнадзор – Судебная практика за 2024 год [Электронный ресурс]. – URL: https://rkn.gov.ru/activity/ (дата обращения: 30.05.2024).

8. Дулькина Л.В. Социально-политические основания криминализации публичного распространения фейковой информации об использовании Вооруженных Сил и деятельности государственных органов России / Перспективные прикладные исследования и инновации: материалы Международной научной конференции. – Санкт-Петербург: МИПИ им. Ломоносова, 2023. – С. 45–47.

9. Критерии оценки материалов и (или) информации, необходимые для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети Интернет, а также сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие запрещенную информацию, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено»: утв. приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, МВД России, Феде-

ральной службы по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службы от 18 мая 2017 г. № 84/292/351/ММВ-7-2/461 [Электронный ресурс] // СПС «Гарант».

10. Статистика Интернета и соцсетей на 2024 год – цифры и тренды в мире и в России [Электронный ресурс]. – URL: https://www.web-canape.ru/business/ (дата обращения: 30.05.2024).

11. Соловьев В.С. Методики оценки криминогенного потенциала социальных сетей. – Краснодар: Краснодарский университет МВД России, 2017. – 69 с.

О ВОЗМОЖНОСТЯХ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОВД С ЦЕЛЬЮ ПРОФИЛАКТИКИ И КОНТРОЛЯ ЗА ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ

Мельникова С.Д.,
Калашникова А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: технологии искусственного интеллекта на сегодняшний день играют важную роль в жизни социально-правового государства. Изучение вопросов использования технологий искусственного интеллекта влияет на многие сферы и области жизнедеятельности, в том числе науку и юриспруденцию. Актуальность данной темы состоит в том, что в России, как и во многих странах, происходит изменение системы общественных отношений за счет внедрения информационно-коммуникационных технологий, что способствует формированию отраслей и подотраслей права – и это уже получило свое название «цифровое право». Усовершенствование технологий искусственного интеллекта позволяет систематизировать расширенный поиск информации о наркотических средствах, а также способствует укреплению профилактических мер для пресечения попытки употребления или внедрения противозаконных препаратов на территории России. В данной статье будут рассмотрены вопросы: что из себя представляет оборот наркотических средств? каковы тенденции развития технологий искусственного интеллекта с целью профилактики ограничения движения наркотических средств? какие существуют возможности применения цифровых технологий для пресечения оборота наркотических средств? Также будет проанализирован вопрос о наиболее важных направлениях регулирования технологий искусственного интеллекта, которые необходимы для профилактики и контроля за оборотом наркотических средств, а также устойчивого развития государства в целом.

Ключевые слова: технологии искусственного интеллекта, наркотики, правовое регулирование, оборот наркотических средств, информационное законодательство, государство, профилактические меры, контроль, направления развития.

ABOUT THE POSSIBILITIES OF USING INFORMATION TECHNOLOGY IN ATS FOR THE PURPOSE OF PREVENTION AND CONTROL OF DRUG TRAVEL

Melnikova S.D.,
Kalashnikova A.A.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: artificial intelligence technologies today play an important role in the life of a social and legal state. The study of the use of artificial intelligence technologies covers many spheres and areas of life, including science and law. The relevance of this topic lies in the fact that in many countries, in particular in Russia, the system of social relations is changing due to the introduction of information and communication technologies, which contributes to the formation of branches and subsectors of law and this has already received its name - digital law. Improving artificial intelligence technologies makes it possible to systematize an expanded search for information about narcotic drugs, and helps to strengthen preventive measures to suppress attempts to use or introduce illegal drugs into the territory of our country. This article will address questions such as: What is drug trafficking? What are the trends in the development of artificial intelligence technologies for preventing restrictions on the movement of narcotic drugs? What opportunities exist for using digital technologies to curb drug trafficking? The issue of the most important areas of regulation of artificial intelligence technologies, which are necessary for the prevention and control of drug trafficking, as well as the sustainable development of the state as a whole, will also be analyzed.

Keywords: artificial intelligence technologies, drugs, legal regulation, drug trafficking, information legislation, state, preventive measures, control, development directions.

Сегодня в России происходит ускоренное вовлечение технологий искусственного интеллекта в общественную жизнь государства. Данный процесс оказывает свое влияние почти на каждую сферу жизнедеятельности людей, будь то экономика, политика или социология, а также воздействует на все отрасли российского права, в частности на уголовное право. Это явление затронуло и юриспруденцию, так как развитие новых IT-технологий и внедрение их в повседневную жизнь требует усовершенствования правового регулирования и соответствующего закрепления в законодательстве страны. Рассмотрим возможность использования информационных технологий в целях профилактики пресечения оборота наркотических средств на территории нашей Российской Федерации.

Что же такое оборот наркотиков? Данное понятие представлено в Федеральном законе о наркотических средствах и психотропных веществах. Оборот наркотических средств, психотропных веществ – это разработка, производство, изготовление, переработка, хранение, перевозка, пересылка, отпуск, реализа-

ция, распределение, приобретение, использование, ввоз на территорию Российской Федерации, вывоз с территории Российской Федерации, уничтожение наркотических средств, психотропных веществ, разрешенных и контролируемых в соответствии с законодательством Российской Федерации [1]. В свою очередь, мы проанализируем процесс незаконного оборота наркотиков, который прямо противоположен вышеприведенному определению. Данный процесс заключается в скрытной, незаконной реализации наркотических средств на территории государства без наличия на то должного разрешения.

На сегодняшний день число преступлений, связанных с незаконным оборотом наркотических средств, только увеличивается, так как большинство таких преступлений совершается посредством сети Интернет. Данное явление объясняется тем, что в информационной сети присутствуют как открытые для пользователя сведения о составе наркотических и психотропных веществ, способе их приготовления и их видах, так и закрытые источники, содержащие сведения о покупке и продаже наркотических средств, личные сведения продавцов и их контакты. В результате чего государственной антинаркотической политикой Российской Федерации была разработана Стратегия, содержащая меры по предупреждению совершения преступлений, связанных с наркотиками. В данный перечень мер входят:

1. Осуществление совершенствования государственного управления и законодательства в сфере оборота наркотиков.
2. Создание государственной системы мониторинга наркоситуации в РоссийскоЙ Федерации.
3. Оптимизирование работы сотрудников правоохранительных органов для улучшения показателя раскрываемости преступлений, связанных с незаконным оборотом наркотических средств.
4. Формирование механизмов выявления потребления наркотических средств другие.

В условиях современного постиндустриального мира, где информация – это и есть главное оружие, защита и нападение, а следовательно, бороться с какими-либо правонарушениями и преступлениями необходимо также с использованием глобальной сети Интернет, поэтому для полного и всестороннего изучения вопроса незаконного оборота наркотических средств, необходимо создание информационных технологий, которые позволят систематизировать массив данных о всей системе такого оборота.

Именно для этого по Указу Президента Российской Федерации [2] была разработана и внедрена система мониторинга наркоситуации в России. Под мониторингом в данном случае следует понимать систему наблюдения за развитием ситуации в сфере оборота наркотических и психотропных веществ, а также их прекурсоров.

Процесс изучения вопроса незаконного оборота наркотиков осуществляется Государственным антинаркотическим комитетом, антинаркотическими комиссиями в субъектах Российской Федерации, а также органами исполнительной власти и общественными объединениями. Такого рода контроль ведется в целях опреде-

ления состояния наркоситуации, выявления и пресечения преступлений в этой сфере, оценки имеющихся способов и методов раскрытия преступлений и др.

Мониторинг наркоситуации проводится с использованием единого банка данных и в целом предусматривает систематические исследования по установлению причин незаконного оборота наркотиков с целью пресечения таких действий и эффективной борьбы.

Помимо изучения и последующего анализа данных о состоянии оборота наркотических средств на территории Российской Федерации сотрудниками органов внутренних дел и иными подразделениями на постоянной основе должна проводиться работа на предмет обнаружения на различных интернет-сайтах и в мессенджерах подозрительной деятельности в данной сфере (вербование, сбыт, покупка, реклама и т.д.). Кроме того, анализу подлежат различные электронные платежные системы, с помощью которых производятся скрытые расчеты в сети Интернет.

Сложность проведения такого рода анализа и выявления фактов незаконного оборота наркотических средств заключается в анонимности наркоторговцев, осуществляющих свою преступную деятельность, посредством интернет ресурсов, а именно использование наркоторговцами современных технологий, которые позволяют сбывать наркотические вещества бесконтактным способом, так называемых тайники-закладки. Кроме того, существует возможность создания интернет-магазинов теневом секторе DarkNet, позволяющих в условиях анонимности совершать сделки онлайн, не раскрывая своих личных данных. Также анонимность обеспечивается за счет обезличенных криптосчетов, используемых для проведения расчетных операций.

Поэтому для эффективной реализации мероприятий по пресечению незаконного оборота наркотиков сотрудники правоохранительных органов несомненно должны обладать специальными знаниями в сфере IT-технологий, устройств, приложений.

Профилактика и контроль со стороны органов внутренних дел в системе предупреждения незаконного оборота наркотиков имеет важное значение, поскольку данный вид деятельности направлен на устранение и нейтрализацию криминогенных факторов, способствующих совершению преступлений, а также пресечение такого рода преступлений.

Борьба с наркопреступностью является актуальным и повседневным вопросом в России. С этой целью необходимо совершенствовать имеющиеся и, несомненно, разрабатывать новые оперативно-тактические методы и приемы по противодействию незаконному обороту наркотиков.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 08.01.1998 №-3 ФЗ «О наркотических средствах и психотропных веществах» [Электронный ресурс] // СПС «КонсультантПлюс».

2. Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» (с изменениями и дополнениями) [Электронный ресурс] // СПС «КонсультантПлюс».

3. Положение о государственной системе мониторинга наркоситуации в Российской Федерации, утвержденное постановлением Правительства Российской Федерации от 20.06.2011 № 485 [Электронный ресурс] // СПС «КонсультантПлюс».

4. Воронцов А.В., Михайлов Б.П., Хазов Е.Н. Современные проблемы организации оперативно-разыскной профилактики и пути их решения // Вестник экономической безопасности. – 2017. – № 3. – С. 137.

5. Кузина Л.С. Предупреждение вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов. – Краснодар, 2020.

6. Кустов А.В. Криминалистическая концепция механизма преступления // Вестник МФЮА. – 2016. – № 2. – С. 164–169.

7. Лебедева С.Я. Предупреждение преступлений и административных правонарушений органами внутренних дел: учебник для студентов, обучающихся по направлениям подготовки «Юриспруденция» и «Правоохранительная деятельность». – 3-е изд. – Москва: ЮНИТИ-ДАНА, 2017.

8. Меняйло Д.В., Семенюк А.Ф. Использование информационных технологий при профилактике наркомании / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 5-й Международной научно-практической конференции, Белгород, 12 октября 2018 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2019. С. 153–156.

9. Михайлов Б.П., Тузов Л.Л., Чварков М.А. К вопросу о проведении специальных оперативно-разыскных операций по противодействию незаконному обороту наркотиков // Вестник Московского университета МВД России. – 2021. – № 1. – С. 199–204.

10. Степаненко Д.А., Рудых А.А Цифровые технологии в криминалистическом обеспечении процесса доказывания / Криминалистика: теория и практика: материалы VII Международной научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2019. С. 317–322.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРОТИВОДЕЙСТВИЕ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ В СОВРЕМЕННОМ МИРЕ

Меняйло Д.В.,
кандидат юридических наук, доцент;
Лебедева К.К.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в научной статье рассматривается глобальная проблема, которая связана с незаконным оборотом наркотических средств. Актуальность данной темы связана с высоким уровнем совершения преступлений в данной области с использованием современных технологий, технических средств. Необходимость решения данного вопроса ложится в основу исследования. В связи с разработкой и активным внедрением в деятельность правоохранительных органов технологии искусственного интеллекта важно выделить динамику преступности в рассматриваемой сфере.

Ключевые слова: наркотические средства, правоохранительные органы, технология искусственного интеллекта, противодействие преступности.

ARTIFICIAL INTELLIGENCE AND COUNTERING DRUG TRAFFICKING IN THE MODERN WORLD

Menyailo D.V.,
Candidate of Law, Associate Professor
Lebedeva K.K.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the scientific article examines the global problem associated with illicit drug trafficking. The relevance of this topic is related to the high level of crime in this area using modern technologies and technical means. The need to address this issue forms the basis of the study. In connection with the development and active implementation of artificial intelligence technology in the activities of law enforcement agencies, it is important to highlight the dynamics of crime in this area.

Keywords: narcotic drugs, law enforcement agencies, artificial intelligence technology, crime prevention.

Несмотря на технологическое развитие современного общества, по-прежнему уровень преступности достаточно высок. Более того, появляются новые способы совершения преступлений, когда злоумышленники в своих преступных целях используют информационно-телекоммуникационные технологии. Высокий уровень знаний и правовой культуры не является гарантом соблюдения законности. Люди могут совершать преступления по тем или иным

мотивам. Такое положение вещей подтверждает статистика МВД России: «общее количество зарегистрированных в 2022 году на территории Российской Федерации преступлений по сравнению с 2021 годом снизилось на 1,9%, в том числе тяжких и особо тяжких – на 4,1%. Число преступлений против личности сократилось на 5,5%, в том числе фактов умышленного причинения тяжкого вреда здоровью – на 2,8%, изнасилований и покушений на изнасилование – на 4,2%. Отмечается снижение количества зарегистрированных в 2022 году разбоев на 10,5%, грабежей – на 7,1%, краж – на 4,8%, в том числе квартирных – на 7,5%, краж транспортных средств – на 19,6% и их угонов – на 9,3%, уголовно наказуемых хулиганств – на 13%» [1].

На основе представленных данных мы можем сделать вывод о том, что количество преступлений, которые носят непосредственный характер и связаны с фактическим осуществлением противоправных действий в отношении человека или собственности, снизилось. Однако пресс служба МВД России приводит статистику, связанную с совершением киберпреступлений: «Показатели киберпреступности остались стабильными. С использованием высоких технологий совершается каждое четвертое преступление» [1].

Все это наталкивает на мысль о том, что преступники все больше и больше в своей противоправной деятельности используют современные технические средства и программное обеспечение, с помощью которых преступными путями достигается максимальная выгода.

Такая же ситуация прослеживается и в сфере незаконного оборота наркотических средств. Опять же, обращаясь к официальной статистике МВД России: «по сравнению с январем–декабрем 2021 года сотрудниками органов внутренних дел выявлено и пресечено на 42,3% больше преступлений, связанных с производством наркотиков, на 11% – связанных с их пересылкой и на 7,6% – со сбытом»[1]. В подтверждение реального существования данной проблемы и ее глобального масштаба хотелось бы привести пример из своей профессиональной деятельности. В процессе осуществления патрулирования на территории города Белгорода в составе патрульно-постовой группы в дневное время было задержано лицо несовершеннолетнего возраста, в кармане которого в дальнейшем было обнаружено вещество по внешнему виду схожее с наркотическим веществом.

Несмотря на частности, в целом мы можем говорить о положительной динамике снижения уровня преступности, однако современные преступники все чаще и чаще стали прибегать к современным технологическим решениям, способным обеспечивать скрытность их действий.

В связи с этим обстоятельством у сотрудников правоохранительных органов возникает необходимость использования современного опыта и технологий для вычисления, отслеживания и пресечения преступности как в сфере незаконного оборота наркотических средств, так и в иных вида преступлений.

---

[1] Статистические сведения о состоянии преступности в 2022 году: официальный сайт Пресс-центра МВД России [Электронный ресурс]. – URL: https://mvdmedia.ru/news/ (дата обращения: 26.11.2023).

Мы полагаем, что исследование данной темы сегодня является достаточно актуальным. При этом важно отметить, что и проблема внедрения в повседневное пользование сотрудниками правоохранительных органов различных современных систем имеет весомое значение. На сегодняшний день все большую известность приобретает технология искусственного интеллекта, которая также, отчасти внедряется в деятельность сотрудниками органов внутренних дел для раскрытия преступлений и расследования уголовных дел. Для анализа технических и функциональных возможностей технологии искусственного интеллекта важно понимать ее сущность и значение для сотрудников органов внутренних дел России.

Искусственный интеллект занимается решением когнитивных задач (например, обучение, создание и распознавание образов), обычно отведенных человеку. Современные организации собирают большие объемы данных из различных источников – интеллектуальных датчиков, инструментов мониторинга, системных журналов и контента, созданного человеком[1].

Многие когнитивные задачи, которые необходимо решать человеку в процессе своей жизни и профессиональной деятельности, лежат в основе работы искусственного интеллекта. Использование искусственного интеллекта актуально и для решения задач, стоящих перед подразделениями МВД России.

Возвращаясь к вопросу о незаконном обороте наркотических средств, необходимо уточнить, что при расследовании таких преступлений также используются современные технологии и потенциал искусственного интеллекта. При этом можно выделить несколько программных направлений искусственного интеллекта в правоохранительной деятельности:

1. Программы видеонаблюдения со считыванием биометрических данных человека.

2. Программы распознавания голоса.

3. Программы, которые распознают украденные транспортные средства.

4. Программы, которые способны распознавать существенное нарушение общественного порядка, митинги, акты вандализма и др.

5. Системы при проведении судебной экспертизы.

6. Роботы, которые позволяют производить осмотр особо опасных объектов.

7. Боты, которые используются для первичных автономных контактов с гражданами и организациями [3].

Максимальная реализация и полнота внедрения таких программ в деятельность сотрудников правоохранительных органов во многом снизит нагрузку, увеличит возможность раскрытия преступлений в более сжатые сроки, увеличит раскрываемость преступлений в целом. Однако для полноценного внедрения и приспособления сотрудников к таким программам необходимо дополнительное обучение и подготовка.

Для расследования преступления и раскрытия уголовных дел, связанных с незаконным оборотом наркотических средств, сотрудники полиции исполь-

[1] Что такое искусственный интеллект (AI)? [Электронный ресурс]. – URL: https://aws.amazon.com/ru (дата обращения: 26.11.2023).

зуют программы видеонаблюдения. В качестве примера можно привести программу «Безопасный город», которая получила свое распространение с 2014 года перед Олимпийскими играми в Сочи. На первый взгляд может показаться, что установление отдельных камер видеонаблюдения и фиксация всего проходящего – всего лишь повседневное действие, которое лишь в немногом обеспечивает безопасное времяпрепровождение граждан. Безусловно в таком действии заложен метод наблюдения, так и сама программа видеонаблюдения использует этот метод. Так как в чем здесь заключается сущность искусственного интеллекта?

В данном случае мы будем говорить о сети видеокамер, осуществляющих видеонаблюдение, и к тому же такие камеры способны самостоятельно считывать биометрические данные человека. Но и на этом их работа не заканчивается. Данная программа ко всему этому автоматически осуществляет поиск по базам данных схожего на основе полученных данных человека [4; 5].

Это весьма практично и экономит большое количество времени для сотрудника. Также уменьшается или вовсе исключается необходимость самостоятельного просмотра, наблюдения и анализа информации с камер видеофиксации. Такая программа применима в отношении дилеров, которые раскладывают «закладки» по различным местам и попадают в объектив камеры, в отношении дилеров, которые передают товар непосредственно.

Другим примером являются системы судебной экспертизы. Без их проведения не обходится не один факт задержания дилера или человека, которого подозревают в употреблении наркотических средств или в их изготовлении. В любом случае при изъятии неизвестного вещества назначается судебная экспертиза, которая должна быть проведена в короткие сроки для принятия конкретного решения в отношении задержанного лица. И здесь на помощь приходит искусственный интеллект. Безусловно его деятельность полностью дублирует деятельность человека, но она осуществляется в 10 или в 100 раз быстрее. При необходимости проведения нескольких экспертиз в короткий промежуток времени система судебной экспертизы в буквальном смысле этого слова «спасает» эксперта и оставляет ему лишь формальный аспект ее проведения.

Таким образом, подводя итог, отметим, что искусственный интеллект играет большую роль при расследовании преступлений и раскрытии уголовных дел вне зависимости от того, в какой сфере они совершаются. Рассматривая проблему использования искусственного интеллекта при раскрытии преступлений, связанных с незаконным оборотом наркотических средств, мы пришли к выводу, что искусственный интеллект применяется сотрудниками правоохранительных органов. По своей сути, он полностью дублирует действия сотрудника, однако делает это в разы быстрее и с меньшей долей вероятности на ошибку, а это очень важно при большом количество материалов уголовных дел и сжатых сроках уголовного расследования. Поэтому мы считаем, что дальнейшее развитие таких технологий и их внедрение в деятельность подразделений правоохранительных органов необходимо для повышения раскрываемости преступлений, снижения количества преступных посягательств и пресечения их совершения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Боровская Е.В., Давыдова Н.А. Основы искусственного интеллекта. – Москва: Лаборатория знаний, 2018. – 127 с.
2. Меняйло Д.В., Лебедева К.К., Меняйло Л.Н. Роль и значение АПК «Безопасный город» в правоохранительной системе / Актуальные вопросы устойчивого развития государства, общества и экономики: сборник научных статей 2-й Всероссийской научно-практической конференции, Курск, 2–3 ноября 2023 года. – Курск, 2023. – С. 231–234.
3. Меняйло Д.В., Родина О.Н. Актуальные вопросы применения видеотехнологий в правоохранительных органах России / Правоохранительные органы России: проблемы формирования и взаимодействия: сборник материалов Межвузовской научно-практической конференции с международным участием. Псков, 9–10 ноября 2023 года. – Псков: университет ФСИН России, 2023. – С. 136–141.

АНАЛИТИЧЕСКАЯ РАБОТА В МВД РОССИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Минаев В.А.,
доктор технических наук, профессор;
Лапшин И.О.,
кандидат технических наук;
Стручков И.С.
(Московский университет МВД России им. В.Я. Кикотя)

Аннотация: рассмотрены основные принципы аналитической работы в органах внутренних дел, ее обеспеченность математическими моделями, методами и программно-техническими средствами, позволяющими изучать количественные и качественные характеристики исследуемых социально-правовых и криминологических процессов, а также формировать на этой основе варианты управленческих решений.

Ключевые слова: аналитическая работа, МВД России, модели и методы, большие данные.

ANALYTICAL ACTIVITY IN THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA: CURRENT STATE AND PROSPECTS

Minaev V.A.,
Doctor of Technical Sciences, Professor;
Lapshin I.O.,
Candidate of Technical Sciences;
Struchkov I.S.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: the article represents the basic principles of analytical activities in the internal affairs agencies, its provision with mathematical models, methods, software and hardware tools that allow to determine the quantitative and qualitative characteristics of the studied socio-legal and criminological processes, as well as to form options for management decisions on this basis, are considered.

Keywords: analytical activity, Ministry of Interior of Russia, models and methods, big data.

Аналитическая деятельность в органах внутренних дел (далее – ОВД) для повышения эффективности раскрытия и расследования преступлений и решения других оперативно-служебных задач всегда выступала в качестве приоритетной.

В ходе реализации этой деятельности формируется информационное отображение события преступления – его криминологические, криминалистические и иные характеристики. Наиболее существенными при этом являются данные о субъекте расследуемого преступления, непосредственном объекте преступного посягательства, особенностях способа совершения преступления, в том числе – характеристиках используемых средств и орудий совершения преступления [1; 2].

Развиваются нормативные, организационные и технологические основы создания информационных массивов. Так, традиционные ручные картотеки применялись в правоохранительной деятельности, начиная с начала двадцатого века. В шестидесятых-семидесятых годах по мере расширения возможностей компьютерной техники создавалась база для организации автоматизированных учетов. Автоматизированные системы оперативно-разыскного и профилактического назначения прошли несколько модификаций: «Зона-М», автоматизированный банк данных (АБД), интегрированный банк данных (ИБД), информационно-поисковые сервисы ИСОД МВД России.

В качестве основных функций информационно-аналитической деятельности ОВД в самом общем виде выделяются [3]:

– накопление, обобщение, анализ, многократное и разноплановое использование данных, поступающих в ОВД из различных источников (официальных, неофициальных, общественных, реализованных на основе применения различных информационных технологий);

– организация социологических и криминологических исследований, прогнозирование криминогенной обстановки;

– подготовка для руководящего состава ОВД и различных инстанций информационно-аналитических и справочных материалов об основных результатах работы, оценках криминогенной обстановки на обслуживаемой территории;

– формирование справочно-информационного и аналитического фондов для обеспечения стратегической и тактической деятельности подразделений ОВД.

Информационную базу анализа и прогнозирования направлений функционирования ОВД составляет главным образом *статистическая информация* о состоянии преступности и результатах оперативно-служебной деятельности.

В то же время, уже давно ведутся дискуссии о недостатках традиционных статистических методов и подходов. Однако простота производимых расчетов, определенная их стереотипность, другие имеющиеся преимущества пока сдерживают развитие математических технологий в указанной сфере.

Однако с годами произошло и продолжает происходить значительное изменение многих факторов детерминации противоправных деяний, совершенствование методов их раскрытия и расследования на основе достижений науки и техники. Все это в совокупности привело к формированию новых требований к количественной поддержке принимаемых решений.

Нарастающая необходимость изменения существующего положения в указанной сфере приводит к новым подходам, технологиям, методам совершенствования информационно-аналитического обеспечения деятельности подразделений МВД России.

Пределы и перспективы развития

В связи со сказанным представляются важными следующие соображения:

1. Статистическое оценивание базируется, как правило, на *классических показателях представления информации*: абсолютные, относительные, средние значения, индексные величины – как основа расчетных преобразований математической статистики. При этом математическая статистика, как система методов обработки данных, располагая набором развитых алгоритмов, имеет определенные ограничения по их корректному применению.

В результате использование аппарата математической статистики приводит, с одной стороны, к оперативному и наглядному получению итоговых данных, позволяющему проводить требуемые аналитические сравнения. С другой стороны, невыполнение ряда условий корректного применения методов статистики приводит к искаженным, а подчас и противоречивым результатам.

Отмеченные положения объясняют сложность создания на основе традиционных методов статистики надежных алгоритмов обработки, отражающих изменения в современных правовых явлениях, проверку исследовательских гипотез, прогнозов развития изучаемых криминологических процессов.

2. *Большие данные.* Масштаб информационных массивов, возможности их современной математической обработки привели к необходимости применения технологии больших данных. В работе В.С. Овчинского, Е.С. Ларионой [4] подчеркивается, что искусственный интеллект и большие данные определены как основные цифровые технологии. Это отмечено в Стратегии развития ин-

формационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента России № 203 от 9 мая 2017 г. [5].

Если говорить просто, большие данные (англ. *Big Data*) – обозначение огромных объемов структурированных и неструктурированных данных, эффективно и оперативно обрабатываемых современными математическими методами и программными инструментами.

Для иллюстрации указанного феномена применительно к информационным системам МВД России приведем лишь один пример. Так, двадцать три года тому назад только за полгода информационными центрами ОВД поставлено на учеты более 35 млн объектов, представляющих оперативных интерес (общее число единиц, стоящих на учете в тот период, было почти в 10 раз больше). Сотрудники ОВД за те же полгода обратились к указанным системам с запросами около 60 млн раз [6]. Для сравнения – информационная система Национального центра криминальной информации (NCIC) ФБР США 23 года назад насчитывала около 40 млн единиц учета.

3. К важнейшим вопросам использования информационных ресурсов относится *обеспечение их актуализации*. Полнота и достоверность учетных документов основывается на постоянном контроле (логической, содержательной и иной проверки учтенных и новых вводимых данных) регистрируемой и корректируемой информации об объектах учетов.

Задачи и особенности актуализации данных необходимо рассматривать в ряду самостоятельных аспектов. Отметим два важнейших из них:

– различная степень актуализации данных по конкретным учетам сказывается и на других учетах, связанных с ними;

– отличающееся представление данных приводит к отсутствию единого формата при создании информационных массивов для исследования криминогенной обстановки. По многим причинам разработать такой формат почти нереально, если учитывать различия хранилищ уголовно-правовой статистики, особенности специализированных автоматизированных учетов ОВД, неструктурированность информации из социальных сетей и многие другие факторы.

Современные тенденции информационного обеспечения правоохранительной деятельности указывают на постоянное расширение как перечней баз данных, так и технологических возможностей их обработки, а также подходов к автоматизированному управлению ими. В перспективе именно в гармоничном сочетании информационных сервисов, интеграции систем с разнородными данными видится эффективное решение информационно-аналитических и управленческих задач ОВД [7].

Существует множество причин (сбои при обработке данных, технические ошибки, алгоритмическое несоответствие, нечеткое выполнение регламентов ввода или корректировки исходных данных), определяющих появление ошибок в информационных базах. Ошибки приводят к следующим недоработкам в формировании статистических учетов, специализированных банков и баз данных ОВД: неполные данные, данные с ошибочными значениями, пропуски данных, несоответствие форматам представления данных и т.д.

Совокупность ошибок и неточностей затрудняет, делает некорректной обработку информационных массивов, а также приводит к подготовке недостаточно обоснованных и даже неверных управленческих решений. Этому, в частности, могут способствовать ошибки восприятия данных, которые оцениваются человеком или автоматизированными системами (например, при применении систем искусственного интеллекта).

4. При анализе особенностей функционирования систем информационного обеспечения ОВД необходимо обратить внимание на их *динамичность* как системное свойство, а также на изменение содержания задач управления в данной сфере, характеризующегося проявлением в ней характеристик *сложных динамических систем* [8].

Обратимся к признакам таких систем. В первую очередь они отличаются вариативностью, адаптивностью к изменениям окружающей среды, требующим наилучшие стратегию и тактику реагирования. Согласно этим важнейшим свойствам у системы управления имеется способность воспринимать управляющее воздействие, переходить в новое состояние в течение определенного переходного процесса. В результате обеспечивается возможность ее перестройки, требующейся реально возникшими объективными обстоятельствами.

Эти положения относятся и к системам информационного обеспечения деятельности ОВД. При этом прослеживается устойчивая зависимость между раскрываемостью преступлений и информационной активностью сотрудников практических подразделений. В числе основных параметров информационной активности можно назвать: количество документов, поступающих в информационную систему за единицу времени; количество удаляемых документов; объем накопленных массивов [6].

Можно отметить и другие особенности, связанные с динамикой изменения информационных массивов, например:

– изменение представлений о выполняемой задаче, определяемых промежуточными результатами, новыми возникающими гипотезами, более глубоким экспертным осмыслением ситуации. Это, как правило, влечет новые скорость и производительность проверки информационных массивов;

– вариацию выбора и последовательности оцениваемых параметров (структуры и форматов данных, степени их полноты, соответствия определенным правилам);

– возможные искажения из-за несовершенства алгоритмов ввода, удаления и корректировки данных.

Знание реальной динамики информационных массивов, ее прогноз позволяют достоверно определить характеристики персонала, способного на требуемом качественном уровне осуществлять управление системой информационного обеспечения деятельности ОВД.

Еще одной стороной рассматриваемого вопроса является *динамичность задач управления*. При этом выделяются такие свойства информационных систем, как их стабильность (способность сохранять свои качества), равновесие между динамичностью и стабильностью (обеспечение существования, функционирования, в конечном итоге – живучести), целевое поддержание равновесия

(сохранение гомеостаза как противодействия разрушению и дезорганизации). В системах с перечисленными признаками обязательно наблюдаются процессы саморегуляции и самоорганизации.

Совокупность отмеченных системных свойств определяет непрерывное влияние и подверженность динамическим изменениям информационного обеспечения ОВД. Этому способствует информационный характер процессов раскрытия и расследования преступлений, проведения аналитической и иной деятельности ОВД.

В итоге оценка реальных процессов развития системы информационного обеспечения деятельности ОВД связана с динамичностью задач управления, возникновением классов новых подзадач. Данные обстоятельства накладывают на функционирование информационных систем ОВД требований поддержки динамического характера существования, реализации в программно-аппаратных средствах и приложениях возможностей по учету возникающих изменений.

5. Значимым фактором в развитии информационных систем и их методического обеспечения, поддерживающих эффективность информационно-аналитической и управленческой деятельности ОВД, является учет *латентности преступлений*. Речь идет о скрытой преступности, которая по тем или иным причинам не стала известной правоохранительным органам.

Существуют различные методы косвенной оценки латентности правонарушений и преступлений. Например, часто обращаются к результатам, полученным в работе Д.А. Ли [3]. Его исследования почти в трех десятках стран мира показали, что значения показателей латентных преступников оцениваются в 5–6% от общего числа населения в них.

Исходя из указанных результатов, при разработке математических моделей криминогенной обстановки следует учитывать фактор латентности во избежание серьезных ошибок в управленческих решениях ОВД.

В то же время методология традиционной статистической обработки информации о преступности не позволяет учесть и интерпретировать влияние латентности на состояние и динамику криминогенной обстановки, обеспечивать аналитическую деятельность в ОВД на современном уровне. Кроме того, в рамках традиционного анализа сложно отвечать на многие вопросы о скрытых характеристиках криминогенной обстановки, обосновать на этой основе необходимые по масштабу, структуре и направлению управленческие решения по противодействию преступности.

В целом современные условия проведения информационно-аналитической работы в ОВД приводят к необходимости разработки и внедрения перспективных моделей, технологий и методов анализа данных.

Они должны развиваться в направлениях:

– предварительной системной подготовки (в том числе – с применением методов искусственного интеллекта) информационных массивов, доведения их до требуемых форматов, полноты, соответствия логике преобразований в математических моделях;

– производительных алгоритмов обработки информации, приближающихся к технологии больших данных.

Технологии больших данных должны учитывать новые структурные, сервисные, аппаратно-программные, телекоммуникационные и иные принципы, подходы, ресурсы, что позволит достичь следующего качественного уровня развития информационно-аналитической и управленческой деятельности ОВД [9–13].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нестеров А.В. Миграция населения и проблемы борьбы с организованной преступностью / Актуальные проблемы теории и практики борьбы с организованной преступностью. – Москва, 1994. – С. 132–141.

2. Полевой Н.С. Криминалистическая кибернетика: теория информационных процессов и систем в криминалистике. – Москва: МГУ, 1982. – 208 с.

3. Бондарь К.М., Рыбак А.В., Скрипко П.Б. Основы управления в органах внутренних дел: курс лекций. – Хабаровск: Дальневосточный юридический институт МВД Россий, 2015. – 180 с.

4. Овчинский В.С., Ларина Е.С. Искусственный интеллект. Большие данные. Преступность. – Москва: Книжный мир, 2018. – 391 с.

5. Указ Президента Российской Федерации от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электронный ресурс] // СПС «КонсультантПлюс».

6. Бондарь К.М., Киселев В.И. Автоматизированные банки данных и их использование в органах внутренних дел: учебное пособие. – Хабаровск: ДВЮИ МВД России, 2000. – 92 с.

7. Бондарь К.М., Дунин В.С. Пути интеграции геоинформационных систем для аналитического обеспечения раскрытия и расследования преступлений / Новые информационные технологии в научных исследованиях: материалы XXV Юбилейной Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. – Рязань, 2020. С. 248–249.

8. Бондарь К.М., Рыбак А.В., Скрипко П.Б. Основы управления в органах внутренних дел: курс лекций. – Хабаровск: Дальневосточный юридический институт МВД Россий, 2015. – 180 с.

9. Барсегян А.А. Анализ данных и процессов: учебное пособие. – Санкт–Петербург: БХВ-Петербург, 2009. – 512 с.

10. Барсегян А.А. Методы и модели анализа данных: OLAP и Data Mining. – Санкт-Петербург: БХВ-Петербург, 2004. – 336 с.

11. Барсегян А.А. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP. – 2-е изд. – Санкт-Петербург: БХВ-Петербург, 2007. – 383 с.

12. Минаев В.А, Бондарь К.М., Дунин В.С., Скрипко П.Б. Математические модели анализа, оценки, прогнозирования и управления в органах внутренних дел: монография. – Хабаровск: ДВЮИ МВД России, 2022. – 308 с.

13. Минаев В.А., Бондарь К.М., Рабчевский А.Н., Федорович В.Ю. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: монография. – Хабаровск: ДВЮИ МВД России, 2023. – 232 с.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИНСТРУМЕНТОВ ВЕБ-АНАЛИТИКИ ДЛЯ МОНИТОРИНГА ОНЛАЙН-РЫНКОВ НАРКОТИЧЕСКИХ СРЕДСТВ

Молодых В.А.,
кандидат экономических наук, доцент
(Санкт-Петербургский университет МВД России)

Аннотация: российский онлайн-рынок запрещенных наркотиков растет благодаря возможности анонимно расплачиваться виртуальными валютами и наличию бесконтактных способов доставки наркотических средств. Этот тип сервиса доступен во всех крупных городах России и предоставляет продавцу более безопасную и анонимную альтернативу покупкам «на улице». Веб-аналитика с открытым исходным кодом является перспективным инструментом анализа новых глобальных криминальных трендов, а его использование в деятельности правоохранительных органов позволит повысить эффективность противодействия преступности, связанной с распространением наркотических средств.

Ключевые слова: онлайн-торговля наркотиками, криптовалюта, цифровая экономика, веб-аналитика.

PROSPECTS FOR USING WEB ANALYTICS TOOLS TO MONITOR ONLINE DRUG MARKETS

Molodykh V.A.
Candidate of Economic Sciences, Associate Professor
(St. Petersburg University of the Ministry of Internal Affairs of Russia)

Abstract: the Russian online illicit drug market is growing due to the ability to pay anonymously with virtual currencies and the availability of contactless drug delivery methods. This type of service is available in all major cities of Russia and provides the seller with a safer and more anonymous alternative to shopping «on the street». Open source web analytics is a promising tool for analyzing new global criminal trends, and its use in law enforcement activities will increase the effectiveness of countering crime related to the distribution of narcotic drugs.

Keywords: online drug trafficking, cryptocurrency, digital economy, web analytics.

Распространение подключения к интернету по всему миру способствовало росту как законной, так и нелегальной экономики. Глобализация сделала международные географические границы и физическое расстояние между покупателями и поставщиками стало в значительной степени неактуальными. Цифровая экономика позволила потребителям оплачивать счета, осуществлять

денежные переводы и приобретать товары с минимальными затратами времени как на местных, так и на международных рынках.

Онлайн-платежи впервые появились в конце 1990-х годов в виде сервисов e-gold, принадлежащих Gold & Silver Reserve Inc. (G&SR), который разрешил пользователям открывать онлайн-счета и приобретать золото, а затем переводить их на другие счета в качестве платежей. Независимо от того, использовалось ли e-gold для законных бизнес-возможностей или для схем виртуальных финансовых пирамид, данный сервис положил начало индустрии виртуальной валюты.

Ключевой особенностью, которая стала определять успех или неудачу виртуальной валюты, является простота внесения денег на онлайн-счет. При этом электронные валюты часто не соблюдают меры по борьбе с противодействием отмыванию доходов, полученных преступных путем, поскольку виртуальные валюты не эмитируются банками и не контролируются ими, и в результате эти организации не подпадают под действие одних и тех же правил. Как итог, в 2011 г. появился Silk Road – первый крипторынок незаконных наркотиков, за которым последовало множество преемников, который стал альтернативой традиционным моделям розничной торговли [1]. По данным ООН, 90% государств-членов определили интернет как источник незаконного оборота наркотиков. Это особенно верно в отношении новых психоактивных веществ (далее – НПВ), также известных как «легальные наркотики», которые являются химически отличными аналогами традиционно используемых наркотиков, которые еще не регулируются законом.

Традиционные наркотики остаются доминирующей частью международного оборота наркотиков, несмотря на растущую популярность НПВ. Диверсификация рынка, однако, способствовала злоупотреблению полинаркотическими препаратами, что создает риски для потребителей, поскольку все большее число различных и новых веществ становится доступным для покупки. Потребители опиоидов, например, подвергаются риску употребления гораздо более сильного фентанила вместо традиционного героина, поскольку производство синтетических опиоидов более экономически эффективно.

Соблюдение Единой конвенции о наркотических веществах отличается во всем мире – от мягкой политики в отношении наркотиков (например, Нидерланды и Португалия) до более строгих и бескомпромиссных подходов (например, Великобритания и Россия). Каннабис, опиаты и стимуляторы амфетаминового ряда являются тремя наиболее продаваемыми и потребляемыми видами наркотиков на сегодняшний день. Криминализация традиционных наркотиков во всем мире в конечном итоге привела к частичному переходу рынка к новым «дизайнерским препаратам», так называемым «легальным наркотикам».

Производители таких веществ могут опередить законодателей и распространять психоактивные вещества, которые еще не криминализированы. Некоторыми из наиболее известных новых психоактивных веществ являются спайсы (синтетические каннабиноиды) и «соли для ванн» (синтетические катиноны). Спайс относится к травяной смеси с добавлением синтетических каннабиноидов, обычно продаваемой как благовония, которая продается онлайн и в неко-

торых странах в специализированных магазинах, таких как табачные лавки. Впервые такие смеси появились в Европе и Соединенных Штатах в начале 2000-х годов и использовались в качестве альтернативы марихуане, поскольку пользователи сообщали об эффектах, сходных с теми, которые достигаются при курении каннабиса [2].

Наряду с различными моделями потребления наркотиков, формирующиеся рынки НПВ привели к появлению новых моделей распространения. Спайсы и «соли для ванн» доступны для покупки онлайн на специализированных вебсайтах, которые можно найти с помощью любой поисковой системы. Интернет обеспечил легкий доступ к торговым точкам, реализующим рецептурные лекарства из-за трудностей регулирования, присущих контролю за предприятиями, которые разбросаны по разным юрисдикциям. «Соли для ванн» обычно рекламируются онлайн как легальная альтернатива стимулирующим препаратам амфетаминового ряда. В начале 2000-х годов эти вещества продавались легально в розничных магазинах, но после их запрета в 2010-х годах в США и Европе Интернет стал основным источником распространения «солей для ванн» и аналогичных НПВ.

Точки незаконной торговли наркотиками появились в интернете благодаря анонимности, глобальному охвату и доступности обезличенных способов оплаты, которые не требуют идентификации клиента. Silk Road, архетипический крипторынок незаконных наркотиков, был структурирован аналогично eBay, предоставляя платформу, где любой поставщик может продавать свой продукт, а пользователь совершать покупки. Эта бизнес-модель стала возможна, благодаря способности клиентов совершать анонимные платежи с помощью криптовалюты Bitcoin, в то время как сам Silk Road был размещен в зашифрованной сети Tor для максимальной анонимности и минимизации рисков для участников [3].

Бизнес-модель, впервые предложенная Silk Road, была революционной, поскольку позволяла пользователям получать доступ к отзывам поставщиков и подробной информации о продукте, что способствовало снижению недоверия в условиях неопределенности. Клиенты Silk Road перечислили ряд причин для использования торговой площадки: доступ к более широкому ассортименту наркотиков, удобство, доверие к продавцам с высоким рейтингом и более низкие цены, отсутствие необходимости обращаться за наркотиками к уличным торговцам [4]. Таким образом, удобство, высокий ассортимент и низкий риск были ключевыми причинами, по которым интернет-пользователи перешли на онлайн рынки.

В Российской Федерации появилась еще одна форма интернет-торговли, получившая название «бесконтактная торговля наркотиками». Как и Silk Road, этот метод основан на онлайн-витрине магазина, где показывается реклама наркотиков, но способ доставки отличается. Вместо традиционной доставки на рынках бесконтактной торговли используются заранее организованные тайники с наркотиками, расположенные по отдельной территории, которую контролирует отдельный продавец.

Как только оплата за наркотики получена, операторы рынка передают клиентам инструкции о том, как найти тайник, в виде мгновенного сообщения. Продавец и покупатель никогда не взаимодействуют, кроме как онлайн, и покупатель совершает денежный перевод, используя один из новых цифровых способов оплаты с минимальными мерами идентификации.

Данный метод обсуждается в русскоязычной литературе по онлайн-торговле наркотиками, а также в отчете Целевой группы по финансовым мероприятиям (далее – ФАТФ), в котором подчеркивается злоупотребление виртуальными валютами, такими как Qiwi, WebMoney и Яндекс-деньги, для совершения этих незаконных транзакций [5].

В отчете ФАТФ, который включал описание метода бесконтактной торговли наркотиками, использовался пример, относящийся к России и Таджикистану. Суть бесконтактного метода продажи наркотиков можно описать следующим образом:

– покупатель делает заказ онлайн (через веб-сайт или мессенджер);

– далее покупатель производит платеж виртуальной валютой или мобильным денежным переводом;

– покупатель получает инструкции в виде СМС или мгновенного сообщения о том, где найти тайник с наркотиками.

Этот метод распространения наркотиков стал обычным явлением, поскольку он значительно снижает все виды рисков как для продавцов, так и для покупателей.

Для противодействия онлайн торговле наркотиками необходимо использовать преимущества «цифровых следов», что позволяет исследователям изучать онлайн активность преступников в их естественной среде в так называемых «условиях конвергенции».

Ручной сбор данных – трудоемкий процесс, поскольку он может потребовать от исследователей анализа тысяч веб-страниц, которые необходимо сохранить локально, закодировать и подвергнуть анализу. Несмотря на это, ручной сбор данных может обеспечить большие и точные наборы данных, которые можно использовать для углубленного анализа преступной деятельности в интернете.

Автоматизированный сбор данных основан на программном обеспечении, которое создает локальные копии целевого контента, размещенного в интернете. Данный процесс называется «зеркальным отображением» и извлекает соответствующие данные из сохраненного содержимого веб-страницы и часто используется для исследования поведения потребителей и маркетинговых целей. Внимание обычно фокусируется на социальных сетях, блогах и форумах, а также веб-сайтах.

Контекст большинства исследований по автоматизированному сбору данных с веб-страниц существенно отличается от криминального контента, размещенного в общедоступной сети или «темном интернете», где администраторы сайта могут предпринять активные шаги для защиты содержимого веб-сайта от доступа и индексации автоматизированными средствами. Например, Silk Road использовал файлы cookie, которые позволяли пользователям оста-

ваться в системе в течение недели до истечения срока действия, что позволяло исследователям обходить капчи при обходе веб-сайта. Однако данный подход подвергся критике из-за нестабильности веб-сайтов, размещенных в сети Tor, что подрывает автоматизированные методы сбора информации, которые, возможно, приводят к неполным наборам данных.

«Зеркальное отображение» обычно выполняется следующим образом. Начиная с одной веб-страницы, программа индексирует все гиперссылки внутри нее, затем переходит по этим ссылкам, повторяя процесс для каждой последующей веб-страницы в пределах, установленных пользователем. Существуют готовые решения, способные зеркально отображать веб-страницы, например, HTTrack. Однако HTTrack и аналогичное программное обеспечение будут только зеркально отображать веб-страницы без анализа, что потребует последующих шагов по очистке данных и преобразованию неструктурированных данных в структурированные. Очистка также может выполняться отдельными программами, называемыми «scrapers», которые могут анализировать веб-страницы для идентификации релевантного контента, такого как имена пользователей, прикрепленные к сообщениям на форуме, или названия наркотиков.

Специально написанные веб-сканеры, как правило, обладают большей функциональностью, чем свободно доступные решения, такие как сканер DATACRYPTO, который специально был разработан для изучения списков наркотиков на оригинальном Silk Road. Этот поисковый робот одновременно отображал и очищал веб-страницы, создавая базу данных наркотиков, информации о поставщиках и отзывах покупателей. Основным недостатком создания пользовательского веб-сканера с нуля является высокая стоимость услуг.

Для исследования содержимого целевых веб-сайтов можно использовать веб-сканер Dark Crawler (TDC), который первоначально был создан для изучения хакерских форумов и экстремистских веб-сайтов, а также для выявления террористического и прочего криминального контента. В дополнение к автоматизированному сбору данных TDC позволяет интегрировать другие аналитические инструменты для изучения извлеченного контента. Например, обработка естественного языка (NLP), дополненная тегами частей речи (POS), используется для расчета оценок настроений для сообщений на хакерских форумах, в которых упоминаются атаки на критически важные объекты инфраструктуры, такие как правительственные учреждения, банки и больницы. Еще одним преимуществом использования автоматизированного веб-сканера является отсутствие необходимости вручную просматривать потенциально вызывающие беспокойство медиаресурсы для установления их криминального содержания. Например, выявление изображений, связанных с эксплуатацией детей и терроризмом, возможно с помощью хэширования изображений, где каждому из них присваивается хэш-значение, которое можно сравнить с соответствующими базами данных правоохранительных органов.

Будучи самым известным рынком сбыта наркотиков, Silk Road был первым из них, который был тщательно изучен до его закрытия. Количество методов и подходов были весьма разнообразными: от качественного анализа отношения к онлайн-покупкам наркотиков до анализа тенденций в их списках путем

сохранения снимков веб-сайта за определенный период. Собирая имена поставщиков и ключи PGP (криптографические последовательности, используемые для аутентификации пользователя) с помощью автоматизированного веб-сканера, была описана организационная структура онлайн-сетей распространения наркотиков.

Для оценки влияния закрытия Silk Road на экономику незаконного оборота наркотиков в Даркнете и динамику количества поставщиков на конкурирующих рынках, веб-сайты анализировались примерно в течение месяца. Несмотря на закрытие крупного дистрибьюторского центра, участники рынка наркотиков смогли быстро адаптироваться и переместиться на конкурирующие рынки, о чем свидетельствует взрывной рост числа продавцов на них. Многочисленные исследования классифицировали незаконные товары, предлагаемые на этих рынках, от наркотиков до порнографии, украденных данных и оружия.

Таким образом, бесконтактная торговля наркотиками является актуальной темой, которая широко обсуждается как среди ученых, так и специалистов правоохранительных органов. Однако исследования в первую очередь касаются организационных аспектов бесконтактной торговли наркотиками, а также методов и практики проведения расследований с использованием цифровых инструментов. Требуется проведение комплексных исследований, характеризующих рынок наркотиков, доступ к которому осуществляется через множество онлайн-площадок, с точки зрения видов наркотиков, цен и объемов реализации. Использование возможностей специализированных программных продуктов, таких как веб-сканеры для сбора данных позволит проводить такие обзоры на основе общедоступных данных для определения общих тенденций и факторов, влияющих на динамику оборота всех видов наркотических веществ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Васильева Н.А. Анализ цифровых платформ в сфере незаконного оборота наркотиков для построения криминалистической характеристики данного вида преступлений // Юридическая наука. – 2020. – № 2. – С. 71–76.

2. Волкова О.В., Высоцкий В.Л., Дроздова Е.А. Актуальные вопросы противодействия наркопреступлениям, совершенным бесконтактным способом // Пробелы в российском законодательстве. Юридический журнал. – 2018. – № 6. – С. 176–178.

3. Земцова С.И. Криптовалюта в незаконном обороте наркотических средств: вопросы деанонимизации и ответственности // Криминалистика: вчера, сегодня, завтра. – 2020. – № 1 (13). – С. 54–63.

4. Рогозин В.Ю., Вепрев С.Б. Криминализация Интернета и WEB технологий // Расследование преступлений: проблемы и пути их решения. – 2016. – №. 3. – С. 160–163.

5. Сидоренко Э.Л. Криптопреступность как новое криминологическое явление // Общество и право. – 2018. – № 2 (64). – С. 15–21.

СПЕЦИФИКА РАБОТЫ ПОДРАЗДЕЛЕНИЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ: МЕТОДЫ ВЫЯВЛЕНИЯ И ПРЕДОТВРАЩЕНИЯ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ

Нестеренко И.С.,
кандидат педагогических наук, доцент;
Ачкасова А.А.
(Краснодарский университет МВД России)

Аннотация: в статье рассматриваются вопросы специфики деятельности подразделений, занимающихся противодействием экономическим преступлениям в сфере информационных технологий и внесены предложения в содержание программы повышения квалификации сотрудников данной категории.

Ключевые слова: экономическая преступность, анализ данных, машинное обучение, искусственный интеллект, большие данные, информационные системы кибербезопасности, многофакторная аутентификации, цифровая грамотность, личность киберпреступника, моделирование девиантного поведения.

THE SPECIFICS OF THE WORK OF THE DEPARTMENTS ECONOMIC SECURITY IN THE BANKING SECTOR: METHODS OF DETECTION AND PREVENTION FINANCIAL CRIMES

Nesterenko I.S.,
Candidate of Pedagogical Sciences, Associate Professor;
Achkasova A.A.
(Krasnodar University of the Ministry of the Interior Affairs of Russia)

Abstract: the article examines the issues of the specifics of the activities of departments engaged in countering economic crimes in the IT – sector and makes proposals for the content of the professional development program for employees of this category.

Keywords: economic crime, data analysis, machine learning, artificial intelligence, big data, cybersecurity information systems, multifactor authentication, digital literacy, cybercriminal identity, deviant behavior modeling.

Изучение нормативно-правовой базы, регулирующей сферу деятельности противодействия экономическим преступлениям, и отдельных научных трудов (Ю.В. Трунцевского, С.В. Иванцова, А.Г. Корчагина) позволило нам выделить ряд проблем:

1. Отсутствие четких определений понятий «экономическая преступность» и «экономические преступления» на законодательном уровне.

2. Сложности в квалификации некоторых деяний как преступлений в сфере экономической деятельности.

3. Необходимость постоянной адаптации методов работы подразделений экономической безопасности к новым схемам финансовых преступлений.

4. Недостаточная координация между банками, правоохранительными органами и регуляторами в сфере противодействия экономическим преступлениям.

Одной из ключевых проблем в правовом поле является отсутствие единого подхода к определению экономической преступности. Ряд ученых, например В.В. Лунеев, определяют ее как «совокупность корыстных преступлений, совершаемых в сфере экономики лицами в процессе их профессиональной деятельности, в связи с этой деятельностью и посягающих на собственность и другие интересы потребителей, партнеров, конкурентов и государства, а также на порядок управления экономикой в различных отраслях хозяйства» [5].

По нашему мнению, экономическая преступность – это совершение преступных действий, направленных на незаконное получение финансовой выгоды или нанесение ущерба экономике, бизнесу, государственным или частным организациям. Она часто носит транснациональный характер и может серьезно повлиять на экономическую стабильность и развитие общества.

Отсутствие четких формулировок на законодательном уровне создает сложности в квалификации некоторых деяний. Например, манипулирование рынком ценных бумаг (ст. 185.3 Уголовный кодекс Российской Федерации (далее – УК РФ) или неправомерное использование инсайдерской информации (ст. 185.6 УК РФ) не всегда однозначно трактуются как преступления, что затрудняет работу правоохранительных органов [1].

Еще одной проблемой является постоянное совершенствование методов и схем совершения финансовых преступлений. Как отмечает Ю.В. Трунцевский, «преступность в сфере экономической деятельности отличается высокой степенью латентности, адаптивностью к изменениям в законодательстве и правоприменительной практике, активным использованием пробелов и коллизий в нормативно-правовой базе» [2].

В таких условиях особую важность приобретает эффективная работа подразделений экономической безопасности банков. Они играют ключевую роль в выявлении и предотвращении финансовых преступлений, защищая интересы кредитных организаций и их клиентов. От таких подразделений требуется осуществление постоянного мониторинга угроз и своевременной адаптации методов противодействия им.

Одним из основных методов противодействия преступлениям рассматриваемого вида являются тщательный мониторинг и анализ финансовых операций с помощью специальных программных комплексов. Это позволяет в режиме реального времени выявлять подозрительные транзакции, которые могут быть связаны с отмыванием денег (ст. 174, 174.1 УК РФ), финансированием терроризма (ст. 205.1 УК РФ) или другими противоправными действиями.

На наш взгляд, внедрение современных технологий анализа данных, таких как машинное обучение и искусственный интеллект (далее – ИИ), может значительно повысить эффективность выявления финансовых преступлений.

Например, использование нейронных сетей для анализа поведенческих паттернов клиентов позволяет выявлять нетипичные операции и потенциальные риски в режиме реального времени. Такой подход уже применяется некоторыми крупными банками и показывает хорошие результаты в борьбе с отмыванием денег и мошенничеством.

Не менее важным является активное взаимодействие банков с правоохранительными органами, такими как Росфинмониторинг, МВД России и ФСБ России. Своевременное информирование указанных структур о признаках финансовых преступлений и предоставление необходимых документов в рамках расследования помогает пресекать противоправную деятельность и привлекать виновных к ответственности по соответствующим статьям УК РФ.

Для повышения эффективности такого взаимодействия представляется необходимым создание единой информационной системы, которая бы позволяла банкам и правоохранительным органам оперативно обмениваться данными о подозрительных операциях и лицах. Это помогло бы ускорить процесс расследования преступлений и повысить раскрываемость. Кроме того, важно регулярно проводить совместные учения и тренинги для сотрудников банков и правоохранительных структур, чтобы отрабатывать навыки взаимодействия и координации в условиях реальных угроз.

В этом контексте стоит отметить положительный опыт создания в России межведомственных рабочих групп по противодействию экономическим преступлениям. Как отмечает С.В. Иванцов, «такие группы, объединяющие представителей правоохранительных органов, контролирующих структур и банковского сообщества, позволяют наладить эффективный обмен информацией, координировать усилия и вырабатывать единые подходы к решению проблем» [3]. На наш взгляд, развитие подобных форматов сотрудничества должно стать одним из приоритетов в сфере борьбы с финансовыми преступлениями.

Подразделения экономической безопасности и противодействия коррупции МВД России также уделяют большое внимание предотвращению внутренних угроз, проводя проверки сотрудников и осуществляя мониторинг их действий. Это позволяет выявлять случаи мошенничества (ст. 159 УК РФ), присвоения или растраты (ст. 160 УК РФ), коммерческого подкупа (ст. 204 УК РФ) на ранних этапах.

По нашему мнению, для минимизации рисков внутренних угроз необходимо не только проводить регулярные проверки сотрудников, но и внедрять комплексные программы обучения и повышения осведомленности персонала о методах противодействия финансовым преступлениям. Например, в одном из крупных российских банков была запущена программа «Антифрод», в рамках которой сотрудники проходят регулярные тренинги по выявлению признаков мошенничества, изучают реальные кейсы и участвуют в ролевых играх. Такой подход позволяет не только повысить бдительность персонала, но и сформировать культуру нетерпимости к любым противоправным действиям внутри организации.

На основе информации из открытых интернет-источников можно сделать вывод, что ИИ уже начинает применяться в МВД России для раскрытия преступлений экономической направленности, хотя пока не столь широко, как в некоторых зарубежных странах.

Так, в 2021 г. МВД России сообщило о внедрении системы на основе ИИ для выявления и расследования картельных сговоров на торгах. Система анализирует большие данные из различных источников, чтобы находить признаки антиконкурентных соглашений.

Главное управление экономической безопасности и противодействия коррупции (ГУЭБиПК) МВД России использует ИИ-системы для выявления подозрительных финансовых операций и транзакций, которые могут быть связаны с отмыванием денег и другими экономическими преступлениями.

В ряде регионов России, например в Нижегородской области, полиция применяет технологии больших данных и машинного обучения для прогнозирования и предотвращения экономических преступлений, мошенничества, а также для поиска скрытых связей между фигурантами дел.

МВД России разрабатывает единую информационную систему, которая на основе алгоритмов искусственного интеллекта будет анализировать данные из различных баз для выявления признаков экономических преступлений, коррупции, конфликта интересов. Система позволит автоматизировать процессы и повысить эффективность работы подразделений экономической безопасности.

Еще одним важным аспектом является обеспечение защиты лиц, сообщающих о фактах финансовых преступлений в банках (так называемых информаторов). Как отмечает А.Г. Корчагин, «в России пока отсутствует эффективный механизм защиты информаторов от преследования и дискриминации со стороны работодателя» [4]. Между тем наличие таких гарантий могло бы существенно повысить эффективность выявления правонарушений и усилить превентивную функцию подразделений экономической безопасности.

В условиях цифровизации банковского сектора особую актуальность приобретает защита информационных систем и данных клиентов. Банки инвестируют значительные средства в современные системы кибербезопасности для противодействия преступлениям, предусмотренным гл. 28 УК РФ «преступления в сфере компьютерной информации».

Полагаем, что, помимо внедрения технических средств защиты, например шифрования данных и многофакторной аутентификации, важно уделять внимание повышению цифровой грамотности клиентов. Многие случаи хищения средств с банковских счетов происходят из-за недостаточной осведомленности пользователей о правилах безопасности в Интернете. Поэтому банки должны проводить регулярные информационные кампании, разъясняя клиентам основные методы защиты от кибермошенничества. Такие простые шаги, как использование сложных паролей, установка антивирусного программного обеспечения и игнорирование подозрительных ссылок, могут значительно снизить риски, чтобы не стать жертвой преступников.

Наконец, нельзя не отметить важность международного сотрудничества в сфере противодействия финансовым преступлениям. Многие схемы легализации преступных доходов и финансирования терроризма носят трансграничный характер, что требует тесной координации усилий банков и правоохранительных органов разных стран. Как подчеркивает Г.А. Тосунян, «развитие каналов обмена информацией, проведение совместных расследований и операций, унификация законодательства и правоприменительной практики – все это необходимые условия для эффективной борьбы с экономической преступностью в глобальном масштабе» [5].

В заключение подведем итоги, отметив, что особенности деятельности подразделений, занимающихся противодействием экономическим преступлениям, имеют решающее значение для эффективной борьбы с такого рода преступлениями. Успех в этой сфере зависит от комплексного подхода, включающего в себя совершенствование законодательства и правоприменительной практики, внедрение передовых технологий выявления и анализа финансовых преступлений, активное межведомственное и международное сотрудничество, повышение осведомленности сотрудников банков и их клиентов о методах противодействия противоправным действиям. Только объединив усилия государства, банковского сектора и общества, можно создать надежный заслон на пути экономической преступности и обеспечить стабильное развитие финансовой системы страны.

Нами разработаны следующие рекомендации по повышению квалификации сотрудников подразделений экономической безопасности и противодействия коррупции МВД России в области противодействия экономическим преступлениям в сфере информационных технологий.

Предлагаем разработать и внедрить специализированную программу повышения квалификации для сотрудников отдел по борьбе с экономическими преступлениями, направленную на углубленное изучение современных методов выявления, расследования и предотвращения экономических преступлений с использованием информационных технологий. Программа должна включать в себя следующие ключевые компоненты:

1. Изучение актуальных трендов и схем совершения экономических преступлений в сфере информационных технологий, таких как кибермошенничество, хищение конфиденциальных данных, использование криптовалют для отмывания денег и т.д.
2. Освоение передовых технологий анализа больших данных, машинного обучения и искусственного интеллекта, применяемых для выявления подозрительных финансовых операций и транзакций в режиме реального времени.
3. Развитие навыков использования специализированного программного обеспечения и аналитических инструментов для расследования экономических преступлений в цифровой среде.
4. Изучение особенностей сбора и анализа электронных доказательств, обеспечения их сохранности и допустимости в рамках уголовного судопроизводства.

5. Повышение уровня цифровой грамотности и информационной безопасности сотрудников отдела по борьбе с экономическими преступлениями, обучение методам защиты конфиденциальной информации и противодействия киберугрозам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / К.А. Барышева, Ю.В. Грачева, Г.А. Есаков и др.; под ред. Г.А. Есакова. – 7-е изд., перераб. и доп. – Москва: Проспект, 2019. – 736 с.

2. Трунцевский Ю.В. Экономические и финансовые преступления: понятие, виды, проблемы квалификации // Международное публичное и частное право. – 2019. – № 4. – С. 32–35.

3. Иванцов С.В. Организация деятельности подразделений экономической безопасности по выявлению и раскрытию преступлений в сфере экономики // Вестник Московского университета МВД России. – 2018. – № 3. – С. 116–120.

4. Корчагин А.Г. Правовые основы защиты лиц, сообщающих о фактах коррупции: сравнительный анализ законодательства России и зарубежных стран // Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – № 5. – С. 83–89.

5. Лунеев В.В. Криминология: учебник для вузов. – Москва: Юрайт, 2024. – 686 с.

6. Меняйло Д.В., Крупенникова К.К. О противодействии коррупции в условиях цифровой трансформации // Проблемы правоохранительной деятельности. – 2022. – № 3. – С. 28–32.

7. Тосунян Г.А. Противодействие легализации (отмыванию) преступных доходов и финансированию терроризма в банковской системе: международные стандарты и российская практика // Деньги и кредит. – 2020. – № 1. – С. 12–18.

СИСТЕМА СТАНДАРТИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Поликарпов Е.С.,
кандидат технических наук, доцент;
Рягузова П.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: кибербезопасность становится все более актуальной сферой в современном мире, где зависимость от информационных технологий продолжает расти. Угрозы, связанные с компьютерными инцидентами, стали неотъемлемым элементом нашей цифровой реальности. Для эффективного противодействия этим угрозам необходимы четкие и эффективные методы выявления и управления компьютерными инцидентами. В данной статье мы рассматривается система стандартизации в области выявления компьютерных инцидентов, исследуется важность стандартов, их роль в обеспечении кибербезопасности, а также их эволюция и современные вызовы. Этот анализ раскрывает значимость систем стандартизации и их воздействие на способность организаций адекватно реагировать на угрозы в цифровом мире.

Ключевые слова: информационная безопасность, компьютерная защита информации, защита информации, законодательство

STANDARDIZATION SYSTEM IN THE FIELD OF INFORMATION SECURITY

Polikarpov E.S.,
Candidate of Technical Sciences, Associate Professor;
Ryaguzova P.A.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: cybersecurity is becoming an increasingly relevant area in the modern world, where dependence on information technology continues to grow. Threats related to computer incidents have become an integral part of our digital reality. To effectively counter these threats, clear and effective methods of detecting and managing computer incidents are needed. In this article, we will consider the standardization system in the field of computer incident detection, exploring the importance of standards, their role in ensuring cybersecurity, as well as their evolution and modern challenges. This analysis is intended to shed light on the importance of standardization systems and their impact on the organization's ability to adequately respond to threats in the digital world.

Keywords: information security, computer information protection, information protection, legislation

Современные организации и государства сильно зависят от информационных технологий, что делает их уязвимыми к различным угрозам. Для обеспечения информационной безопасности и минимизации потенциальных рисков необходимы стандарты и нормы, которые помогают выявлять и эффективно реагировать на инциденты. Стандарты в области выявления компьютерных инцидентов играют важную роль в обеспечении безопасности информации. Они устанавливают единые методологии, практики и процедуры, которые организации и государства могут использовать для обнаружения и реагирования на инциденты. Стандарты также способствуют улучшению сотрудничества между структурами, обеспечивая более эффективное реагирование на угрозы.

Согласно Федеральному закону от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации», стандартизация – деятельность по разработке (ведению), утверждению, изменению (актуализации), отмене, опубликованию и применению документов по стандартизации и иная деятельность, направленная на достижение упорядоченности в отношении объектов стандартизации. В Российской Федерации систему служб стандартизации составляют: Госстандарт России, Госстрой России, группы специалистов в центральных подразделения по стандартизации, создаваемые субъектами (предприятиями, организациями).

Правовая основа дает нам несколько элементов системы информационной безопасности, каждую из которых регламентирует определенный технический комитет (далее – ТК), разрабатывающий нормативные документы, используемые в России. В таблице 1 представлены основополагающие направления и технические комитеты, регламентирующие их стандартизацию.

Таблица 1. Технические комитеты, организующие стандартизацию по направлениям информационной безопасности

Элемент информационной безопасности	Технический комитет	Специфика технического комитета
Защита информации	362 ТК	Разрабатывает средства защиты информации, информационно-телекоммуникационных систем, обеспечивает услуги и работы, связанные с этим направлением
Информационные технологии	22 ТК	Обеспечивает организацию информационных технологий, эффективность, качествао и безопасность информационных технологий во всех отраслях
Криптографическая защита информации	26 ТК	Разрабатывает нормативные документы по стандартизации, организовывающие работу криптографических механизмов

Защита информации (далее – ЗИ) является ключевой составляющей системы информационной безопасности. Этот раздел рассматривает методы и стандарты, связанные с физической и логической безопасностью информации, а также средствами обеспечения конфиденциальности данных. Защита информации – это комплекс мероприятий и технологий, направленных на обеспечение конфиденциальности, целостности и доступности информации, а также на защиту от несанкционированного доступа, использования, раскрытия, модификации и уничтожения информации.

Основополагающим стандартом Российской Федерации в области защиты информации является ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения».

Система стандартов по защите информации (далее – ССЗИ) – совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации. Законодательно установленная ССЗИ помогает урегулировать организованность в области ЗИ, что, в свою очередь, повысит эффективность ЗИ, работ по стандартизации, упорядочит структуру системы, разработки и учета стандартов. На рисунке 1 наглядно представлено разграничение в ССЗИ.

Следует помнить, что национальные стандарты (ГОСТы) в общем случае являются рекомендательными. Однако в ряде случаев обязательность следования стандартам и спецификациям закреплена законодательно. В соответствии со ст. 6 Федерального закона ри 29 июня 2015 г. № 162 «О стандартизации в Российской Федерации» в том случае, если речь идет о «стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также в отношении процессов и иных объектов стандартизации, связанных с такой продукцией», стандарты являются обязательными к применению.

Информационные технологии (далее – ИТ) – это совокупность средств, методов и процессов, используемых для сбора, обработки, передачи и хранения информации с использованием компьютерных систем и программного обеспечения.

Стандарты в области информационных технологий содержат требования к средствам вычислительной техники и сетям, программному и информационному обеспечению, информационным системам и т.д. К данным стандартам относятся стандарты жизненного цикла системы, взаимосвязи и среды открытых систем, а также стандарты, регулирующие документацию программного обеспечения и сферу информационной безопасности ИТ.

Основным документом, регламентирующим деятельность в области стандартизации информационных технологий, является Федеральный закон от 27.10.2002 № 184-ФЗ «О техническом регулировании» в котором прописано,

что стандарты, регулирующие требования к безопасности, охраны здоровья и окружающей среды, являются обязательными к выполнению как гражданами Российской Федерации, так и субъектами, участвующими в производстве, создании, снабжении и продаже компонентов и средств информационных систем.

Ключевую роль в стандартизации данной сферы занимают международные организации и принимаемые ими стандарты. Международной организацией, в которой разрабатываются стандарты в области информационно-телекоммуникационных технологий, является JTC1 ISO/IES. Структура ТК 22 зеркально отображает ее структуру, подразделяясь на:

1. ИСО (система сертификации).
2. МЭК (система стандартизации в области электротехники).

Благодаря данной организации, появились следующие программы по стандартизации. STEP – международная программа, направленная на разработку стандарта по обмену данными, который обеспечивает полное описание изделия для передачи информации от одной системы автоматизированного программирования к другой, независимо от отрасли промышленности. ESPRIT – региональная программа, в рамках которой проводятся работы по стандартизации и обеспечению качества информационных технологий.

Криптографическая защита информации – это множество технических и организационных мероприятий, направленных на обеспечение безопасности компьютерных систем, данных и информации, а также на предотвращение несанкционированного доступа, разрушения, модификации или утечки информации.

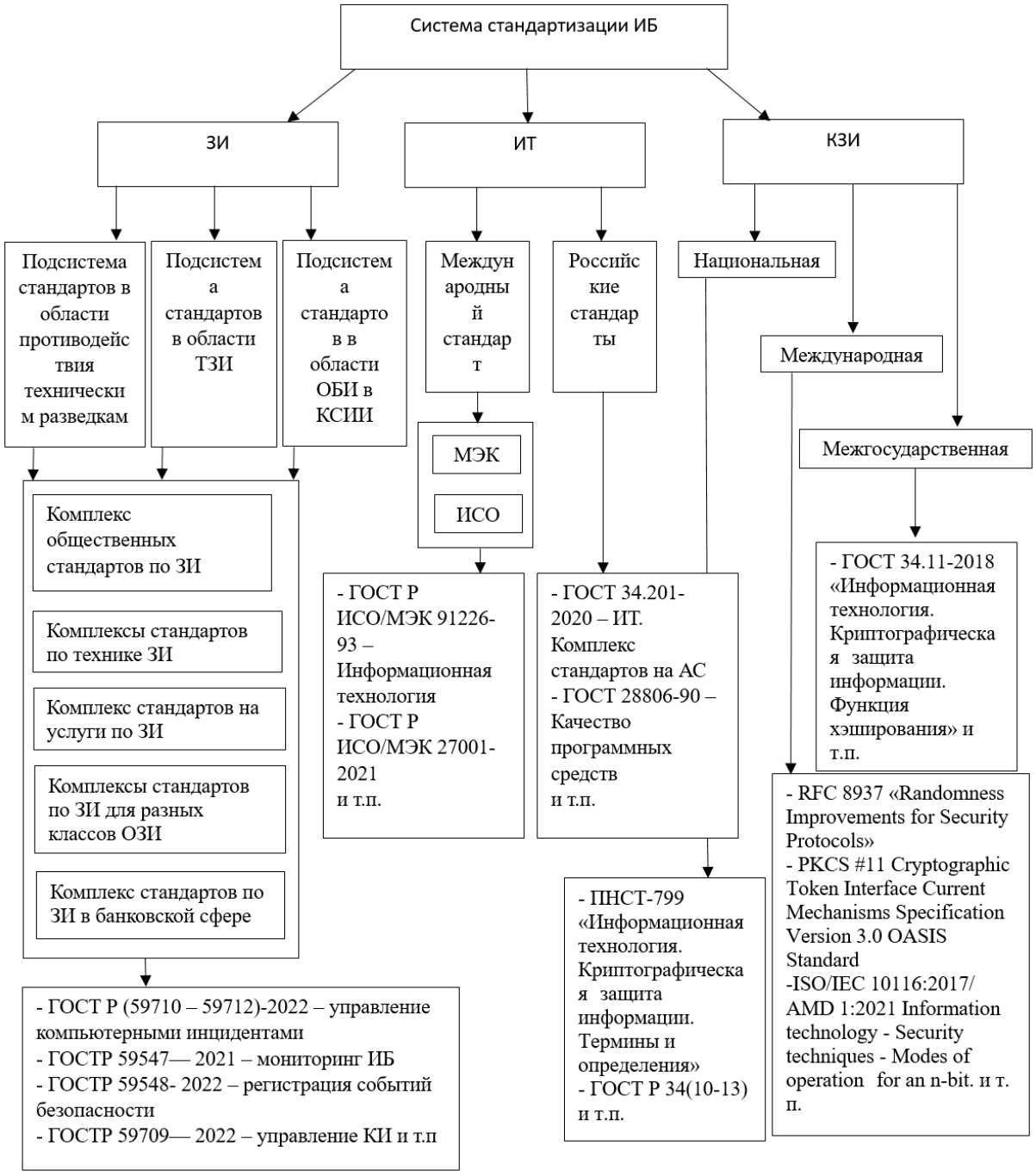


Рисунок 1. Система стандартизации информационной безопасности

В заключение важно отметить, что стандартизация информационной безопасности в литературе и среди специалистов – неустоявшаяся дефиниция. В современном мире существует множество законодательных актов в области информационной безопасности, поэтому комплекс мер по стандартизации необходим.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Цветков В.Я. Стандартизация информационных программных средств и программных продуктов. – Москва: МГУГиК, 2000. – 116 с.

2. Клишин Д.В., Чечулин А.А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 37–54.

3. Основы кибербезопасности в деятельности сотрудников правоохранительных органов / Прокопенко А.Н., Страхов А.А., Ковалева Е.Г., Акапьев В.Л., Гаврющенко А.П., Рыбальченко А.Ю. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – 153 с.

4. Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс».

5. Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс».

6. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения [Электронный ресурс] // СПС «Гарант».

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ КОНТЕЙНЕРИЗАЦИИ ДЛЯ ОРГАНИЗАЦИИ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Попов А.В.,
кандидат технических наук
(Воронежский институт МВД России)

Аннотация: рассматривается возможность и перспективы использования технологий контейнеризации при оптимизации организации серверной инфраструктуры органов внутренних дел. Оценивается текущее состояние серверной инфраструктуры, построенной на технологиях виртуализации. Обосновывается рациональность использования контейнеризации, перспективы ее использования в деятельности подразделений органов внутренних дел.

Ключевые слова: контейнеризация, инфраструктура, серверы, виртуализация, гипервизоры, сети связи

USING CONTAINERIZATION TECHNOLOGIES TO ORGANIZE SERVER INFRASTRUCTURE OF INTERNAL AFFAIRS BODIES

Popov A.V.,
Candidate of Technical Sciences
(Voronezh institute of the Ministry of the Interior of Russia)

Abstract: the article considers the possibility and prospects of using containerization technologies to optimize the organization of server infrastructure of internal affairs bodies. The current state of the server infrastructure built on virtualization technologies is evaluated. The rationality of the use of containerization and the prospects of its use in the activities of internal affairs departments are substantiated.

Keywords: containerization, infrastructure, servers, virtualization, hypervisors, communication networks.

Реализация полномочий органов внутренних дел по охране общественного порядка и обеспечению общественной безопасности сопряжена с обязательной и непрерывной координацией сил и средств полиции, а также информационным обеспечением их деятельности. Наряду с этим обеспечение надежного и бесперебойного функционирования систем и сетей связи, информационных систем (далее – ИС) различного назначения, баз данных, серверов и прочих элементов внутренней информационно-телекоммуникационной инфраструктуры территориальных органов МВД России является одной из наиболее приоритетных задач инженерного состава подразделений информационных технологий, связи и защиты информации.

Как правило, под информационно-телекоммуникационной инфраструктурой понимается комплекс вычислительной техники, программных и аппаратных средств, обеспечивающих информационное взаимодействие между элементами информационной сферы различного уровня и назначения. К таким элементам могут относиться различные сервисы, базы данных, удаленные рабочие столы сотрудников, ERP- и CRM-системы и т.д.

К аппаратной части относятся периферийное сетевое оборудование, серверы, персональные абонентские устройства. Доступ пользователей к различным сервисам осуществляется посредством предоставления необходимых вычислительных мощностей серверным оборудованием, в то время как программная часть включает в себя хостовые и гостевые операционные системы (далее – ОС), гипервизоры, базы данных и системы управления ими, брандмауэры и др. Полная совокупность используемых инструментов определяется инженерным персоналом.

Рассматривая серверную инфраструктуру органов внутренних дел, следует отметить, что наиболее важными требованиями в таких ИС являются отказоустойчивость, масштабируемость и безопасность. Данные требования соблюдаются при использовании рационально подобранного комплекса аппаратных и

программных средств, грамотно выбранной топологии и инфраструктуры сети. Пример защищенного сегмента представлен на рис. 1.

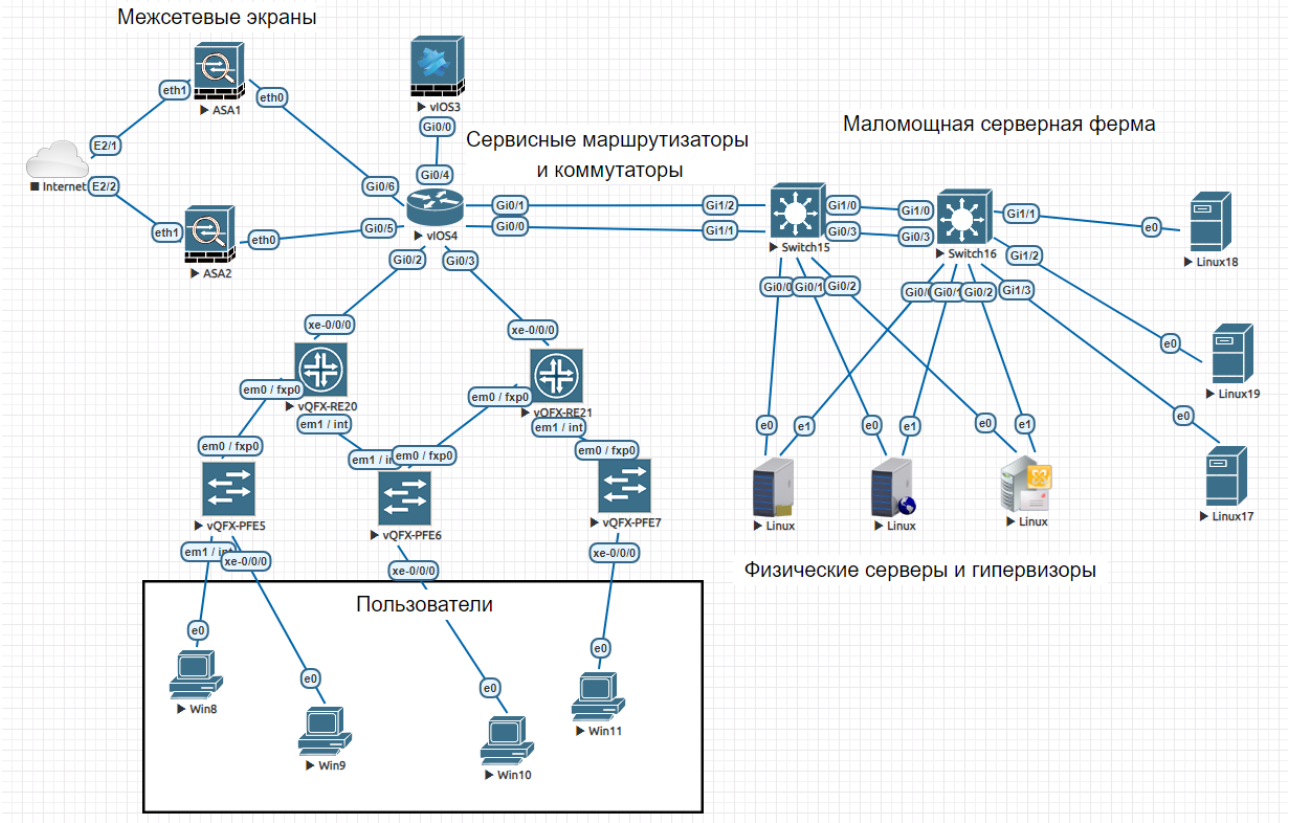


Рисунок 1. Пример реализации внутренней инфраструктуры сети

Как видно из рисунка 1, определенное количество ресурсов сети выделяется на организацию серверов и их поддержку. В таком случае на инженерный состав, отвечающий за их обслуживание, возлагаются следующие обязанности [6]:

– непрерывный аудит серверного и сетевого оборудования;

– анализ и оценка используемого программного обеспечения;

– разработка рекомендаций по модернизации серверного программно-аппаратного комплекса;

– техническое обслуживание оборудования с требуемой периодичностью;

– мультивендорное взаимодействие;

– исследование и анализ проблем безопасности и защиты от несанкционированного доступа.

С 2000-х годов сервисы и приложения разворачивались на физических серверах необходимой мощности [2, с. 18]. Однако у таких технологий были достаточно серьезные проблемы с масштабированием, поскольку при увеличении количества пользователей в сегментах и расширения сервисного функционала требовалось больше вычислительных мощностей и, соответственно, более современного оборудования.

Немного позднее появилась технология виртуализации, обладающая большей, но все еще недостаточной масштабируемостью. Благодаря ей использованию стало возможно использовать имеющиеся свободные мощности на

серверах для запуска дополнительных сервисов без покупки нового оборудования. Однако для запуска каждой виртуальной машины требовалось достаточно много ресурсов для запуска и поддержки ее ОС, которая требует обслуживания, установки обновлений, исправления ошибок, а также лицензий.

На данный момент в подразделениях МВД России большое количество серверов различного назначения (FTP, DNS, DHCP, SMTP, видеоконференцсвязи, HTTP) развернуты именно в средах виртуализации и функционируют посредством использования гипервизоров (платформ для создания и запуска виртуальных машин). Однако в силу приведенных выше причин такая инфраструктура не является оптимальной.

В настоящее время в сфере IT используется и активно развивается технология контейнеризации [1–3, 5], первостепенной является система Linux Container. Основные отличия между системами виртуализации и контейнеризации представлены на рис. 2.

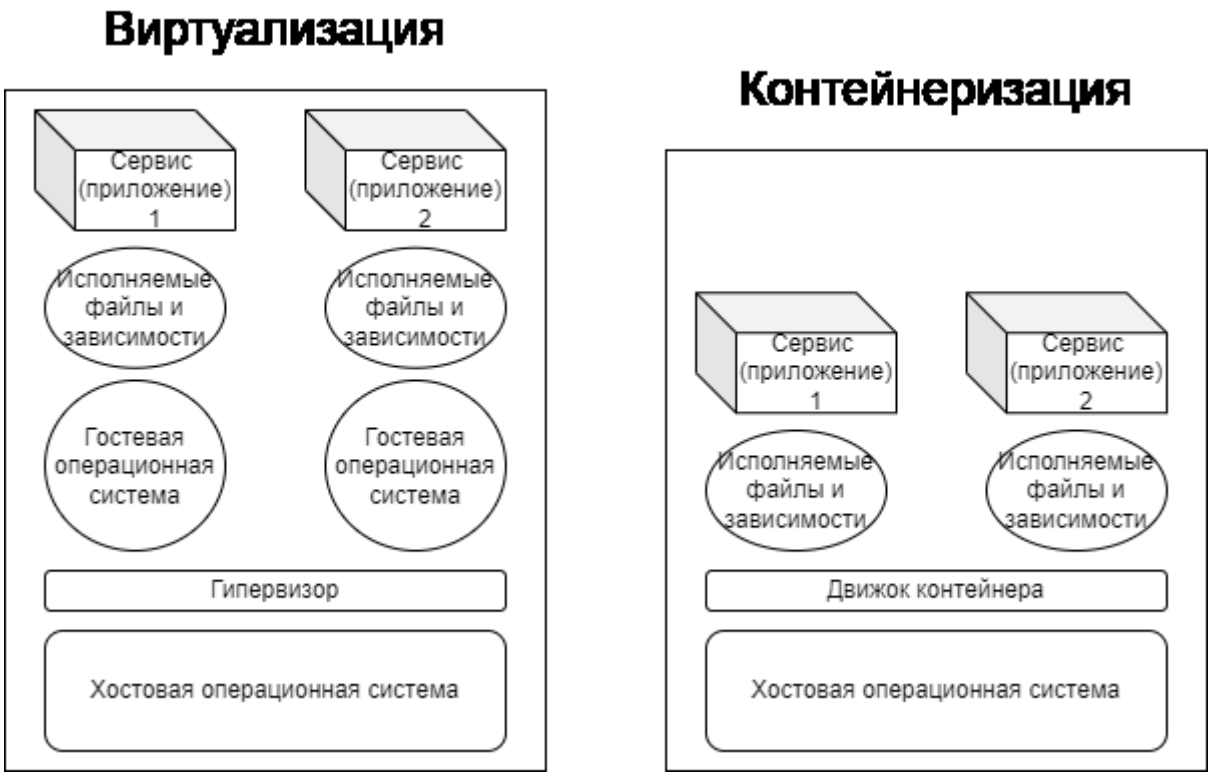


Рисунок 2. Структурная схема ресурсов виртуальной машины и контейнера

Как видно из рис. 2, контейнеру не требуется использование гостевой ОС, поскольку он использует ядро хостовой. В результате чего процессы его запуска занимают намного меньше времени, чем запуск виртуальной машины и составляют порядка нескольких секунд.

Помимо этого контейнеры вмещают в себя не только конкретное приложение или сервис, но и необходимые файлы конфигурации, библиотеки и другие зависимости, необходимые для его развертывания и функционирования, т.е. фактически он может быть перенесен в любую другую среду либо ОС в том виде, в котором был «собран» [4].

Основными преимуществами использования технологий контейнеризации являются:

- меньшая потребляемость ресурсов хостовых ОС;
- отсутствие слоя гипервизора, что позволяет разместить намного больше контейнеров на одном физическом сервере;
- легкость запуска и масштабирования;
- изолированная среда функционирования контейнера;
- идентичность среды разработки и рабочей среды;
- возможность использования для конвейера непрерывной интеграции и доставки (CI/CD процессов);
- возможность использования оркестраторов контейнерных нагрузок для балансировки и распределения трафика запросов к серверной инфраструктуре.

Таким образом, использование технологии контейнеризации является рациональным решением по оптимизации функционирования серверной инфраструктуры ИС органов внутренних дел. Следует отметить, что при реализации мер по ее внедрению в деятельность подразделений МВД России возникнут определенные трудности, связанные, в первую очередь, с необходимостью стандартизации данной технологии. Юридическая составляющая в данном случае является неотъемлемым аспектом при модернизации серверной инфраструктуры ИС органов внутренних дел, поскольку определенный кластер контейнеров работает на базе программного обеспечения Docker, обладающего открытым исходным кодом, что чревато наличием определенных уязвимостей. Однако при грамотном подходе к построению инфраструктуры, использованию методов обеспечения информационной безопасности технология контейнеризации может стать эффективным инструментом обеспечения функционирования ИС органов внутренних дел при реализации их полномочий по охране общественного порядка и обеспечению общественной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверина П. Контейнеризация понятным языком: от самых азов до тонкостей работы с Kubernetes [Электронный ресурс]. – URL: https://habr.com/ru/companies/slurm/articles/ (дата обращения: 10.05.2024).

2. Гош С. Docker без секретов / пер. с англ. – Санкт-Петербург: БХВ-Петербург, 2024. – 224 с.

3. Контейнеризация [Электронный ресурс]. – URL: https://blog.skillfactory.ru/glossary/kontejnerizacziya (дата обращения: 05.05.2024).

4. Маркелов А. Введение в технологии контейнеров и Kubernetes. – Москва: ДМК Пресс, 2019. – 194 с.

5. Парминдер С.К. Микросервисы и контейнеры Docker. – Москва: ДМК Пресс, 2019. – 240 с.

6. Серверная инфраструктура [Электронный ресурс]. – URL: https://sky-dynamics.ru/stati/servernaya-infrastruktura/ (дата обращения: 10.05.2024).

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Пупынина А.А.;
Самойлова Ю.М.,
кандидат технических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: на сегодняшний день процент киберпреступлений достаточно высок. По мере прогрессивного развития области информационно-коммуникационных технологий широко распространились случаи выявления преступлений в информационно-цифровом пространстве. Законодатель вынужден непрерывно совершенствовать действующие мера и предпринимать новые по противодействию таким преступлениям. Существующие комплексы профилактических мер находят свое отражение в Уголовном Кодексе Российской Федерации, приказах МВД России, а также иных нормативно-правовых актах, регламентирующих действия по профилактике правонарушений в сфере информационных технологий.

Ключевые слова: информационно-коммуникационные технологии, электронно-финансовые операции, мошенничество, преступление, денежные средства, нормативно-правовой акт, правовые основы профилактики.

CRIME PREVENTION IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Pupynina A.A.;
Samoilova J.M.,
Candidate of Technical Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: now the percentage of cybercrimes is quite high. With the progressive development of the field of information and communication technologies, cases of detection of crimes in the information and digital space have become widespread. The legislator is forced to continuously improve existing and take new measures to counteract such crimes. To date, complexes of preventive measures are reflected in the Criminal Code of the Russian Federation, orders of the Ministry of Internal Affairs of Russia, as well as other normative legal acts regulating actions for the prevention of offenses in the field of information technology.

Keywords: information and communication technologies, electronic financial transactions, fraud, crime, money, regulations, legal framework for prevention.

В XXI веке информационные технологии стали охватывать практически все сферы жизни общества. Прежде всего это обусловлено интенсивной модернизацией различных технических средств связи, средств вычислительной техники, а также появлением новых отраслей в области информационно-компьютерных технологий и их дальнейшим совершенствованием.

Однако даже такие положительные достижения современной науки нередко влекут за собой наступление неблагоприятных последствий [1, с. 43]. Так, по мере прогрессивного развития области информационных технологий, постепенно распространялись и случаи выявления преступлений в информационно-цифровом пространстве.

На сегодняшний день процент киберпреступлений достаточно высок.

Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц.

Наиболее часто встречаются преступления с электронно-финансовыми операциями, где воровство безналичных средств у граждан с их банковских счетов происходит с помощью реквизитов платежных карт, а также путем взлома личного кабинета физического лица в онлайн-банкинге [2, с. 226].

Как правило, для совершения таких преступлений злоумышленники используют различные технические и программные средства оказания услуг связи. С помощью электронной техники (мобильных телефонов, компьютеров, ноутбуков и иных средств связи) правонарушители, посредством телефонного звонка, переписки в социальных сетях и на других онлайн-платформах для коммуникации, связываются с гражданином и далее действуют по одной из четко разработанных и наиболее эффективных схем. Например, злоумышленники часто «играют роль» сотрудников банка. Потерпевшему поступает телефонный звонок, в процессе диалога мошенники представляются сотрудниками службы безопасности банка, клиентом которого является потерпевший, и сообщают заведомо ложную информацию о том, что денежные сбережения гражданина были подвергнуты некой опасности (произведен неверный платежный перевод, взлом личного кабинета или попытка взять кредит на имя потерпевшего). После чего, действуя по разработанному алгоритму и используя тонкие психологические приемы, мошенникам удается завладеть доступом к электронным счетам гражданина, откуда в скором времени списывается крупная денежная сумма.

Следующим распространенным способом, который используют злоумышленники, является имитирование в телефонном разговоре ситуации, в которой родственник потерпевшего якобы попал в беду, например, в дорожно-транспортное происшествие, произошедшее по его вине. Потерпевший, в порыве желания помочь своему близкому человеку, как правило, идет на любые условия, поставленные преступниками.

Также не менее распространенными считаются телефонные мошенничества, в процессе которых жертве сообщается о возможности поучаствовать в беспроигрышной лотерее или конкурсе. Тонкие психологические приемы позволяют мошенникам с легкостью оказать незаметное давление на человека, по-

сле чего он соглашается на фиктивное участие и переводит свои финансовые средства на счет злоумышленников.

Широко распространено и мошенничество под предлогом телефонного вируса. Как правило, гражданину приходит смс-сообщение, в котором содержится информация о том, что его мобильное устройство было подвергнуто проникновению вредоносного программного обеспечения, которое может исключить возможность дальнейшего функционирования устройства. В СМС-сообщении указывается ссылка, по которой необходимо перейти для устранения данной проблемы, или, например, для скачивания антивирусной программы. При переходе по предоставленной ссылке в телефон действительно проникает вирус и осуществляется списание денежных средств со счетов потерпевшего.

Все вышеперечисленные противоправные деяния объединены общей целью – хищением денежных средств, а значит, должны иметь и единую правовую основу профилактики в данной области. С учетом быстрого роста уровня такого вида киберпреступности, законодатель совершенствует действующие и создает новые нормативно-правовые акты, регламентирующие порядок действий сотрудников правоохранительных органов при раскрытии таких преступлений, а также порядок действий граждан, столкнувшихся с возможностью стать жертвой таких преступлений [3, с. 33]. Так, например, в приказе МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений установлены требования к проверке сообщений о преступлениях в сфере информационных технологий, а также к принятию незамедлительных мер по установлению всех обстоятельств и раскрытию такого преступления: «Проведение проверки сообщения о преступлениях, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, в ходе которой незамедлительно принимать исчерпывающие меры к раскрытию преступлений и установлению лиц их совершивших, направлять в установленном порядке запросы в кредитные организации, операторам связи, оказывающим услуги связи, в том числе по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет, получать объяснения от заявителя и возможных очевидцев преступления» [4]. Данный нормативно-правовой документ предписывает осуществление принятия решения о возбуждении уголовного дела в органе внутренних дел, в который поступило сообщение о преступлении в сфере информационных технологий, независимо от места его совершения. Далее данное заявление будет передано соответствующему территориальному органу МВД России для дальнейшего разбирательства.

Поскольку противоправные деяния в сфере информационных технологий являются преступлениями, их правовая регламентация содержится в Уголовном Кодексе Российской Федерации (далее – УК РФ). Санкции, налагаемые на правонарушителя, в какой-то мере также носят профилактический характер. Преступлениям в сфере компьютерной информации уделена целая глава. В качестве примера необходимо привести несколько положений из УК РФ. Статья 273 предполагает наступление уголовной ответственности за «создание, распро-

странение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для уничтожения, блокирования, модификации, копирования компьютерной информации…» [5]. Также, например, статьей 159.6 УК РФ предусмотрена ответственность за мошенничество в сфере компьютерной информации. На самом деле УК РФ регулирует достаточно большой объем преступлений в сфере информационных технологий. Огромное значение при попытках совершения преступлений в области информационно-компьютерных технологий имеют действия самого гражданина, поэтому государство предпринимает комплекс мер по обеспечению осведомленности слоев населения о существующих современных явлениях. Так, к правовым основам профилактики преступлений в сфере информационных технологий можно отнести регулярные плановые профилактические работы, проводимые сотрудниками органов внутренних дел. В ходе таких мероприятий граждане получают от сотрудника наиболее полную информацию о распространенных в настоящее время схемах мошенничества с использованием информационной техники, а также о способах, позволяющих избежать подобные неприятности. Также совместными усилиями подразделений МВД России с органами государственной власти осуществляется регулярная демонстрация видеороликов и трансляция голосовых объявлений в местах проведения крупных мероприятий или массового скопления людей о существующих видах мошенничества в сфере компьютерных технологий. В наиболее оптимальных местах устанавливаются баннеры с краткой информацией о специфике преступлений, совершаемых с помощью достижений современных технологий, а также с информацией о том, в каком случае и в какие подразделения органов внутренних дел гражданину необходимо обратится в случае выявления признаков подобных преступлений.

Исходя из всего вышесказанного, можно сделать вывод о том, что в современном мире тенденция совершения преступлений в сфере информационных технологий имеет высокую скорость развития, а соответственно, законодатель вынужден непрерывно совершенствовать действующие меры и предпринимать новые по противодействию таким преступлениям. На сегодняшний день комплексы профилактических мер находят свое отражение в УК РФ, приказах МВД России, а также иных нормативно-правовых актах, регламентирующих действия по профилактике правонарушений в сфере информационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Колчевский И.Б., Бицадзе Г.Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. – 2021. – № 2. – С. 40–47.

2. Гумаров И.А., Саетгараев В.Ф. Некоторые проблемы организации работы оперативных подразделений органов внутренних дел по противодействию мошенничествам общеуголовной направленности // Вестник Казанского юридического института МВД России. – 2018. – № 3. – С. 223–229.

3. Ульянов М.В. Преступления, совершаемые с использованием информационных технологий: динамика и тенденции // Общество и право. – 2020. – № 4. – С. 32–36.

4. Приказ МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» // Официальный сайт Управления на транспорте МВД России по Южному федеральному округу [Электронный ресурс]. – URL: https://юфоут.мвд.Российской Федерации/ (дата обращения: 30.04.2024).

5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 06.04.2024) [Электронный ресурс] // СПС «КонсультантПлюс».

УЧЕТ ПРАВОВОГО РЕГУЛИРОВАНИЯ УСЛУГ ЦИФРОВОГО ОБЩЕСТВА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ (ОПЫТ РЕСПУБЛИКИ МОЛДОВА)

Редкоус В.М.,
доктор юридических наук, профессор
(Институт государства и права РАН, Академия управления МВД России)

Аннотация: в статье на основе анализа положений Закона Республики Молдова от 22 июля 2004 г. № 284-XV «Об услугах информационного общества» показаны возможности учета правового регулирования услуг цифрового общества в деятельности органов внутренних дел.

Ключевые слова: органы публичного управления, органы внутренних дел; услуги информационного общества; поставщики услуг, посредники; сотрудничество, правовой режим электронных сообщений, мониторинг и контроль услуг информационного общества, национальная безопасность, сравнительное правоведение.

TAKING INTO ACCOUNT THE LEGAL REGULATION OF DIGITAL SOCIETY SERVICES IN THE ACTIVITIES OF INTERNAL AFFAIRS BODIES (EXPERIENCE OF THE REPUBLIC OF MOLDOVA)

Abstract: the article, based on an analysis of the provisions of the Law of the Republic of Moldova of July 22, 2004 № 284-XV “On Information Society Services,” shows the possibilities of taking into account the legal regulation of digital society services in the activities of internal affairs bodies

Keywords: public authorities; internal affairs bodies; information society services; service providers; intermediaries; cooperation; legal regime of electronic communications; monitoring and control of information society services; National security; comparative law.

В настоящее время одним из приоритетных направлений научных исследований вопросов обеспечения общественной безопасности и охраны общественного порядка является повышение эффективности деятельности органов внутренних дел, являющихся ведущими в системе органов исполнительной власти органами, наделенными компетенцией в рассматриваемой области [1, 96 с.; 2, с. 93–94; 3; 4]. Этот вопрос является актуальным и для области услуг информационного общества, которые активно развиваются и в России, и за рубежом, в том числе и государствах – участниках СНГ [5; 6, с. 357–363; 7, с. 1–11; 8, с. 82–97; 9, с. 29].

Рассмотрим опыт Республики Молдова (далее – РМ), где был принят Закон Республики Молдова от 22 июля 2004 г. № 284-XV «Об услугах информационного общества» (далее – Закон РМ) [10].

В деятельности органов внутренних дел сотрудникам необходимо четко учитывать пределы действия закона. Это важно для сотрудников органов внутренних дел любого государства, реализующего свои полномочия в той или иной сфере. Поэтому следует учитывать, что рассматриваемый Закон РМ применяется к поставщикам услуг, зарегистрированным и/или учрежденным в РМ, поставщикам услуг, деятельность которых направлена на РМ, а также к предоставляемым ими услугам.

Так, деятельность поставщика услуг, представленная на его веб-странице или веб-странице посредника, считается направленной на РМ, если еще до предполагаемого заключения договора с потребителем, проживающим на территории РМ, соответствующие веб-страницы и глобальная деятельность поставщика достаточно ясно свидетельствуют о его намерении вступить в индивидуальном порядке в торговые отношения с потребителями, проживающими в РМ или на территории нескольких стран, включая РМ.

Сочетание по меньшей мере двух из следующих элементов, перечень которых не является исчерпывающим, может являться признаком того, что деятельность поставщика услуг направлена на страну проживания потребителя: международный характер деятельности; указание нескольких маршрутов с отправной точкой из других стран до местонахождения поставщика услуг; использование языка или валюты, обычно применяемых в стране местонахождения потребителя, при условии, что они отличаются от языка или валюты, обычно используемых в стране местонахождения поставщика услуг, и возможность забронировать или подтвердить бронь именно на этом языке; оплата соответствующих услуг службы интернет-ссылок с целью облегчения доступа лиц, находящихся в стране проживания потребителя, к веб-странице или к услугам поставщика услуг или посредника; использование имени домена высшего уровня, отличного от названия страны местонахождения поставщика услуг.

Признаками, являющимися недостаточными для определения, что деятельность поставщика услуг направлена на страну проживания потребителя, являются: доступность веб-страницы и/или услуг поставщика либо его посредника в стране, на территории которой проживает получатель; указание адреса электронной почты и другой контактной информации; указание языка или валюты, которые обычно используются в стране местонахождения поставщика услуг.

Достоинством Закона РМ является раскрытие в нем основных используемых понятий: «электронное сообщение», «коммерческое сообщение», «потребитель», «получатель услуг», «поставщик услуг, учрежденный в определенной стране», «электронная почта», «услуга информационного общества», «услуга, предоставленная с помощью электронных средств» и ряда других.

Выделим базовое понятие – «*услуга информационного общества*», под которой понимается любая услуга с целью получения вознаграждения, предоставляемая на расстоянии при помощи электронных средств и по индивидуальному запросу получателя услуги, включая продажу товаров в режиме онлайн. Услуги информационного общества не ограничиваются исключительно услугами, в результате которых заключаются онлайновые договоры, но в той мере, в какой они представляют собой экономическую деятельность, включают и услуги, предоставление которых не оплачивается получателем услуг, например, рассылка информации в режиме онлайн или коммерческих сообщений либо услуги, предоставляющие инструменты поиска, доступа и восстановления данных. Услугами информационного общества являются и услуги, состоящие в передаче информации посредством сети электронных коммуникаций, в обеспечении доступа к сети электронных коммуникаций или размещении информации, предоставляемой получателем услуги. Услуги, которые передаются в режиме «точка-точка», такие как предоставление видеоуслуг по запросу или рассылка коммерческих сообщений по электронной почте, также являются услугами информационного общества.

В понимании настоящего закона не являются услугами информационного общества следующие виды деятельности: услуги, оказанные в присутствии поставщика и получателя, даже если при этом предполагается использование электронного оборудования; услуги, имеющие материальное выражение, даже если они оказываются посредством электронных средств; услуги, предоставленные без использования сети Интернет (офлайн-услуги), такие как распространение программ на устройствах для хранения данных; услуги, которые не предоставляются посредством систем электронной обработки и хранения данных, а именно – услуги голосовой телефонии, факс/телекс; услуги, предоставленные посредством голосовой телефонии или факса; прямые продажи по телефону/факсу; услуги, оказанные путем передачи данных без индивидуального запроса с целью их одновременного получения неограниченным количеством индивидуальных получателей (передача в режиме «точка–многоточка»), такие как услуги трансляции или ретрансляции аудиовизуальных программных комплексов, телетекст.

В соответствии с ч. 5 ст. 5 Закона РМ предоставление услуг информационного общества поставщиком услуг, учрежденным в другой стране, не может быть ограничено на территории РМ при условии соблюдения им положений национального законодательства. Положения вышеназванного абзаца не применяются: к авторским и смежным правам, а также к правам промышленной собственности; к эмиссии электронных денег; к рекламе организаций коллективного инвестирования; к страховой деятельности; к свободному выбору сторонами права, применимому к их договору; к договорным обязательствам, вы-

текающим из договоров, заключенных потребителями; к формальному признанию договоров, которые создают или передают права на недвижимое имущество, в случае, если соответствующие договоры подпадают под формальные обязательные положения законодательства государства, на территории которого находится недвижимое имущество; к авторизации незапрошенных по электронной почте коммерческих сообщений.

Однако в отступление от положений ч. (5) ст. 5 Закона РМ уполномоченные органы публичной власти могут принимать меры, необходимые для поддержания общественного порядка, предотвращения, расследования и раскрытия преступлений, осуществления уголовного преследования, защиты несовершеннолетних, для борьбы с призывами в любой форме к розни по признаку расы, пола, религии или национальности, с унижением человеческого достоинства, для защиты здоровья населения, национальной обороны и безопасности, для защиты потребителей и инвесторов. Перечисленные меры применяются в соответствии с положениями, установленными действующими законодательными и иными нормативными актами, против любых услуг информационного общества, которые угрожают или представляют серьезный риск нанесения вреда достижению вышеперечисленных целей, а также должны быть соразмерны этим целям.

Электронная почта – это «любое текстовое, голосовое, звуковое или графическое сообщение, отправленное посредством сети электронных коммуникаций общего пользования, которое может быть сохранено в сети или оконечном оборудовании получателя услуг до его открытия получателем».

Субъектами отношений по предоставлению услуг информационного общества могут быть физические и юридические лица, в том числе иностранные, независимо от вида собственности и организационно-правовой формы (за исключением лиц, осуществляющих деятельность на основе предпринимательского патента), а также государство как субъект права, которые участвуют в отношениях по предоставлению услуг информационного общества в качестве: 1) поставщиков услуг; 2) получателей услуг; 3) посредников в отношениях по предоставлению услуг информационного общества.

Получатели услуг несут в соответствии с законом ответственность за содержание информации, по их запросу переданной и хранящейся посредством сетей электронных коммуникаций поставщиками услуг.

Поставщик услуг обязан предоставлять получателям услуг и государственным контрольным органам свободный, прямой и постоянный доступ к достоверной информации о себе в электронной форме на румынском языке. По собственной инициативе данная информация может быть предоставлена дополнительно и на любом другом широко используемом языке.

В целях обеспечения обмена электронными документами и электронными сообщениями поставщики и получатели услуг могут на договорной основе пользоваться услугами посредника в отношениях по предоставлению услуг информационного общества, связанных с организацией и управлением соответствующими информационными системами и сетями электронных коммуникаций.

Нарушение поставщиками услуг положений настоящего закона влечет по обстоятельствам гражданскую, уголовную или правонарушительную ответственность согласно закону. Поставщики услуг несут ответственность за предоставленную по собственной инициативе или от своего имени информацию.

В случае если услуга информационного общества состоит в хранении информации, предоставленной получателем услуги, поставщик услуг не несет ответственности за хранимую информацию по запросу соответствующего получателя услуги (формы хранения, именуемые hosting) при условии, что поставщик услуг не располагает сведениями о том, что деятельность или хранящаяся информация незаконна, и в отношении исков о возмещении ущерба не осведомлен о фактах или обстоятельствах, свидетельствующих о незаконном характере соответствующей деятельности или информации.

Поставщик услуг обязан незамедлительно принять меры по удалению информации или блокированию доступа к ней с момента обнаружения незаконного характера деятельности или хранящейся информации.

Считается, что поставщик услуг осведомлен о незаконном характере деятельности или хранящейся информации либо о фактах или обстоятельствах, свидетельствующих о явной незаконности соответствующей деятельности или информации, в случае, если поставщик:

a) получает в письменной форме изданное в соответствии с положениями законодательства распоряжение судебной инстанции или уполномоченного органа публичной власти, в котором констатируется незаконный характер деятельности или специфической информации, хранящейся на серверах поставщика услуг или на подконтрольных ему серверах, с требованием удалить соответствующую веб-страницу или заблокировать доступ к ней;

b) получает письменное уведомление (в оригинале) от заинтересованного лица, в котором последнее сообщает под свою ответственность, что определенная деятельность или специфическая информация, хранящаяся на серверах поставщика или на подконтрольных ему серверах, является незаконной, с требованием удалить соответствующую веб-страницу или заблокировать доступ к ней.

Уведомление, указанное в пункте b) части (3) ст. 17 Закона РМ, считается действительным, если содержит следующие сведения: a) дату уведомления; b) фамилию, имя, место проживания, гражданство, дату и место рождения, место работы в случае, если уведомляющая сторона является физическим лицом; название, организационно-правовую форму, юридический адрес, фамилию и имя администратора (руководителя), если уведомляющая сторона является юридическим лицом; c) фамилию, имя и место проживания получателя уведомления или – в случае юридического лица – название и юридический адрес; d) описание оспариваемых фактов и точное местонахождение; e) причины, по которым данная информация должна быть удалена или заблокирована, включая ее указание и доказательства, свидетельствующие о предполагаемых фактах; f) копию письма, адресованного автору или издателю оспариваемой информации или деятельности, с требованием удалить или блокировать информацию либо доказательства невозможности установления контактов с автором.

После получения уведомления, указанного в пункте b) части (3) ст. 17 Закона РМ, поставщик услуг без необоснованного промедления отсылает уведомление получателю услуг, которому оказывает услуги по хранению соответствующей веб-страницы. Получатель услуг без необоснованного промедления сообщает в письменной форме поставщику услуг о своем согласии или несогласии с поступившим требованием. В случае получения поставщиком услуг несогласия получателя соответствующей услуги в течение 10 рабочих дней со дня отправки уведомления, указанного в пункте b) части (3) ст. 17 Закона РМ, он освобождается от обязанности удалить соответствующую веб-страницу или заблокировать доступ к ней. По требованию заинтересованного лица судебная инстанция вправе обязать поставщика удалить соответствующую веб-страницу или заблокировать доступ к ней. В случае получения поставщиком услуг письменного согласия получателя соответствующей услуги или отсутствия ответа в течение 10 рабочих дней со дня отправки уведомления, указанного в пункте b) части (3) ст. 17 Закона РМ, поставщик услуг обязан незамедлительно удалить соответствующую веб-страницу или заблокировать доступ к ней.

Положения части (1) ст. 17 Закона РМ не применяются в случае, если получатель услуги действует под руководством или под контролем поставщика услуг.

Органы внутренних дел РМ и органы национальной безопасности РМ наделены полномочиями по мониторингу и контролю услуг информационного общества.

Важно учитывать закрепленные в Законе РМ обязанности поставщиков услуг (ст. 25).

Так, поставщики, оказывающие услуги доступа в Интернет или постоянного хранения информации, обязаны предоставлять в распоряжение общественности доступные и видимые инструменты (средства), позволяющие любому лицу доводить до сведения соответствующих поставщиков услуг информацию об осуществляемых видах деятельности, составляющих предусмотренные статьями 140, 175-1, 208-1, 279-2 и 346 Уголовного кодекса РМ [11] преступления, совершенные получателями услуг посредством этих услуг. Поставщики услуг после получения подобной информации обязаны незамедлительно информировать уполномоченные органы публичной власти о незаконной деятельности, осуществляемой получателями услуг посредством этих услуг.

Поставщики услуг обязаны оперативно сообщать уполномоченным органам публичной власти по их запросу информацию, позволяющую идентифицировать получателей услуг, с которыми поставщики услуг заключили договоры о постоянном хранении информации. Информация может запрашиваться уполномоченными органами публичной власти в соответствии с их компетенциями только в случае, если у них есть доказательства, позволяющие сделать вывод, что услуги, предоставленные поставщиком, используются получателем услуг для осуществления незаконной деятельности, включая передачу незаконной информации.

Уполномоченным органом публичной власти, которому поставщики услуг обязаны сообщать информацию, предусмотренную частью (1) ст. 25 За-

кона Республики Молдова, является Министерство внутренних дел Республики Молдова [12], а уполномоченными органами публичной власти, которым поставщики услуг обязаны сообщать информацию, предусмотренную частью (2) ст. 25 Закона РМ, являются Министерство внутренних дел Республики Молдова, Служба информации и безопасности [13] и Генеральная прокуратура [14].

В случае если получатель услуг отправляет с помощью электронных средств коммуникации оферту на заключение договора или информацию в отношении акцепта оферты поставщика услуг на заключение договора, поставщик услуг обязан подтвердить получение оферты или по обстоятельствам информации в отношении акцепта оферты одним из следующих способов: 1) незамедлительная отправка доказательства получения по электронной почте или с помощью другого эквивалентного индивидуального средства связи по адресу, указанному получателем; 2) подтверждение получения оферты или подтверждение акцепта оферты с помощью средства, эквивалентного использованному для отправки оферты или информации в отношении акцепта оферты, как только оферта или акцепт оферты были получены поставщиком услуг, при условии, что такое подтверждение получатель услуг сможет сохранить и воспроизвести.

Надзор и контроль за соблюдением положений о защите прав потребителей в процессе реализации товаров и услуг посредством электронных средств осуществляются органами, наделенными функциями контроля в области защиты прав потребителей, согласно областям компетенции, предусмотренным Законом о защите прав потребителей № 105/2003 [15].

Контроль законности обработки персональных данных в сфере услуг информационного общества осуществляется Национальным центром по защите персональных данных [16].

Контроль в сфере услуг информационного общества осуществляется и другими органами в пределах и в соответствии с полномочиями, установленными законом. Государственный контроль лиц, занимающихся предпринимательской деятельностью в сфере услуг информационного общества, планируется, осуществляется и регистрируется в соответствии с положениями Закона о государственном контроле предпринимательской деятельности № 131/2012 [17].

Государственная инспекция по надзору за непищевыми продуктами и защите прав потребителей и иные органы, наделенные функциями контроля в области защиты прав потребителей, сотрудничают с уполномоченными органами других стран в целях осуществления эффективного надзора и контроля над деятельностью поставщиков услуг.

Ассоциации патронатов или общественные объединения, осуществляющие деятельность в области защиты прав потребителей, несовершеннолетних или лиц с ограниченными возможностями, вправе разрабатывать в сотрудничестве с Министерством экономики и компетентными органами, перечисленными в ст. 26 Закона РМ, этические кодексы с целью соответствующего применения положений настоящего закона.

Поставщики услуг должны информировать получателей услуг в соответствии со статьей 21 о разработанных надлежащих этических кодексах, которы-

ми руководствуется поставщик услуг, а также о возможностях ознакомления с этими кодексами с помощью электронных средств.

Таким образом, органы внутренних дел РМ являются публичными органами, наделенными компетенцией в области услуг информационного общества. Прежде всего, органы внутренних дел реализуют информационные, административные и охранительные полномочия юрисдикционного характера. Сложность решаемых задач в области услуг информационного общества предполагает координацию деятельности и взаимодействие органов внутренних дел с иными уполномоченными органами, что также требует тщательного правового регулирования.

По мнению автора, необходимо расширять сравнительно-правовые исследования в рассматриваемой области с целью расширения перечня правовых средств, которые можно использовать для реализации органами внутренних дел своих полномочий в сфере услуг информационного общества [18, с. 107–116].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новеллы конституционного законодательства России: учебное пособие / В.А. Лысенко, А.А. Ерыгин, Д.В. Меняйло [и др.]. – Белгород: Белгородский юридический институт МВД Россий имени И.Д. Путилина, 2022. – 96 с.

2. Кирюхин В.В. Участие граждан в охране общественного порядка: в поисках разумного баланса / Закон и правопорядок в Третьем тысячелетии: IX Балтийский юридический форум: материалы международной научно-практической конференции, Калининград, 12 декабря 2020 года. – Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2021. – С. 93–94.

3. Виноградова Е.В., Кобзарь-Фролова М.Н. Международная научно-практическая конференция «Актуальные проблемы науки административного права и административного процесса («Лазаревские чтения – 2022») // Административное право и процесс. – 2022. – № 5. – С. 79–88.

4. Редкоус В.М. Законодательное регулирование общественного контроля в государствах-участниках СНГ // Право и государство: теория и практика. – 2024. – № 4 (232). – С. 147–149.

5. Трансформация информационного права / Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов [и др.]. – Москва: Институт государства и права РАН, 2023. – 256 с.

6. Кирюхин В.В. Цифровая полиция для цифрового общества / Цифровая трансформация системы МВД России: сборник научных статей по материалам Международного форума. В 2 частях, Москва, 20 октября 2022 г. / под ред. И.Г. Чистобородова. Т. 1. – Москва: Академия управления МВД России, 2022. – С. 357–363.

7. Дубень А.К. Информационная безопасность в Союзном государстве: универсальное правовое измерение // Международное право. – 2024. – № 1. – С. 1–11.

8. Конохов М.В., Дубень А.К. Актуальные проблемы действия норм международного гуманитарного права в информационном пространстве / Шестые Бачиловские чтения: сборник статей участников Международной научно-практической конференции, Москва, 2–3 февраля 2023 года. – Москва: Институт государства и права РАН, 2023. – С. 82–97.

9. Меняйло Д.В., Крупенникова К.К. О противодействии коррупции в условиях цифровой трансформации // Проблемы правоохранительной деятельности. – 2022. – № 3. – С. 28–32.

10. Закон РМ от 22 июля 2004 г. № 284-XV «Об услугах информационного общества» // Официальный монитор Республики Молдова. – 2004. № 138–146. Ст. 741; Официальный монитор Республики Молдова. – 2018. – № 40–47. – Ст. 104.

11. Уголовный кодекс Республики Молдова от 18 апреля 2002 г. № 985-XV // Официальный монитор Республики Молдова, 2009. – № 72–74. – Ст. 195.

12. Закон Республики Молдова от 27 декабря 2012 г. № 320 «О деятельности полиции и статусе полицейского» // Официальный монитор Республики Молдова. 2013. № 42–47. Ст. 145.

13. Закон Республики Молдова от 8 июня 2023 г. № 136 «О Службе информации и безопасности Республики Молдова» // Официальный монитор Республики Молдова. 2023. – № 204-207. – Ст. 358.

14. Закон Республики Молдова от 25 февраля 2016 г. № 3 «О Прокуратуре» // Официальный монитор Республики Молдова. 2016. № 69–77. – Ст. 113.

15. Закон Республики Молдова от 13 марта 2003 г. № 105-XV «О защите прав потребителей» // Официальный монитор Республики Молдова. 2003. – № 126–131. – Ст. 507; Официальный монитор Республики Молдова. 2011. – № 176–181. – Ст. 513; Официальный монитор Республики Молдова. 2024. – № 122–124. – Ст. 195.

16. Закон Республики Молдова от 10 июля 2008 г. № 182-XVI «Об утверждении Положения о Национальном центре по защите персональных данных, структуры, предельной штатной численности и порядка финансирования Национального центра по защите персональных данных» // Официальный монитор Республики Молдова. 2008. – № 140–142. – Ст. 578.

17. Закон Республики Молдова от 8 июня 2012 г. № 131 «О государственном контроле предпринимательской деятельности» // Официальный монитор Республики Молдова. 2012. – № 181–184. – Ст. 595.

18. Редкоус В.М. Использование зарубежного опыта в целях подготовки документов стратегического планирования в области общественной безопасности в государствах – участниках СНГ // Труды Академии управления МВД России. – 2024. – № 2 (70). – С. 107–116.

МОДЕЛИРОВАНИЕ КИБЕРАТАК С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ УПРАВЛЯЕМОГО ИМИТАТОРА В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ МОСКОВСКОГО УНИВЕРСИТЕТА МВД РОССИИ ИМЕНИ В.Я. КИКОТЯ

Ромашкин Т.Р.;
Бабина Л.В.,
кандидат технических наук, доцент
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в данной работе рассмотрены системы управляемого имитатора в образовательном процессе Московского университета МВД России имени В.Я. Кикотя.

Ключевые слова: информационная среда, информационная безопасность, уязвимости, компьютерные атаки.

SIMULATION OF CYBER ATTACKS USING A CONTROLLED SIMULATOR SYSTEM IN THE EDUCATIONAL PROCESS OF THE KIKOT MOSCOW UNIVERSITY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Romashkin T.R.;
Babina L.V.,
Candidate of Technical Sciences, Associate Professor
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: in the artide the systems of a controlled simulator in the educational process of the Kikot Moscow University of the Ministry of Internal Affairs of Russia are considered.

Keywords: information environment, information security, vulnerabilities, computer attacks.

Современная информационная среда требует от всех ее участников не только умения пользоваться компьютерами и сетями, но и знания основ информационной безопасности. К сожалению, далеко не все пользователи понимают важность защиты своих данных и часто не обладают достаточными знаниями, чтобы защитить свои устройства от различных угроз. Поэтому важно, чтобы специалисты в области информационной безопасности имели навыки работы с реальными уязвимостями и могли оперативно реагировать на возникающие угрозы.

Одним из инструментов, позволяющих получить практический опыт в работе с реальными уязвимостями, является управляемый имитатор компьютерных атак. Данный инструмент позволяет имитировать различные виды атак

на информационную систему и проводить тренировки для повышения навыков по ее защите.

Управляемые имитаторы – это системы моделирования кибератак, позволяющие произвести симуляцию реального взлома, атаки на инфраструктуру в автоматическом контролируемом режиме.

Моделирование или эмуляция злоумышленников – это процесс имитации поведения злоумышленника. Он предлагает возможность проверить устойчивость организации к продвинутым злоумышленникам в ситуации, известной как предполагаемое нарушение, т.е. все симуляции выполняются системой добровольно. Задача состоит в том, чтобы определить различные пути атаки, которые может предпринять противник, устранить наиболее серьезные угрозы и расставить приоритеты с помощью действенного плана исправления, чтобы максимально использовать ресурсы безопасности и снизить киберриски.

Применение управляемых имитаторов в образовательном процессе играет огромную роль в образовании, становлении и развитии сотрудников органов внутренних дел. Применение имитаторов может базироваться на готовых решениях и программах либо на создании собственных управляемых имитаторов.

К готовым решениям относятся такие программы, как:

1. MITRE CALDERA.
2. Atomic Red Team.
3. DumpsterFire.
4. Firedrill.
5. Infection Monkey.

Использование контролируемых имитаторов компьютерных атак имеет целью решение нескольких задач, связанных с обеспечением безопасности критически важной инфраструктуры:

- обнаружение уязвимостей в системе управления и оценка возможностей злоумышленников при реализации угроз компьютерных атак;
- агрегированная оценка динамики процессов использования средств защиты, включающая автоматизированные рабочие места, серверы сбора данных и электронную почту, средства предупреждения компьютерных атак и другие компоненты;
- комплексная оценка устойчивости функционирования системы в условиях компьютерных атак на основе разработанных методов и алгоритмов противодействия.

Использование управляемых имитаторов компьютерных атак и стендовых полигонов позволяет осуществить отработку методов и показателей оценки эффективности противодействия компьютерным атакам на критически важной инфраструктуре в практических условиях.

Управляемые имитаторы компьютерных атак используют компьютерные сети для проведения модели нападения на них. Это могут быть реальные компьютерные сети либо искусственно созданные сети, которые имитируют реальные.

Каждый персональный компьютер (далее – ПК), будь то ПК злоумышленника или ПК в сети, будет представлен окном на мониторе запущенной программы.

Необходимо предоставить в окнах программы возможность назначения адреса и шлюза, что позволит смоделировать как локальные, так и внешние сети, аналогично функционалу симулятора сети передачи данных Cisco Packet Tracer. Также важно добавить возможность отправки сетевого пакета данных из окна ПК злоумышленника. Для упрощения моделирования и повышения наглядности программой будет использоваться собственная структура сетевых пакетов. Используя язык программирования «C#», данный код создает новый TCP клиент, подключается к серверу по адресу «localhost» и указанному порту, передает сообщение в виде строки и закрывает соединение.

Конкретно в коде создается объект класса TcpClient, передавая ему строку «localhost» и конвертированное в целочисленное значение порта. Затем создается байтовый массив размером 256 байт для хранения сообщения. Строка сообщения кодируется в байтовый массив и при необходимости обрезается до 256 байт. После этого создается объект NetworkStream для передачи данных, и сообщение записывается в поток методом Write. Закрытие потока и удаление объекта TcpClient происходит в конце кода.

Наконец, в текстовом поле textBox3 выводится информация о том, что сообщение было отправлено на указанный порт и содержимое отправленного сообщения. Функция Environment.NewLine используется для добавления новой строки в конце выводимой информации.

```
using (TcpClient client = new TcpClient())
{
   try
   {
      client.Connect("localhost", Convert.ToInt32(port));
      using (NetworkStream stream = client.GetStream())
      {
         byte[] msg = Encoding.UTF8.GetBytes(str);
         stream.Write(msg, 0, msg.Length);
      }
      textBox3.AppendText("Отправлено " + oppPort + " »» " + str + Environment.NewLine);
   }
   catch (Exception ex)
   {
      // обработка ошибок при подключении или отправке данных
   }
}[1]
```

Получение данных должно реализовываться через потоки, а именно: на каждом порте, который прослушивается, генерируется персональный поток, что обеспечит одновременное обслуживания всех портов. При появлении в потоке массива байтов, который передается между окнами программы, этот массив будет переводиться в string-переменную (строковую).

Как было упомянуто ранее, для ПК злоумышленника и обычных ПК сети предусмотрена возможность отправки данных на определенные адреса. Логика маршрутизации построена таким образом, что при неизвестном порте адресата будет послан широковещательный запрос, так называемый ARP-Request. Необходимо добавить обработчик, который проверяет входящий пакет данных и на основе этого либо отклоняет, либо инициализирует последовательность определенных действий [6].

```
//Если ARP-Request
if (instr[13] == '1')
{
textBox.Text += "ARP REQUEST от " + instr.Substring(10, 3) + Environment.NewLine;
//Обычное + Mac-адрес назначения + наш Mac-адрес + адрес назначения + наш адрес + ARP-Reply
string macAdr = instr.Substring(4, 3);
string port = "0" + localPort;
string destAdr = instr.Substring(10, 3);
string srcAdr = adres;
string arpReply = "2";
string str = port + macAdr + srcAdr + destAdr + arpReply;
Thread.Sleep(1000);
//Отправка
Send(str);
return;
}
```

Также следует добавить окно сервера, которое будет принимать и записывать MAC-адреса, делать таблицу соответствий и записывать подключения.

Стендовый полигон является одним из важнейших элементов в образовательном процессе, когда речь заходит о наглядности, доступности и студентоориентированности. Стендовый полигон – это комплекс, объединяющий в себе различные программные, информационные и технические средства для оценки эффективности средств противодействия компьютерным атакам в закрытой локальной вычислительной сети.

Применение управляемых имитаторов компьютерных атак в образовательном процессе МВД России позволяет существенно повысить уровень подготовки сотрудников в борьбе с киберугрозами. Обучение на таких стендовых полигонах позволяет понять принципы работы злоумышленников, научиться выявлять и предотвращать атаки на инфраструктуру, а также разрабатывать и тестировать собственные средства противодействия компьютерным атакам.

Таким образом, использование управляемых имитаторов компьютерных атак в образовательном процессе в МВД России может существенно улучшить качество обучения и подготовку сотрудников в борьбе с киберугрозами, что является важным направлением развития систем безопасности в цифровую эпоху.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Безопасные информационные технологии: сборник трудов 8-й всероссийской научно-технической конференции / под ред. М.А. Басараба. – Москва: МГТУ им. Н.Э.Баумана, 2017. – 541 с.

2. Безопасные информационные технологии: сборник трудов 10-й международной научно-технической конференции. – Москва: МГТУ им. Н.Э. Баумана, 2019. – 409 с.

3. Климов С.М., Сычев М.П., Астрахов А.В. Противодействие компьютерным атакам. Методические основы. – Москва: МГТУ им. Н.Э. Бауна, 2013. – 70 с.

4. Степашкин М.В., Котенко И.В., Богданов В.С. Моделирование атак для активного анализа уязвимостей компьютерных сетей: материалы 2-й Всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» ИММОД–2020. – Санкт-Петербург, 2020. С. 269–273.

5. Внедрение облачных технологий в образовательный процесс образовательных организаций системы МВД России: учебно-методическое пособие / Прокопенко А.Н., Жукова П.Н., Савотченко С.Е., Насонова В.А., Акапьев В.Л., Ковалева Е.Г., Дрога А.А., Ковалева Л.А. – Белгород, 2017. – 88 с.

6. Шоров А.В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети. – Санкт-Петербург, 2012. – 21 с.

ТРАСОЛОГИЧЕСКАЯ ЭКСПЕРТИЗА ПРИ РАССЛЕДОВАНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ

Савотченко С.Е.,
доктор физико-математических наук, доцент
(Российский государственный геологоразведочный университет
имени Серго Орджоникидзе);
Акапьев В.Л.,
кандидат педагогических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной работе рассмотрена трасологическая экспертиза при расследовании дорожно-транспортных происшествий.

Ключевые слова: дорожно-транспортные происшествия, трасологическая экспертиза, трасология.

TRACOLOGICAL EXAMINATION IN THE INVESTIGATION OF ROAD ACCIDENTS

Savotchenko S.E.,
Doctor of Physical and Mathematical Sciences, Associate Professor
(Sergo Ordzhonikidze Russian State University for Geologicfl Prospecting named after);
Akapev V.L.,
Candidate of Pedagogical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in this artide the tracological examination in the investigation of road accidents is considered.

Keywords: traffic accidents, tracological examination, tracology.

С течением времени транспортные средства становятся все мощнее, удобнее, безопаснее, однако их количество на дорогах России растет. Наличие почти у каждого человека автомобиля приводит к напряженной ситуации на дорогах, что объясняется рядом причин: во-первых, большое количество автомобилей на дорогах требует надежной и эффективной системы регулирования дорожного движения; во-вторых, подрывается экологическая ситуация из-за большого выброса в атмосферу вредных веществ, получившихся в результате сгорания топлива; в-третьих, интенсивное движение, большие скорости и другие опасные факторы приводят к немалому количеству аварий на дорогах, некоторая часть которых сопряжена с человеческими жертвами.

Ежегодно в России происходят десятки тысяч дорожно-транспортных происшествий (далее – ДТП), в результате которых причиняется значительный вред здоровью, а порой и жизни человека. Об этом говорит официально опубликованная статистика дорожно-транспортных происшествий с теми или иными последствиями. Так, по статистическим данным сайта Государственной инспекции безопасности дорожного движения (далее – ГИБДД) за октябрь 2023 года на автомобильных дорогах общего пользования России произошло 12 529 случаев ДТП, в которых погибло 1 468 человек, пострадало 15 349 [1].

Таким образом, можно наблюдать сложную ситуацию – в России происходит большое количество ДТП, в которых погибают и страдают тысячи людей. Нельзя не отметить важность и остроту данной проблемы на сегодняшний день, которые вызывают необходимость осуществления разного рода мероприятий, направленных на улучшение сложившейся ситуации.

Исследование обусловлено необходимостью совершенствования процесса установления тех или иных фактов по поводу произошедшего ДТП сотрудниками правоохранительных органов [2]. В данном контексте предпочтительно обратиться к теоретическим основам предупреждения аварийных ситуаций на дорогах общего пользования и выявления причин происшествий и факторов, им сопутствующих, исследованием которых занимается наука трасология, представляющая собой составную часть криминалистической техники, разрабаты-

вающая средства и приемы собирания и исследования следов. Одной из отраслей трасологии является транспортная трасология, которая непосредственно занимается исследованием мест ДТП и всех тех явлений, которые этому способствовали. В рамках транспортной трасологии существует трасологическая экспертиза при ДТП [4], которая позволяет изучать происшествия на дороге, а также устанавливать причины и другие факторы, влияющие на динамику дорожно-транспортных происшествий [5].

Как было сказано ранее, в рамках транспортной трасологии проводится трасологическая экспертиза ДТП. Для воссоздания полной картины аварии рассматриваются причины образования тех или иных следов, например, оставленных автомобилем на поверхности асфальта. Это могут быть следы от торможения, заноса, аварийной блокировки колес, буксирования и скольжения транспортного средства. В рамках трасологической экспертизы при ДТП объектами изучения являются, как правило, участники ДТП – водители автотранспортных средств, пешеходы, водители иных транспортных средств [6].

Иногда к объектам также относят и косвенные факторы:

– причины тех или иных нарушений Правил дорожного движения, которые были допущены водителями;

– климатические или погодные условия;

– техническое состояние транспортных средств;

– нарушения правил эксплуатации транспортных средств и т.д.

Специфика следственных мероприятий при исследовании ДТП заключается еще и в том, что при проведении экспертизы учитываются не только крупные повреждения транспортных средств, но и мелкие детали, которые зачастую трудно разглядеть невооруженным глазом. Это могут быть небольшие слепки или оттиски следов протекторов, осколки от стекол внешних световых приборов, поврежденная одежда, ссадины и кровоподтеки пострадавших.

Трасологическая экспертиза при ДТП направлена на создание схемы движения автомобилей, а точнее сказать – механизма ДТП, то есть совокупность действий участников дорожного движения, приведших к дорожно-транспортному происшествию [7]. Это необходимо для получения более полного объема информации о случившемся, исследования самих автомобилей и оставленных ими следов, что в общем итоге способствует восстановлению более объективной картины произошедшего ДТП.

В рамках данной работы стоит выделить цели проведения трасологической экспертизы:

1. Идентификация автотранспортного средства по оставленным им следам на месте случившегося.

2. Определение принадлежности тех или иных частей автомобиля к конкретному автотранспортному средству.

3. Установление соответствия между повреждениями автомобиля и реально произошедшим столкновением.

4. Установление факта, определяющего, действительно ли повреждения произошли во время ДТП или были нанесены ранее.

Независимо от тяжести последствий необходимо воссоздать объективную картину дорожного происшествия. Современная трасология ДТП по-прежнему использует такие виды доказательств, как, например, видеозаписи с портативных записывающих автомобильных устройств или видеорегистраторов, материалы с камер наружного наблюдения, установленных на месте происшествия или в непосредственной близости, показания очевидцев и участников ДТП с последующим документированием этих показаний.

Основная задача, решаемая трасологической экспертизой, заключается в определении механизма автодорожного происшествия, о котором уже говорилось ранее и который призван отражать последовательность всех его стадий. Стоит рассмотреть случай, демонстрирующий практическую пользу транспортной трасологии.

Например, разобраться без вышеуказанных мероприятий затруднительно при авариях, связанных с перестроением транспортных средств, движущихся в одном направлении. Специфика такого рода ДТП обусловлена тем, что каждый из участников ДТП утверждает, что двигался без изменения направления движения и, что именно другой водитель совершил противоправный маневр, который и повлек за собой дорожно-транспортное происшествие. С помощью специальных трасологических средств можно установить настоящего виновника.

Ко всему прочему, к транспортной трасологии обращаются в тех случаях, когда требуется провести идентификационное сравнение следов происшествия с представленными образцами. Например, при осмотре поврежденного автомобиля с места происшествия были изъяты образцы следов наслоения автоэмали, оставленные скрывшимся с места аварии транспортным средством. В ходе расследования дела по подозрению в совершении происшествия задержан автомобиль, имеющий следы отслоения автоэмали на переднем бампере. Обнаруженные на задержанном автомобиле следы по цвету, форме и характеру образования соответствуют следам, изъятым при осмотре поврежденного автомобиля. Для ответа на вопрос о причастности задержанного автомобиля к дорожной аварии назначается трасологическое экспертное исследование.

Назначение дорожной экспертизы целесообразно во всех случаях, когда причинами ДТП является загрязнение дорожного покрытия, несоответствие сцепных качеств дороги требованиям безопасности, при авариях в местах проведения ремонтных, строительных и иных дорожных работ, открытых (неисправных) крышек технологических колодцев, при наличии дефектов дорожного покрытия.

Также одной из задач транспортно-трасологической экспертизы является исследование отрицательно влияющих на дорожное движение факторов дорожного покрытия в отдельно взятых местностях. Дефекты дороги включают в себя следующие элементы:

– колейность дорожного покрытия, то есть деформация поперечного профиля относительно полос наката;

– выбоины в виде глубинных разрушений с выраженными краями общей площадью от 200 квадратных сантиметров и глубиной более 3 сантиметров;

– выкрашивание дорожного покрытия общей площадью от 200 квадратных сантиметров и глубиной более 3 сантиметров;

– сдвиги на покрытии, образованные перемещением содержащего битум слоя;

– проломы дороги – прорези покрытия по полосам наката;

– гребенка в виде чередующихся поверхностных углублений и выступов дорожного покрытия;

– просадки в виде впадин с пологими склонами, искажающими профиль дороги.

Таким образом, транспортная трасология – отрасль трасологии, в рамках которой проводятся трасологические экспертизы при ДТП, практическая и теоретическая значимость которых заключается в выявлении причин и механизма дорожно-транспортных происшествий, более точного установления виновных, а также установления тех факторов, устранение которых поможет стабилизировать ситуацию на дорогах и улучшить процесс дорожного движения.

Учитывая актуальность рассматриваемой проблемы, представляется целесообразным акцентировать внимание практических сотрудников на одном из наиболее эффективных способов совершенствования технологии расследования произошедшего дорожно-транспортного происшествия путем восстановления картины ДТП с помощью компьютерных программ для создания графических анимаций.

В заключение следует отметить, что деятельность в рамках транспортной трасологии должна привести к улучшению ситуации по ДТП в России и уменьшить количество человеческих жертв и материальных потерь. Результаты и эффективность трасологической экспертизы, хоть и опосредованно, влияют на количество происходящих дорожно-транспортных происшествий. Нельзя рассчитывать на то, что повышение результативности работы трасологических экспертиз приведет к полному устранению причин происходящих ДТП в силу различных обстоятельств как объективных, так и субъективных, но это повлияет на сложившуюся на данный момент ситуацию и с большой вероятностью приведет к существенному снижению количества ДТП.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сайт статистической информации ГИБДД [Электронный ресурс]. – URL: http://stat.gibdd.ru/ (дата обращения: 11.12.2023).

2. Скирковский С.В. Экспертиза ДТП. – Гомель: БелГУТ, 2018. – 80 с.

3. Короткий А.А. Дорожно-транспортные происшествия: основные причины, анализ аварийности, методы снижения // Научный вестник. – 2019. – № 1. – С. 5–10.

4. Аминев Ф.Г. О современных возможностях криминалистического исследования трасологических объектов // Эксперт-криминалист. – 2016. – № 3. – С. 162.

5. Поляков Д.Н. Понятие и причины дорожно-транспортных происшествий // Вестник Омского ЮИ МВД России. – 2011. – № 6. – С. 6–12.

6. Стрюкова Е.М. Трасологическая экспертиза: современные возможности и перспективы // Форум молодых ученых. – 2019. – № 1–3 (29). – С. 470–474.

7. Хижняк Д.С., Тугушева Н.Р. Трасологическая экспертиза: современные возможности и перспективы // Аллея Науки. 2020. № 10 (49). [Электронный ресурс]. – URL: https://alley-science.ru/ (дата обращения: 11.12.2023).

СИСТЕМА ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА В СФЕРЕ ПРОВЕДЕНИЯ БЕЗНАЛИЧНЫХ РАСЧЕТОВ И ПЛАТЕЖЕЙ

Самойлова Ю.М.,
кандидат технических наук;
Пашкова М.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: современная преступность использует широкий спектр технических средств и оборудования с выходом в информационно-телекоммуникационные сети. Особенно подвержены переходу в интернет-пространство экономические преступления, связанные с безналичными расчетами и платежами. Данные преступления осуществляются путем взаимодействия преступника с жертвой в сети Интернет с целью получения доступа к ее счетам или присвоения от нее денежных безналичных переводов путем обмана или злоупотребления доверием. Жертвами данных преступлений в основном являются слабозащищенные слои населения, что подчеркивает необходимость слаженной и четкой работы правоохранительных органов по противодействию данным преступлениям.

Ключевые слова: безналичный расчет, электронное средство платежа, платежная карта, хищение денежных средств, злоупотребление доверием, персональные данные, киберпреступления.

FRAUD PREVENTION SYSTEM IN THE FIELD OF NON-CASH PAYMENTS AND PAYMENTS

Samoilova J.M.,
Candidate of Technical Sciences;
Pashkova M.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: modern crime uses a wide range of technical means and equipment with access to information and telecommunication networks. Economic crimes relat-

ed to non-cash payments and payments are particularly susceptible to the transition to the Internet space. These crimes are carried out through the interaction of the perpetrator with the victim on the Internet in order to gain access to her accounts or to appropriate money transfers from her by deception or abuse of trust. The victims of these crimes are mainly vulnerable segments of the population, which underlines the need for coordinated and precise work of law enforcement agencies to counter these crimes.

Keywords: cashless payment, electronic means of payment, payment card, theft of funds, abuse of trust, personal data, cybercrimes.

Современная преступность в Российской Федерации активно выходит в интернет-пространство и использует различные технические устройства для дистанционного контактирования с предполагаемыми жертвами, что обуславливает сложность ее выявления и распознавания как самими жертвами, так и сотрудниками правоохранительных органов. Одними из наиболее опасных с точки зрения индивидуальной экономической безопасности населения, особенно его слабозащищенных слоев, являются экономические преступления, в частности, преступления в сфере безналичных расчетов, платежей и электронных средств платежа.

В основной массе потерпевшими преступного и корыстного умысла являются пенсионеры, которые слабо понимают алгоритмы работы мобильных банковских приложений.

Хищение денежных средств с банковского счета граждан осуществляется путем злоупотребления их доверием или обмана. Преступник в ходе взаимодействия с жертвой представляется сотрудником банка или служащим государственной структуры. Благодаря данному вымышленному статусу, злоумышленник получает доступ к платежным картам и банковским счетам граждан [1].

Особенностью преступлений, связанных с безналичными денежными переводами, является их частое совершение организованной преступной группой, в которую входят как настоящие сотрудники банков и государственных структур, предоставляющие за вознаграждение конфиденциальную личную информацию о гражданах, так и непосредственные мошенники. Злоумышленник взаимодействует с предполагаемой жертвой с апеллированием ставшей ему известной их личной информацией и, таким образом, реализует обман или злоупотребляет доверием.

Правоохранительные органы при противодействии преступлений с сфере безналичных расчетов и платежей сталкиваются с целым рядом проблем, к которым относятся:

– существенное удаление преступников как друг от друга, так и от самих жертв их преступных посягательств;

– зачастую нахождение преступников за пределами территории Российской Федерации;

– использование преступниками в ходе реализации своего преступного умысла многочисленных социальных сетей, предоставляющих своим пользова-

телям для повышения конфиденциальности шифрование их данных (система мгновенного обмена сообщениями Telegram);

– высокий уровень латентности незаконной продажи сотрудниками государственных или коммерческих учреждений персональных данных граждан;

– направленность данных преступлений против слабозащищенных слоев населения, к которым относятся пенсионеры и несовершеннолетние лица, плохо разбирающиеся в технических устройствах.

Для более эффективного выявления преступлений в сфере безналичных переводов и расчетов правоохранительные органы налаживают тесное сотрудничество со службами безопасности коммерческих организаций, в частности банковского сектора, которые мониторят активность сотрудников данных учреждений, анализируют подозрительные действия, запросы и копирования персональных данных клиентов и незамедлительно сообщают об этом правоохранительным органам. Это позволяет пресечь утечку личной информации в ее начале и предотвратить попадание конфиденциальных данных в руки мошенников.

В случае выявления махинаций, направленных на хищение денежных средств граждан путем обмана или введения в заблуждение, сотрудники оперативно-разыскных подразделений проводят мероприятия, направленные на поиск счетов, являющихся конечными в цепочке перемещения денежных средств безналичным путем, и их владельцев, которые незамедлительно задерживаются и допрашиваются. Зачастую правоохранители сами вступают в контакт с мошенниками и, действуя по намеченному плану и выставляя себя в качестве возможной жертвы, выясняют их личные данные, необходимые для пресечения их преступной деятельности.

Значительную сложность представляет установление личности преступника, совершившего преступление на территории иностранного государства, либо зарегистрировавшего противоправный интернет-домен в компании, представительство которой находится за рубежом [2]. В данном случае правоохранительные органы Российской Федерации направляют официальный запрос правоохранительным органам иного государства и совместно с ними применяют комплексные меры по установлению личности преступника и его задержанию.

В случае использования злоумышленником для совершения противоправных действий мессенджеров, которые предполагают высокий уровень конфиденциальности своих пользователей, таких как Telegram, Instagram, Viber, WhatsApp, Skype, Jabber, Black-Jack [2], правоохранительные органы требуют у владельцев данных мессенджеров ключей доступа к данным о пользователях, которые существенно облегчают поиск виновного лица и привлечение его к уголовной ответственности.

Предупреждение совершения подобных преступлений, являющееся частью противодействия им, заключается в проведении сотрудниками полиции масштабной профилактической работы. Проводится массовое информирование среди населения о способах и методах преступников, направленных на получение корыстной выгоды путем обмана или злоупотребления доверием. В первую очередь разъяснительная кампания проводится с людьми пожилого возраста, наиболее подверженными данным преступным посягательствам.

Таким образом, преступления в сфере безналичных платежей и расчетов представляют собой сложные преступные деяния. Преступления с электронными платежными средствами отличаются своим многообразием и множественностью возможных субъектов преступления. Учитывая данные обстоятельства, а также постоянное техническое перевооружение средств и оснащения злоумышленников в сфере киберпреступлений, развитие онлайн–приложений мобильного банкинга и социальных онлайн платформ, правоохранительным органам необходимо непрерывно модернизировать уже разработанные методики по противодействию подобным преступлениям, что должно обеспечивать предупреждение, пресечение, выявление, раскрытие и расследование преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Клещенко Ю.Г. Классификация способов совершения хищений денежных средств с использованием электронных средств платежа / Проблемы противодействия киберпреступности: сборник материалов Международной научно-практической конференции. – Москва, 2023. С. 73–77.

2. Галкин Р.С. Содержание криминальной реальности, связанной с подготовкой и совершением преступлений экономической направленности с использованием информационно–телекоммуникационных технологий // Время развития [Электронный ресурс]. – URL: https://vremyarazvitiya.ru/soderzhanie-kriminalnoj-realnosti-svyazannoj-s-podgotovkoj-i-soversheniem-prestuplenij-ekonomicheskoj-napravlennosti-s-ispolzovaniem-informaczionno (дата обращения: 30.04.2024).

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПСИХИКУ ЧЕЛОВЕКА

Смирнов В.М.,
кандидат технических наук;
Миренков В.О.
(Московский университет МВД России имения В.Я. Кикотя)

Аннотация: данная статья исследует влияние развития информационных технологий на психику и ценности нового поколения. Современное общество стремительно развивается в направлении информационных технологий, что непосредственно отражается на мировоззрении и ценностях молодого поколения.

Ключевые слова: информационные технологии, современное поколение, психика, ценности, социальная адаптация, мировоззрение, социализация, влияние, нейросети, искусственный интеллект, цифровая эра.

THE INFLUENCE OF INFORMATION TECHNOLOGY ON THE HUMAN PSYCHE

Smirnov V.M.,
Candidate of Technical Sciences;
Mirenkov V.O.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: this article explores the impact of information technology development on the psyche and values of the new generation. Modern society is rapidly developing in the direction of information technology, which directly affects the worldview and values of the younger generation.

Keywords: information technology, modern generation, psyche, values, social adaptation, worldview, socialization, influence, neural networks, artificial intelligence, digital era.

Развитие общества сегодня направляется к выстраиванию и использованию новейших информационных технологий, таких как нейросети и искусственный интеллект. Это оказывает определенное влияние на психику человека. На современное поколение с первых лет текущего столетия широко распространилось влияние информационных технологий. В это время во многих семьях появились первые вычислительные машины с процессором Pentium 4, где основным браузером был Internet Explorer от Microsoft, а также была выпущена операционная система Windows XP. Ценности нового поколения начинают формироваться под влиянием развития онлайн-социализации и информационных технологий, в большей части и в основном через Интернет.

Одна из самых важных отличительных особенностей нового поколения это «клиповое» мышление. Это способ демонстрации множества различных черт объектов, не принимая связей между ними, характеризующийся резкостью информационного потока, нелогичностью, разнородностью поступающей информации, отсутствием целостности картины восприятия окружающего мира. По этой причине личности неспособны полностью передавать и воспринимать информацию, последовательно выражать свои мнения. Появляется привыкание к постоянной смене образов и представлений, вследствие чего человек уже не может воспринимать все то, что требует концентрации внемания и умения формулировать выводы.

«Клиповому» мышлению свойственны не только негативные стороны – это становление одних когнитивных способностей за счет других. Благодаря данному мышлению у нового поколения значительно повысилась многозадачность. Личности Интернета с легкостью могут одновременно слушать музыку, беседовать в мессенджерах, редактировать фотографии, делая при этом домашнее задание. Однако, к большому сожалению, платой за многозадачность становится рассредоточенность, гиперактивность, у них обнаруживается дефицит внимания и предпочтение визуальных образов логике и глубокому размышлению.

Согласно научным исследованиям, можно с уверенностью заявить, что внимание подрастающего поколения ниже приблизительно в десять раз, чем у прошлом поколения, но переключение и распределение внимания очень развито. У представителей цифрового поколения более развита кратковременная память, нежели долговременная. Современный пользователь Интернета имеет возможность «погуглить», то есть отыскать что-то в поисковике. Найти необходимую информацию можно в любое время, нет надобности хранить всю информацию в своей памяти.

Восприятие людей тоже в значительной степени подверглось преобразованиям. Индивиды, которые проводят большую часть своего времени перед компьютером, планшетом, смартфоном или просто в Интернете, получают определенную недостачу, то есть они лишены некоторых сенсорных сигналов, связанных с внешним миром, таких как обоняние, осязание и т.д.

Интеллектуальные особенности нового поколения становятся наиболее выразительными в экстремальных проявлениях, включая некоторые психологические синдромы, которые выступают в качестве защиты от проблем современного образа жизни, как метод закрыться. На самом деле, это манера отсутствия взаимодействия с обществом. Именно из-за чрезмерной увлеченности Интернетом возрастает риск психологического синдрома. Вероятно, пользователи Интернета, испытывающие трудности в общении с реальными людьми, осознанно и целенаправленно концентрируются на виртуальных коммуникациях, поскольку это в разы легче. Сеть в силу своей определенной анонимности позволяет упражняться в самовыражении, развивать собственную индивидуальность и заводить новых друзей.

Гиперреактивность – это психологический синдром, который можно обнаружить у нового поколения. Он характеризуется чрезмерной активностью и возбудимостью, которые могут негативно влиять на других людей, а также не-

достатком способности сконцентрироваться. Формирование этих явлений обусловлено избыточным информационным насыщением.

Основной психосоциальной тенденцией нового поколения является инфантильность. Инфантилизация – это изменение моделей поведения, структур социального взаимодействия и индивидуальных жизненных циклов, при котором поощряется и становится нормальным такое поведение взрослых которое прежде было свойственно детят. Подростки безответственны, бездеятельны и не готовы признать вину за свои поступки и действия. В то же время они практически всегда ожидают, что общество положительно оценит их деятельность. По сравнению с прошлыми поколениями, противоречия с новым поколением идеологические коллизии стоят более остро.

Стремительное развитие современного общества привнесло своеобразные приоритеты и ценности к новому поколению. Люди все больше осознают, что необходимость поддержания здоровья в условиях современного образа жизни может привести к изменению привычных установок. Граждане все больше осознают, что поддержание и улучшение здоровья требует больших усилий, времени и денег, вследствие чего, спрос на здоровый образ жизни возрастает.

В то же время семейные ценности теряют актуальность и могут отойти на второй план. Интерес смещается с семьи на сообщество, то есть на род занятий и финансовый статус. Однако, если мы оглянемся назад на трудности конфликтов, эмоций и чрезмерной реакции, с которыми сталкивается современное общество, мы можем подумать, что сообщество будет стремиться к достижению большей согласованности между людьми. Новое поколение будет пытаться достичь своих личных целей любыми методами.

Духовные ценности постепенно утратят свою значимость и станут менее важными для большинства молодых людей. Высокообразованное население, придающее большое значение образованию, духовному росту и саморазвитию, будет постепенно сокращаться.

Существует большое количество разных взглядов касательно использования молодым обществом информационных технологий. На данный момент сложно определить, насколько критичными окажутся воздействия информационных сетей, искусственного интеллекта на становление нового поколения. Наблюдаются изменения в механизмах мышления, внимания, памяти, сосредоточенности, восприятия речи, что позволяет пользователям адаптироваться к большим объемам информации. Вместе с тем происходит снижение создания и формирования нужных нейронных связей при сохранении повышенной скорости психических процессов организма. Отсутствие общения с реальными людьми способствует становлению эгоизма и инфантилизма, так как большое увлечение информационной сетью становится современным укладом жизни в цифровой эре, а без технологий жизнь современного сообщества не представляется возможной. Следует признать как преимущества, так и недостатки Интернета и современных технологий, а также осознать ценности цифровой эпохи, чтобы адаптироваться к постоянно меняющемуся миру. Это предполагает необходимость разработки нового подхода к существующим нормам и ценностям, а также поиск устойчивых ориентиров.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гордеева А.В. Увлеченность компьютерными играми: психологический аспект: монография. – Киев: КНУ, 2004. – 210 с.

2. Немов Р.С. Психология. – Москва: Владос, 1999. – 688 с.

3. Практикум по общей психологии: учебное пособие / под ред. А.И. Щербакова. – Москва: Просвещение, 1990. – 288 с.

4. Краснова С.В. Как справиться с компьютерной зависимостью / С.В. Краснова, Н.Р. Казарян, В.С. Тундалева, Е.В. Быковская, О.Е. Чапова, М.О. Носатова [Электронный ресурс]. – URL: http://www.fictionbook.ru (дата обращения: 15.04.2024).

5. Харламова И.Ю. Роль веб-сайта вуза в патриотическом воспитании обучающихся (из опыта работы Московского университета МВД России имени В.Я. Кикотя) // Информационные технологии в образовании. – 2022. – № 5. – С. 263–264.

6. Меняйло Д.В., Хайминова К.Е. Правовое воспитание сотрудников органов внутренних дел в условиях цифровизации общества / Правовая культура в современном обществе: сборник научных статей VI Международной научно-практической конференции, Могилев, 19 мая 2023 года. – Могилев: Могилевский институт МВД Республики Беларусь, 2023. – С. 428–432.

АНАЛИЗ ПРАКТИКИ РАСКРЫТИЯ КИБЕПРЕСТУПЛЕНИЙ: НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ОСОБЕННОСТИ ВЕДЕНИЯ РАССЛЕДОВАНИЯ

Соломина А.А.,
Захаров Д.С.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: данная статья посвящена изучению проблем, которые возникают в процессе расследования киберпреступлений, совершаемых в современном киберпространстве. При рассмотрении данного вопроса мы проводим анализ тенденций усложнения мошеннических схем и методов совершения преступных деяний. В выводе детальное изучение обозначенных выше вопросов позволит не только решить комплекс проблем, связанных с профилактикой киберпреступлений, но и определить перспективы усовершенствования систем и методов кибербезопасности.

Ключевые слова: кибербезопасность, кибератака, мошенничество, уголовное законодательство, информация, взлом, расследование, полиция, федеральный закон.

ANALYSIS OF CYBERCRIME DISCLOSURE PRACTICES: REGULATORY AND LEGAL REGULATION AND THE SPECIFICS OF CONDUCTING AN INVESTIGATION

Solomina A.A.,
Zakharov D.S.
(Kikot Moscow University of the Ministry of Internal Affairs of Russia)

Abstract: this article is devoted to the study of problems that arise in the process of investigating cybercrimes committed in modern cyberspace. When considering this issue, we analyze trends in the complication of fraudulent schemes and methods of committing criminal acts. In conclusion, a detailed study of the issues outlined above will not only solve a set of problems related to the prevention of cybercrime, but also determine the prospects for improving cybersecurity systems and methods.

Keywords: cybersecurity, cyberattack, fraud, criminal law, information, hacking, investigation, police, federal law, investigation, police, federal law.

В условиях современного постиндустриального развития характерной чертой развития общества и социальных отношений, происходящих в нем, стал факт компьютеризации, информатизации и автоматизации процессов взаимодействия отдельных лиц, организаций, должностных лиц и иных субъектов правоотношений.

Ежедневно в сеть Интернет выкладываются терабайты информации, содержащей в себе персональные данные, данные банковских и страховых счетов и другую информацию, которой могут воспользоваться мошенники для достижения какой-либо материальной выгоды. Характерной тенденцией киберпреступников стало усовершенствование, усложнение мошеннических схем, позволяющих незаконно получать доступ к аккаунтам, личным данным жертв.

Стоит отметить, что расследование данных видов преступлений остается достаточно сложным: порой практически невозможно выявить личность киберпреступника. Данным расследованием занимаются многие службы российской Федерации, которые, взаимодействуя, обмениваются важными данными. Среди служб, выполняющих большой комплекс задач по расследованию преступлений в киберпространстве, выделяют МВД России, ФСБ России, ГосСОПКА, ФСТЭК России. Данные службы регламентируют свою служебную деятельность следующими нормативными актами Российской Федерации:

- Конституция Российской Федерации;
- Уголовный кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных»;

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

Для ведения расследования преступлений, совершенных в киберпространстве, важно знать терминологию, которая употребляется в данной сфере деятельности. Уголовный кодекс Российской Федерации определяет, что под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи [8]. К числу же компьютерных устройств можно отнести те электронные устройства, которые обладают способностью принимать, обрабатывать, хранить, передавать информацию, которая поступает на другие устройства в виде электромагнитных сигналов.

В свою очередь киберпреступление как процесс осуществления противоправной деятельности неразрывно связан с нанесением материального, духовного, экономического, культурного и иного ущерба. Данный вред наносится физическим лицам – гражданам Российской Федерации, иностранным гражданам, лицам без гражданства, юридическим лицам (организациям) и государству посредствам любого технического средства с доступом в Интернет [2]. Другими словами, киберпреступность – это совокупность преступлений, которые совершаются в кибернетическом пространстве. Стоит отметить, что ежедневно человечество сталкивается с преступлениями, происходящими в киберпространстве. Данная категория противоправных деяний посягает на безопасность личности, общества и государства в целом и в большей мере затрагивает информационную безопасность. Отметим, что совокупность данных преступлений с каждым годом кратно увеличивается, однако условно, в зависимости от направленности противоправных действий, их можно разделить на 2 группы. Первая группа – внутренние, то есть такие преступления, которые реализуют утечку государственной или иной информации, охраняемой законом; аномальная сетевая активность и т.д. Вторая группа – внешние, то есть преступления, выражающиеся в постороннем вмешательстве киберпреступников в работу чужого компьютера (фишинг, DDoS-атаки). Иначе эти две группы можно назвать компьютерными преступлениями и преступлениями, совершаемыми в киберпространстве [1].

В процессе расследования сотрудники правоохранительных органов используют комплекс методов и мер, позволяющих эффективно производить следственные и оперативные действия. Среди данных методов и средств выделяют.

1. Технические средства, а также системы, программное обеспечение;
2. Криминалистические средства и методы. К данной группе методов и средств относят компьютерное моделирование, а также разносторонний анализ материалов уголовных дел.

Анализируя практику расследования киберпреступлений (как вид противоправных действий), можно сказать, что каждое преступление по своему составу индивидуально. Однако каждое киберпреступление может быть типичным ранее совершенным сходным по отдельным элементам. Следует отметить,

что преступные деяния данной категории могут нести не только имущественный вред как физическим, так и юридическим лицам, но также может быть нанесен вред моральный, физический и наносящий ущерб деловой репутации лица.

Особую роль в рамках расследования киберпреступлений играют оперативно-разыскные мероприятия, которые в процессе усложнения киберпреступлений стали претерпевать качественные и количественные изменения. Однако стоит отметить, что многообразие оперативно-разыскных мероприятий в совокупности не дают гарантий успешного расследования уголовного дела. Завершение расследования зависит от компетентности лиц, непосредственно ведущих данное расследование. Специалисты в области криминологии, криминалистики, информационной безопасности и иных сфер функционируют в рамках поиска преступника и доказательств совершения преступления именно этим лицом (или группой лиц).

На основе результатов многоаспектного анализа практики современного расследования киберпреступлений можно условно выделить этапы данной деятельности. Первое: обеспечение поступления информации о готовящемся или уже совершенном киберпреступлении. Второе: анализ поступившей сотруднику правоохранительного органа информации о киберпреступлении с последующим формированием уголовного дела и определение целей и задач, которые будут достигнуты в процессе ведения расследования по данного уголовному делу. Третье: определение сил (в том числе и взаимодействие с другими службами и организациями), средств и методов, которые будут необходимы для проведения успешных следственных действий, оперативно-разыскных мероприятий и т.д. Четвертое: непосредственно само ведение расследования и осуществление мероприятий по выявлению личности преступника, событиях и подробностях киберпреступления. Пятое: вынесение обвинительного заключения и последующая передача дела в суд.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // ЮП. – 2019. – № 4 (91). – С. 78– 82

2. Кочкина Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3 (17). – С. 162–169.

3. Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» [Электронный ресурс] // СПС «КонсультантПлюс».

4. Пинкевич Т.В. Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалют // ЮП. – 2020. – № 4 (95). – С. 45–48.

5. Пономарев В.Г. Анализ практики применения уголовного законодательства в борьбе с киберпреступлениями // Юридическая наука. – 2021. – № 10. – С. 61–66.

6. Марочкин Н.А., Асташкина Е.Н. Алгоритмизация – эффективный метод оптимизации расследования преступлений // Известия Алтайского государственного университета – 2001. – № 2. – С. 45–49.

7. Федосеев А.Э., Федосеев А.Э., Архипцев И.Н. Конкурентная разведка в деятельности правоохранительных органов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2021. – № 7. – С. 91–96.

8. Уголовный кодекс Российской Федерации от 18 июня 1996 г. № 63-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс».

9. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 177-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс».

СОВРЕМЕННЫЕ МЕТОДИКИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ И ПЛАТЕЖЕЙ

Солощенко А.А.;
Акапьев В.Л.,
кандидат педагогических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной работе рассмотрены современные методики противодействия преступлениям в сфере безналичных расчетов и платежей, а также выделены их особенности.

Ключевые слова: безналичный расчет, мошенничество, дистанционное мошенничество, транзакция, кибербезопасность.

MODERN METHODS OF COUNTERING CRIMES IN THE FIELD OF NON-CASH SETTLEMENTS AND PAYMENTS

Soloshchenko A.A.;
Akapyev V.L.,
Candidate of Pedagogical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in this article, modern methods of countering crimes in the field of non-cash payments and payments are considered, and the features of their counteraction are highlighted.

Keywords: cashless payment, fraud, remote fraud, transaction, cybersecurity.

В настоящее время мошенничество в информационном поле не уменьшилось, а только увеличилось. Одной из причин является появление дистанционного мошенничества. Оно подразумевает совершение такого вида мошенничества, при котором злоумышленник, чаще всего используя компьютерные и телефонные сети, воздействует на сознание потерпевшего путем обмана, склоняет к передаче имущества удаленным образом. С усовершенствованием информационных технологий преступникам становится проще добраться до денежных средств других людей. Росту преступлений, связанных с хищением денежных средств, способствует недостаточная осведомленность граждан в области информационно-телекоммуникационных технологий.

Зачастую мошенники имитируют номера банков с помощью специальных программ, крадут конфиденциальную информацию человека, взламывают личные аккаунты в социальных сетях и других информационных площадках. Но на этом мошенники не останавливаются, у них появился новый способ. Во время звонка они представляются сотрудниками банка, когда собеседник отвечает, они записывают голос и дальше редактируют как им нужно. Таким образом, злоумышленники могут взять кредит или же позвонить вашим родственникам и попросить денег в долг.

Для того чтобы избежать обмана, был разработан ряд методик по противодействию преступлений в сфере безналичных расчетов и платежей. Рассмотрем некоторые из них.

1. Мониторинг транзакций.

Один из самых простых методов. С его помощью него сотрудники банков могут отслеживать подозрительную активность на счетах их клиентов. При обнаружение такой активности сотрудник сообщает клиенту или автоматически блокирует счет во избежание повторных попыток списать денежные средства мошенниками. Для предотвращения утечки личных данных (номер карты) не стоит давать никому или указывать на сайтах (интернет-магазины) свои личные данные банковских карт.

2. Взаимодействие Банка России и МВД России.

21 октября 2023 года вступил в силу законопроект о совместной работе МВД России и Банка России. Причина – увеличение случаев мошенничества в электронной системе. Банк России передает из своей базы данные о попытке совершения противоправных операций. МВД России может передавать данные о попытках переводов без согласия клиента.

3. Повышение кибербезопасности.

Каждый день сотрудники информационных отделов работают над улучшением работоспособности систем, внедрением новых технологий, основная задача которых – защита базы данных.

4. Биометрические данные.

Банки начинают использовать биометрические данные клиента во время осуществления выдаче кредитов. Также многие банки в скором времени будут использовать банкоматы, которые смогут осуществлять услугу, используя лишь биометрические данные клиента. Эту систему разрабатывают для уменьшения вероятности кражи денежных средств.

Основными критериями для успешного раскрытия преступлений данного вида являются: вовремя полученные данные о передвижении денежных средств и быстрое реагирование с момента получения информации.

В настоящее время злоумышленника не всегда можно задержать, зачастую он находится вне территории Российской Федерации. Например, за 2023 год участились случаи информационно-технологического мошенничества со стороны граждан, которые находятся на территории Украины. Задержать их нельзя по причине нахождения в другой стране. В таком случае самым сильным противодействием данного вида мошенничества будет выступать осведомленность граждан. Именно поэтому важна профилактика мошенничества. И следует уделять больше внимания разработкам памяток, которые важны для людей. Благодаря осведомленности граждан, рост подобных преступлений снизится. Самое важное, что нужно знать и что указывают в памятках, это:

1. Мошенники всегда первые выходят на контакт (электронное письмо, звонок и т.д.).
2. Предлагают кредитные карты, сообщают о выигрыше или представляются сотрудниками органов внутренних дел России и сообщают об утечке персональных данных.
3. Запрашивают персональные данные или просят продиктовать код подтверждения, который отправлен на мобильные устройство.

Частыми случаями является утечка информации. Так, в марте 2022 года произошла масштабная утечка данных «Яндекс.Еды», которая произошла из-за IT-атаки с внешнего хостинга. Во избежание таких ситуаций крупным компаниям нужно иметь хорошую защиту информации, постоянно работать над ее совершенствованием и сотрудничать с правоохранительными органами для избежания подобных инцидентов.

При раскрытии мошенничеств с использованием информационно-телекоммуникационных технологий будут считаться оперативно-разыскные мероприятия, которые закреплены в ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-разыскной деятельности» и связаны с использованием технических средств: прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации.

Таким образом, в 2012 году было внесено дополнение в виде новых составов мошенничества в ч. 3 ст. 158 Уголовного кодекса Российской Федерации предусматривающее уголовную ответственность за кражу с банковского счета. Внесение поправок говорит о том, что государство признало высокую общественную опасность данного деяния. Данное преступление совершается специально обученными людьми, которые прорабатываю огромное количество информации перед своими действиями. Они также следят за тенденциями в сфере защиты личных данных и ищут новые способы совершения преступного деяния.

Изучив статистику за январь – февраль 2024 года, можно сказать, что количество зарегистрированных преступлений возросло по сравнению с периодом январь – февраль 2023 года, на 23,5%. В большинстве случаев влиянию мошенников подвергаются люди старшего поколения. Считается, что население среднего возраста хорошо изучило схемы мошенников и реже попадают в

неприятные ситуации. Старшее поколение считается более доверчивым. Защититься от этого можно, с помощью отказа хранения крупных сумм на банковском счету.

Следует отметить, что с учетом роста преступлений в этой направленности и тяжестью раскрытия преступлений приоритетом будет выступать информационное обеспечение банковской деятельности и совершенствование информационных программ, предупреждение незаконных транзакций, совершенствование нормативной базы. Совершенствование систем взаимодействия Банка России и МВД России поможет предупредить преступления в сфере информационных технологий, в частности, с использованием безналичных расчетов и платежей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шавалеев Б.Э. Банковские меры противодействия преступлениям в сфере информационных технологий [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/bankovskie-mery-protivodeystviya-prestupleniyam-v-sfere-informatsionnyh-tehnologiy/viewer.

2. Яковлева Л.В. Современные способы дистанционного мошенничества // Вестник Краснодарского университета МВД России. – 2021. – № 4 (54). – С. 77–80.

3. Статистика МВД Росссии о состоянии преступности в Российской Федерации [Электронный ресурс]. – URL: https://мвд.Российской Федерации/news/item/48902908/.

РОЛЬ ПРИНЯТИЙ РЕШЕНИЙ В СИТУАЦИОННЫХ ЦЕНТРАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ ОБЕСПЕЧЕНИИ ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА

Терентьев А.А.,
кандидат технических наук
(Воронежский институт МВД России)

Аннотация: приводится описание роли принятия решений в ситуационных центрах органов внутренних дел при обеспечении охраны общественного порядка. Принимая во внимание возросшую степень опасности при проведении массовых мероприятий, необходимо понимать, что возрастает и роль подготовленных управленческих решений, которые позволят сотрудникам правоохранительных органов эффективно пресекать все виды правонарушений. В работе сформулирована и приведена блок-схема алгоритма принятий решений в ситуационных центрах при обеспечении охраны общественного порядка.

Ключевые слова: принятие решений, ситуационный центр органов внутренних дел, охрана общественного порядка, блок-схема алгоритма принятий решений.

THE ROLE OF DECISION-MAKING IN THE SITUATIONAL CENTERS OF THE INTERNAL AFFAIRS BODIES IN ENSURING THE PROTECTION OF PUBLIC ORDER

Terentyev A.A.,
Candidate of Technical Sciences
(Voronezh Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article describes the role of decision-making in the situational centers of the internal affairs bodies in ensuring the protection of public order. Taking into account the increased degree of danger during mass events, it is necessary to understand the increasing role of prepared management decisions that will allow law enforcement officers to effectively prevent all types of offenses. The paper formulates and presents a block diagram of the decision-making algorithm in situational centers while ensuring the protection of public order.

Keywords: decision-making, the situational center of the internal affairs bodies, public order protection, a block diagram of the decision-making algorithm.

Современные реалии заставляют общество подстраиваться под постоянные изменяющиеся переменные в жизни общества. Под переменными можно понимать различные степени угроз внутри государства, которые могут нанести вред государству и мирным жителям. В настоящее время большое внимание уделяется охране общественного порядка не только при обеспечении массовых

мероприятий, но и при штатных ситуациях. Прежде всего это обусловлено тем, что участились угрозы со стороны террористических групп. Сейчас именно как никогда требуется профессионализм, четко слаженные действия и в первую очередь эффективные управленческие решения от сотрудников правоохранительных органов, которые обеспечивают охрану общественного порядка и обеспечивают общественную безопасность государства.

Все действия сотрудников органов внутренних дел (далее – ОВД) на прямую зависят от управленческого решения, которое принимает руководитель. В теории принятия решения таким лицом является лицо, принимающее решение (далее – ЛПР) [1]. Решение формируются на основании мнений экспертов или лиц, участвующих в опросе. На основе данных оценок далее происходит формирование альтернатив управленческих решений, из которых ЛПР принимает какое-то одно решение для противодействия какой-либо угрозе.

При этом для сбора полной информации для разработки предложений по решению поставленной задачи требуется современное информационно-аналитическое и телекоммуникационное обеспечение, управление силами и средствами подразделений ОВД, постоянный мониторинг криминальной обстановки на выверенной территории, постоянный обмен информацией как с другими силовыми структурами, таким как МЧС России, ФСБ России, ФСО России, органами государственной власти, так и со средствами массовой информации. Такие многофункциональные задачи в органах внутренних дел может выполнять только ситуационный центр [2–3].

Принятие решения включает в себя не только сбор, обработку информации, а также процедуру подготовки решения. Данная процедура реализуется, как правило, на основе экспертного опроса. В ходе экспертного опроса, эксперты или лица участвующие в экспертном опросе производят сравнение альтернатив между собой и при помощи специализированных шкал дают оценки. На основе данных оценок формируется приоритетность сравниваемых альтернатив. Далее на основе обработанных приоритетов разрабатываются варианты решений.

Учитывая специфику охраны общественной безопасности, объекты, которые подлежат сравнению при экспертном опросе, могут иметь разную природу возникновения, сравнения которых между собой будет некорректным. Для этого при принятии решений в ситуационных центрах ОВД в интересах охраны общественного порядка предлагается использовать кластерный анализ, который будет заключаться в разделении объектов по группам однородности, в зависимости от содержащихся объектов сравнения в каждой кластерной группе будет назначаться компетентные эксперты в данной области.

Учитывая ранее разработанные алгоритмы и методики принятия решений в ситуационных центрах [4–6], разработаем блок-схему алгоритма принятия решений в ситуационных центрах ОВД при обеспечении охраны общественной безопасности.

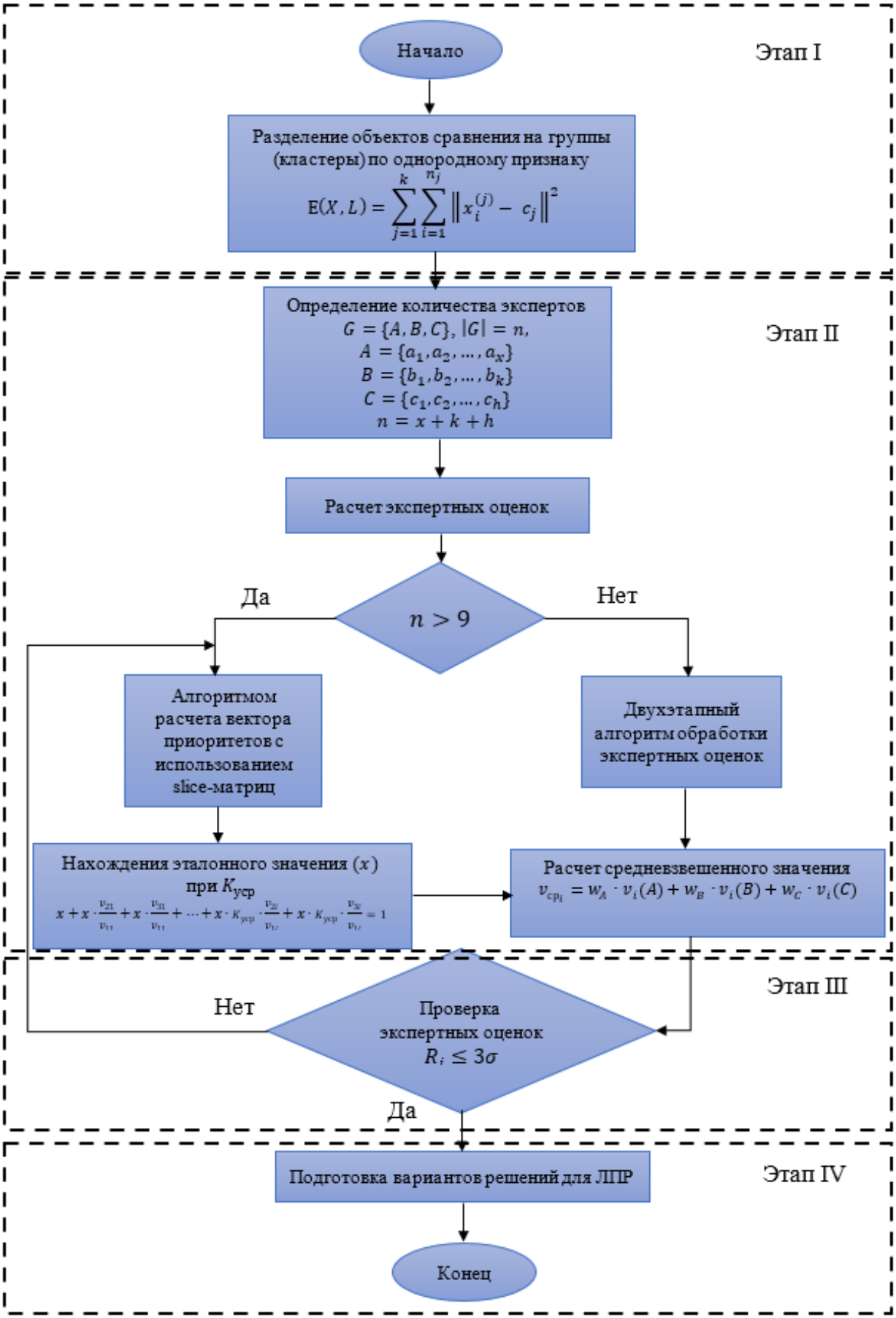


Рисунок 1. Блок-схема алгоритма принятия решения в ситуационных центрах ОВД при обеспечении охраны общественной безопасности

Предлагаемая блок-схема алгоритма принятия решения в ситуационных центрах ОВД при обеспечении охраны общественной безопасности позволит повысить эффективность подготавливаемых управленческих решений при обеспечении охраны общественной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Орлов А.И. Теория принятия решений. – Москва: Экзамен, 2005. – 656 с.

2. Ильин Н.И. Ситуационные центры. Опыт, состояние, тенденции развития / Н.И. Ильин, Н.Н. Демидов, Е.В. Новикова. – Москва: МедиаПресс, 2011. – 336 с.

3. Приказ МВД России от 16.11.2018 № 775 «Об утверждении Положения о Ситуационном центре Министерства внутренних дел Российский Федерации и Регламента работы Ситуационного центра Министерства внутренних дел Российской Федерации» [Электронный ресурс]. – Доступ из СПС «СТРАС «Юрист» (дата обращения: 15.05.2024).

4. Пьянков О.В., Терентьев А.А. Разработка численного метода определения весов конфликтных взаимодействий // Вестник Воронежского института МВД России. – 2019. – № 1. – С. 69–74.

5. Пьянков О.В., Терентьев А.А. Моделирование и параметрическая оптимизация проведения экспертного опроса с помощью slice-матриц // Вестник Воронежского государственного университета. – 2020. – № 2. – С. 127–135.

6. Терентьев А.А. Двухэтапный алгоритм обработки экспертных оценок в ситуационных центрах органов внутренних дел // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 118–126.

НЕКОТОРЫЕ АСПЕКТЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ

Федосеев А.Э.,
кандидат физико-математических наук;
Красноруцкая А.И.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются используемые в криптографии традиционные методы и интерпретация их реализаций. Сравниваются особенности их реализации с современными методами. Оцениваются перспективы их применимости и направления развития.

Ключевые слова: криптография, шифрование, вычислительная сложность, ключ, защита информации.

SOME ASPECTS OF MODERN CRYPTOGRAPHY

Fedoseev A.E.,
Candidate of Physical and Mathematical Sciences;
Krasnorutskaya A.I.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article examines the traditional methods used in cryptography and the interpretation of their implementations. The features of their implementation are compared with modern methods. The prospects of their applicability and development directions are evaluated.

Keywords: cryptography, encryption, computational complexity, key, information security.

Современное общество принято интерпретировать как информационное, поскольку информация давно стала значимой ценностью во всех сферах жизнедеятельности человека, а также породила направленные на ее обслуживание технологии. Обладая ценностью, информация становится самостоятельным продуктом, который в свою очередь может стать и предметом противоправной деятельности, причем его можно как украсть с целью обогащения, так и преобразовать (исказить), сделав инструментом противоправной деятельности, как в экономическом эквиваленте, так и в качестве элемента информационного противодействия. И если идея закрытия определенных сведений исторически проявила свою востребованность еще до нашей эры, то в сегодняшнем информационном обществе защита информации – это необходимость, обязательное условие.

Практическая реализация по обеспечению безопасности сведений и данных может базироваться на криптографических алгоритмах. В их основе лежит идея преобразования информации с целью быть доступной только определенному кругу лиц, обладающих знаниями о методе закрытия конкретного сооб-

щения. Как правило, к ним относятся использование двусторонних функций или шифров, а также ключей для возможности получения открытой информации из закрытого сообщения. Использование односторонних функций нацелено на подтверждение неких свойств и применяется для аутентификации, указания подлинности или целостности, не получая в результате исходного сообщения. Совокупность таких реализаций рассматривает криптография (от греч. «тайнопись»), использующая математические методы для воздействия на информацию и позволяющая производить общение без раскрытия самой информации.

Исторически традиционные алгоритмы шифрования основываются на подстановке – замене элементов информационного сообщения другими, и перестановке – изменении порядка расположения элементов в сообщении. Многослойные комбинации этих воздействий усложняют преобразование текста, делая его более защищенным.

Современный параметр защищенности определяется криптографической стойкостью, т.е. обладанием недостижимого объема вычислительных ресурсов для возможности получения посторонним открытого сообщения. Криптография в связке с возможностями информатики и современными техническими устройствами реализует задачу так называемой высокой вычислительной сложности или же делает теоретическую разрешимость задачи дешифровки посторонним нереализуемой практически.

Использование сетевых технологий, в частности глобальной сети как среды передачи информации, где теоретически возможно нарушение целостности сообщений, сделало востребованным и действенным инструмент подтверждения подлинности – электронную подпись. Она используется в рамках электронного документооборота, считается значимой в финансовом обороте, а также реализована в контексте электронного правительства и информационного общества в Российской Федерации [1]. С одной стороны, она является отражением реквизита документа в цифровом мире, с другой – является средством защиты информации. Построение ее алгоритмов основывается на вышеописанных принципах традиционной криптографии, а их современная реализация расширяется на основе комбинаций преобразований и архитектурных платформ применения.

Среди современных тенденций в криптографии присутствуют методы, основанные на математических задачах, для которых определена вычислительная невозможность нахождения эффективного решения. Однако стойкая на сегодня реализация, по мнению аналитиков, имеет неоднозначное будущее, например, по причине количественной ограниченности схем, связанных с такими задачами [2]. Еще один пример неоднозначного будущего: для задачи по экспоненциализации некоторого простого по модулю числа, на которой построен алгоритм RSA, размерность «безопасных» чисел увеличилась на порядок от начала его применения. При этом алгоритмы, относящиеся к классической криптографии, например, использующих сеть Фейстеля, усложнялись увеличением длины ключа с момента их создания лишь в два раза. С учетом их реализации на одинаковых платформах очевиден экстенсивный путь развития для некоторых из них.

Технологическое развитие влечет за собой, с одной стороны, упрощение реализации процедур криптоанализа, с другой – необходимость инноваций в криптосинтезе. Уменьшение времени проведения вычислений по вскрытию шифра в качестве противодействия со стороны криптографии потребует увеличение длины ключа и используемых блоков, что сделает криптосистемы более громоздкими. Увеличение скорости вычислений может позволить решить «неразрешимые» на сегодня задачи, что повлечет необходимость поиска новых алгоритмов. Например, значительно увеличить произведение расчетов позволят системы на основе квантовых вычислений, активно развивающиеся в последнее время, и которые, вероятно, смогут взламывать современные стойкие алгоритмы. Технологический противовес – квантовое шифрование, использующее многоуровневое кодирование фазовых степеней свободы когерентных оптических состояний, апробированное на практике двадцать лет назад [3].

Альтернативная ветвь развития – легковесная или малоресурсная криптография, потребность в которой спровоцировал расширяющийся Интернет вещей. Его составляют «легкие» или ограниченные по ресурсам конечные устройства, но реализующие обмен суммарно больших объемов информации, которая в свою очередь требует обеспечения достаточного уровня безопасности. Это направление, не смотря на свою упрощенность в реализации, является задачей повышения эффективности, так как должна сочетать в себе достаточный уровень криптографической надежности на минимальной производительности оборудования. Также актуальна идея, отходящая от традиционных методов, – гомомоРоссийской Федерациионое шифрование, позволяющее, не раскрывая исходных данных, производить математические операции над зашифрованной информацией и давать тот же результат, что и операции над открытым текстом. Такой вид шифрования применяется в поисковых системах при «приватном» поиске или в облачных сервисах.

Информационная безопасность является одним из стратегических национальных приоритетов нашего государства [4]. Криптография же является инструментом в обеспечении информационной безопасности [5]. О ее значимости говорит использование криптографических алгоритмов и в древней истории, и в век информационных технологий. Ее актуальность подтверждают современные тенденции в расширяющемся спектре реализаций в условиях развивающихся информационных систем и технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Постановление Правительства РоссийскоЙ Федерации от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» [Электронный ресурс]. – Доступ из СПС «КонсультантПлюс».

2. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. – Санкт-Петербург: НИУ ИТМО, – 2012. – 142 с.

3. Ahn C., Birnbaum K. Exposed-key weakness of αη // Physics Letters A. – 2006. – V. 370. – P. 131–135.

4. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // СПС «КонсультантПлюс».

5. Федосеев А.Э. Построение функционального набора системы безопасности на основе возможных классификаций угроз безопасности информации / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Всероссийской научно-практической конференции (17 мая 2019 года). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2019. – С. 205–210.

ПОТЕНЦИАЛ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КРИМИНОЛОГИЧЕСКИХ ИССЛЕДОВАНИЯХ

Хатунцев М.И.
(Российский государственный гуманитарный университет)

Аннотация: в статье рассматриваются перспективы применения систем искусственного интеллекта в криминологических исследованиях. В современных условиях искуственны интелект не только способен решать конкретные задачи, но и приближается к полноценному мышлению человека. На текущий момент автоматизация исследований анализа преступности, исторических данных, выявление факторов, влияющих на уровень преступности, характеристик личности преступников, а также прогнозирование рецидива среди определенных групп может быть осуществлена при помощи искусственного интеллекта. искуственны интелект может стать незаменимым инструментом для оптимизации исследований в части выявления психологических динамик, оценки эффективности различных видов уголовного наказания и определения ключевых фигур в криминогенных группах.

Ключевые слова: криминология, криминологические исследования, предупреждение преступлений, искусственный интеллект, технологии искусственного интеллекта.

POTENTIAL OF USING ARTIFICIAL INTELLIGENCE SYSTEMS IN CRIMINOLOGICAL RESEARCH

Khatuntsev M.I.
(Russian State University for the Humanities Russia)

Abstract: the article discusses the prospects for the use of artificial intelligence systems in criminological research. In modern conditions, artificial intelligence is not only capable of solving specific problems, but is also approaching full-fledged human

thinking. Currently, automation of crime analysis research, historical data, identification of factors influencing the crime rate, personality characteristics of criminals, as well as prediction of recidivism among certain groups can be carried out using artificial intelligence. artificial intelligence can become an indispensable tool for optimizing research in identifying psychological dynamics, assessing the effectiveness of various types of criminal punishment, and identifying key figures in crime groups.

Keywords: criminology, criminological research, crime prevention, artificial intelligence, artificial intelligence technologies.

Искусственный интеллект – создаваемое с помощью группы смежных технологий программное обеспечение, функционирующее нелинейно, способное к обучению, ограниченному пониманию причинности и выполнению задач интеллектуального, эвристического характера с возможностью обучения, корректировки и уточнения за счет опыта принимаемых решений [3, с. 207].

За последние годы использование искуственны интелект (далее – ИИ) стало широко распространенным: от голосовых помощников до автономных транспортных средств.

Важным направлением для применения ИИ является борьба с преступностью, поскольку он способен охватывать широкий спектр задач и направлений. Используя ИИ, можно анализировать огромные объемы сложных данных и выявлять закономерности и взаимосвязи, которые часто остаются незамеченными для человеческого анализа, включая обработку информации из социальных сетей, камер наблюдения и вышек сотовой связи. Путем применения алгоритмов машинного обучения правоохранители могут извлечь ценные данные, которые помогут повысить раскрываемость преступлений.

Одним из направлений применения ИИ в расследовании преступлений является его использование для анализа доказательств. Традиционные криминалистические методы, такие как анализ ДНК, отпечатков пальцев и баллистическая экспертиза применяются уже десятилетиями для идентификации подозреваемых и установления их причастности к преступлениям. Использование ИИ может улучшить точность и эффективность этих методов.

Таким образом, ИИ становится мощным инструментом, способным улучшить эффективность и результативность процесса анализа.

Применение технологий ИИ в криминологических исследованиях имеет значительный потенциал, предоставляя уникальные возможности для анализа и прогнозирования преступлений, понимания мотивов преступников, а, следовательно, и в оптимизации работы правоохранительных органов и предотвращении преступлений.

Растущий интерес научного сообщества к применению ИИ в правоохранительной деятельности подчеркивает значимость этого нового инструмента.

Криминологический метод не только предоставляет данные о преступности, но и представляет собой подход к решению задач, связанных с выявлением системности совершаемых преступлений на определенной территории за конкретный промежуток времени.

Методика криминологических исследований представляет собой совокупность специфических приемов и средств сбора, анализа и оценки информации о преступности и ее причинах, личности преступника, а также оценки эффективности мер борьбы с ней.

Так, например, анализ статистических данных в криминологии играет важную роль в выявлении тенденций криминальной активности. Это помогает определить факторы, влияющие на уровень преступности, и разработать меры для ее снижения. Также он помогает выявить наиболее распространенные виды преступлений и группы населения, наиболее подверженные криминальной деятельности, что позволяет сосредоточить усилия на предотвращении преступлений в этих областях. Оценка эффективности различных стратегий борьбы с преступностью осуществляется через анализ данных о преступлениях и применяемых мерах. Модели прогнозирования преступлений, основанные на анализе статистических данных, помогают предсказывать места, время и типы преступлений для более эффективного распределения ресурсов правоохранительных органов и предотвращения преступлений.

ИИ в данном случае способен расширить возможности анализа преступности и личности преступников. Он в состоянии обрабатывать большие объемы данных о преступлениях, включая их статистику и характеристики преступников. ИИ может прогнозировать рецидив среди групп риска, предсказывать вероятность совершения преступлений, анализируя исторические данные, а алгоритмы машинного обучения могут создавать профили преступников, определять угрозы, выявлять аномалии в этих данных. Эти возможности не только обогащают понимание преступности как социального явления, но и помогают улучшить эффективность правоохранительных операций.

Метод анкетирования позволяет собирать данные по показателям, которые недоступны в статистических материалах и, что важно, проверять эти данные неоднократно: формирование профиля преступника, включая его характеристики, образ жизни, криминальную историю и другие факторы для более глубокого понимания мотивов преступления. Анализ этих данных помогает лучше интерпретировать природу преступности, выявить риски и защитные факторы, разработать эффективные стратегии предотвращения преступлений и улучшить систему уголовного правосудия.

ИИ представляет собой ценный инструмент для объективного анализа анкетных данных и результатов интервью, используемых для изучения личности преступников, потерпевших и общественного мнения.

«Обработка естественного языка (далее – НЛП) представляет собой комплекс вычислительных методов, разработанных для автоматического анализа и интерпретации человеческого языка. Исторически НЛП возникло в период эпохи пеРоссийской Федерациикарт и пакетной обработки данных, когда анализ текста занимал до 7 минут на предложение. В настоящее время, в эпоху Google и аналогичных систем миллионы веб-страниц могут быть обработаны менее, чем за секунду» [4, с. 1].

«NLP связано с применением различных подходов, которые в итоге приводят текст, представленный на естественном языке, к такому виду, который позволяет алгоритму его обрабатывать и извлекать из него необходимые данные» [1, с. 76].

Так, используя алгоритмы НЛП, ИИ способен выявлять ключевые темы, эмоциональные оттенки и мнения, содержащиеся в тексте, что поможет обнаружить образцы и тренды в данных, связанных с мотивами и поведением преступников, а также оценивать доверие к этим данным. Анализируя социальные взаимодействия и сети преступников, потерпевших и общественности, ИИ выявляет влияние социального окружения на поведение и реакцию общества на преступления. На основе этих данных ИИ может прогнозировать вероятность рецидива, способствуя разработке программ реабилитации.

Социометрический подход позволяет исследовать криминологические аспекты взаимоотношений в группе, оценивать их, выявлять психологические динамики, наличие конфликтов, формирование групп. В криминологических исследованиях этот метод полезен для оценки эффективности различных видов уголовного наказания, таких как тюремное заключение, исправительные работы и ограничение свободы.

ИИ облегчает проведение социометрических исследований в различных отраслях, не исключая и криминологические исследования. Используя ИИ, можно анализировать структуры и динамики, выявлять ключевые фигуры и паттерны влияния, что помогает идентифицировать криминогенные группы и факторы, способствующие преступлениям. ИИ также может прогнозировать возможные криминальные сценарии на основе обрабатываемых данных. Путем анализа рецидива и эффективности наказаний ИИ помогает определить и разрабатывать эффективные стратегии предотвращения преступлений и управления социальными рисками. Наконец, использование ИИ в социометрических исследованиях в криминологии способствует лучшему пониманию социальных динамик и криминальных тенденций, что в конечном итоге повышает эффективность мер предотвращения преступлений и улучшает систему правосудия.

Разумеется, исследование преступности с применением ИИ требует разнообразных методов обучения. Как было указано, машинное обучение является основным методом, который позволяет разрабатывать алгоритмы для выявления закономерностей и прогнозирования будущих событий.

Глубокое обучение, использующее искусственные нейронные сети, позволяет обрабатывать сложные данные и распознавать скрытые шаблоны в криминальном поведении. Обучение с подкреплением помогает разрабатывать стратегии превентивных мер и оптимизировать работу правоохранительных органов на основе взаимодействия с окружающей средой. НЛП позволяет анализировать текстовую информацию, включая обвинительные приговоры, для выявления ключевых слов и тем, связанных с преступлениями. Кластерный анализ и классификация группируют данные на основе сходства и позволяют выделять различные типы преступлений или категории правонарушителей.

Методы обучения с учителем и без учителя могут быть использованы для учебы на известных примерах или для обнаружения скрытых закономерностей в данных. Эти методы могут комбинироваться и адаптироваться в зависимости от конкретных целей и задач исследования в области криминологии.

В заключение можно отметить, что использование ИИ открывает новые перспективы для более глубокого и объективного анализа данных о преступности, личности преступников, социальных взаимодействиях и эффективности правосудия.

С помощью алгоритмов машинного обучения и анализа данных ИИ может выявлять образцы, тенденции и взаимосвязи, которые ранее могли оставаться незамеченными. Это позволяет лучше понять причины преступности, разрабатывать более эффективные стратегии реабилитационных мероприятий.

Внедрение ИИ в криминологические исследования также может способствовать более точному прогнозированию криминальных сценариев, адаптации стратегий и оптимизации использования ресурсов правоохранительных органов.

Однако необходимо помнить об этических и правовых аспектах использования ИИ в криминологических исследованиях. При правильном подходе и учете этих факторов внедрение искусственного интеллекта обещает значительное совершенствование криминологической науки и практики, что в конечном итоге может привести к повышению эффективности борьбы с преступностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Зенин С.С., Кутейников Д.Л., Япрынцев И.М., Ижаев О.А. Технология обработки естественного языка (NLP) в законодательном процессе // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20. – № 3. – С. 76–81.

2. Ильницкий А.С. Технологии искусственного интеллекта в криминологической науке и предупреждении преступлений // Вестник Московского университета МВД России. – 2023. – № 7. – С. 105–111.

3. Степаненко Д.А., Бахтеев Д.В., Евстратова Ю.А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. – 2020. – Т. 14. – № 2. – С. 206–214.

4. Tom Young, Devamanyu Hazarika, Soujanya Poria, Erik Cambria. Recent Trends in Deep Learning Based Natural Language Processing [Электронный ресурс]. – URL: https://arxiv.org/pdf/1708.02709 (дата обращения: 27.04.2024).

ПЕРСПЕКТИВЫ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Худяков В.В.,
Тряпкина Л.Ю.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: киберпреступность представляет собой относительно новое явление в современном понимании права, связанное с совершением преступлений в процессе цифровизации. В этой сфере совершается значительное количество преступлений, что делает ее менее защищенной, более уязвимой и требующей повышенного внимания для регулирования. Таким образом, кибербезопасность приобретает особую значимость для обеспечения защиты всех информационных ресурсов, подвергающихся кибератакам.

Ключевые слова: кибербезопасность, цифровизация, киберпространство, кибератаки, информация.

PROSPECTS FOR THE DEVELOPMENT OF CYBER SECURITY IN THE DIGITALISATION OF SOCIETY

Khudyakov V.V.,
Tryapkina L.Yu.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: cybercrime is a relatively new phenomenon in the modern understanding of law, associated with the commission of crimes in the process of digitalisation. A significant number of offences are committed in this area, making it less protected, more vulnerable and requiring increased attention for regulation. Thus, cybersecurity is of particular importance to ensure the protection of all information resources subject to cyberattacks.

Keywords: cybersecurity, digitalisation, cyberspace, cyberattacks, information.

Развитие общества происходит безостановочно, достаточно посмотреть историю любого государства и общества. Вместе с историческим развитием совершенствуются технологии, наука, промышленность, производство и т.д. С течением времени появлялись новые теоретические осмысления прошлых и существующих в наше время проблем, таких как: рост киберугроз, их разновидности, перспективные методы борьбы. Кибербезопасность, безусловно, сложна, комплексна и особенно динамична, так как идут постоянные изменения в структуре общества, какие-то его элементы теряют свою актуальность, перестают функционировать, а какие-то впервые проявляются. В современном обществе происходит рост цифровых возможностей, которые подчеркивают под-

линную важность кибербезопасности. И именно эти новые компоненты требуют особенного регулирования и внимания, а также подлежат процессу интегрирования.

Современное общество за последние двадцать с лишнем лет столкнулось с новым явлением, сложнейшим процессом, который называется цифровизацией Цифровизацию понимают в двух смыслах: в широком и узком [1, с. 43]. В широком смысле под цифровизацией понимается современная общемировая интеграция и развитие общества и экономики, которая базируется на преобразовании информации в цифровую форму и приводит к повышению эффективности экономики и улучшению качества жизни. Важно всего лишь визуализировать, какое количество данных мы ежедневно обрабатываем на персональном компьютере, смартфоне, планшете, сколько учетных записей мы используем для самых различных приложений, на платформах в сети Интернет. А сколько кредитных, банковских, иных конфиденциальных данных запрашивается в повседневной жизни на различных ресурсах? К сожалению, эти данные уязвимы для киберпреступников, которые злонамеренно используют их в корыстных целях.

Если говорить про узкое понятие, то оно представляется следующим образом – это внедрение современных цифровых технологий в различные сферы жизни общества и производства. Затрагивая данное определение, мы будем рассматривать его с позиции внедрения современных цифровых технологий в жизнь человека и гражданина, а также их влияние на наши права, свободы, интересы. Иными словами, цифровизация в узком смысле представляет собой процесс перехода от аналоговой формы представления информации на цифровую. Однако с расширением использования количества цифровых технологий параллельно становится больше и прогрессивнее вероятность кибератак, кражи персональных данных, что напрямую приводит к увеличению показателя числа преступлений в государстве. Поэтому одним из значимых и заметных изменений, которое непосредственно связано с цифровизацией, является развитие сети Интернет и социальных сетей.

На сегодняшний день мы без трудностей можем общаться с товарищами в любой точке нашей планеты, обмениваться информацией и передавать полезный опыт. Помимо этого социальные сети представлены как одна из самых важных форм проявления отношений между людьми, именно сейчас в них чаще всего и больше всего возникают как правоотношения, так и, собственно, сами права, которые имеют свою специфику, проблематику и сущность. В настоящее время, благодаря цифровым технологиям, мы имеем прекрасную возможность существенно упростить и ускорить решение различных задач, требующих непременного решения, устранение коллизий, которые предстают перед нами, что в свою очередь позволит нам в большем количестве уделять время более важным мероприятиям. Но большинство из пользователей хотя бы раз попадали под давление киберпреступников, которые пытались завладеть информацией далеко не добросовестными способами. Поэтому важно серьезно отнестись к обеспечению безопасности цифровых технологий и информации, хранящейся в сети, следует детально ознакомиться с инструментами кибербез-

опасности, ее перспективами. Именно это является предикативной причиной повышения уровня развития кибербезопасности.

Кибербезопасность трактуется по–разному например:

1) Практическая деятельность, направленная на защиту сетей, конфиденциальной информации, такой как персональные данные, коммерческая тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений и так далее, приложений и пользователей от кибератак [2].

2) Своего рода мера, главной целью которой является масштабное снижение или пресечение несанкционированного доступа к устройствам, сетям и их данным.

3) Состояние защищенности важнейших систем и сети от совокупности преступлений, например цифровых атак, совершаемых в киберпространстве посредством компьютерных систем или иных средств доступа к киберпространству, представляя собой согласованный набор процессов, технологических решений, механизмов и рекомендаций.

К сожалению, напряженность в виртуальной реальности, где мы, пользователи, свободно можем коммуницировать, обмениваться новой и полезной информацией, вести различного рода деятельность набирает огромные обороты. Это обуславливается тем, что в процессе цифровизации колоссально возрастает показатель киберугроз. Стоит отметить, что с каждым разом киберпреступники становятся более опытными и продуманными, досконально изобретая новые методы атак на частных лиц и организации. Также в процессе цифровизации увеличивается объем информации, которая непосредственно хранится в так называемом «виртуальном пространстве», где мы проводим большую часть своего свободного времени. На сегодняшний день практически все, начиная от элементарной покупки в сети Интернет, обучения в школах, высших учебных заведениях, работы, заканчивая обыденными развлечениями, осуществляется с помощью всемирной паутины (World Wide Web), то есть в сети Интернет. Это делает данные пользователей более доступными для ловких рук злоумышленников.

Низкий уровень кибербезопасности также является одной из важнейших причин роста напряжения в интернет-пространстве. Многие пользователи и организации не уделяют достаточного внимания значимости кибератак по различным причинам. Например, у некоторых пользователей частично или даже полностью отсутствует опыт взаимодействия с киберпространством. Для многих кибербезопасность кажется достаточно комплексной, обогащенной непростыми для обыденного восприятия механизмами и темами, так как в условиях непрерывной цифровизации многие аспекты кибербезопасности приобретают более широкий комплекс направлений. Другие же не имеют достаточных ресурсов на углубленное, а не поверхностное изучение кибербезопасности, способов предотвращения киберугроз в современном мире элементарно из-за нехватки времени, что обосновывается плотным трудовым графиком, или же собственной ленью. Вышеперечисленные факты, конечно же, делают пользователей беззащитными. Слабые пароли, низкая защита персональных данных, непроверенное программное обеспечение, недостаточные меры защиты, а также

распространение интернет-вещей, таких как смарт-часы, умные дома, роботы-пылесосы и многие другие – все вышеперечисленное беспрепятственно создает широкие возможности для киберпреступников, что является следствием серьезнейших киберугроз.

Анализируя статистику, содержащуюся в отчете Check Point о безопасности 2023 года [3], количество еженедельных кибератак во всем мире увеличилось примерно на 8%, что вызвало огромный диссонанс, так как это является одним из самых резких показателей роста кибератак за последние два года. Бесспорно, киберпреступления – одна из самых насущных и опасных проблем двадцать первого века. Далее рассмотрим самые распространенные киберпреступления.

- Фишинг (англ. «fishing» – *рыбная ловля, выуживание*) является видом киберпреступлений, при котором мошенник буквально вынуждает пользователя-жертву передать ему информацию личного характера, выдавая себя за надежный и защищенный источник в сети Интернет.
- Вишинг (англ. «vishing», состоит из двух слов: «voice» – голос и «pfhishing» – фишинг) – одна из современных кибератак, разновидность фишинга, которая в качестве средства атаки использует телефон, а именно – телефонный звонок.
- Диссинг (англ. «dissing» – оскорбление, оскорбительный) – своего рода часть кибербуллинга, являющаяся открытой формой травли через распространение недобросовестной и во многих аспектах лживой информации, порочащей честь и достоинство личности. Главной целью данной кибератаки является, конечно же, максимальное снижение репутации пострадавшего через фото- и видео-публикации, которые чаще всего являются фейковыми.
- DDoS-атака (англ. «Distributed Denial of Service» – распределенная атака типа «отказ в обслуживании») – одна из самых распространенных и вредоносных кибератак, которая благодаря нападению на информационную систему вызывает отказ в обслуживании, то есть выводит из состояния нормального функционирования, нарушает работоспособность. Одним из опасных проявлений данной атаки является атака номера телефона обычного пользователя или организации. К неблагоприятным последствиям относится то, что на мобильный телефон будут поступать различные звонки, содержащие информацию о разного рода рекламы без разрешения человека на их получение – спам-звонки.

Именно с процессом цифровизации и развитием информационно-коммуникационных технологий среди многих пользователей и организаций появляется желание в поиске возможности для благоприятного жизненного продвижения в киберпространстве. Перспективы развития кибербезопасности в процессе внедрения технологий в различные сферы жизни человека грандиозны, представляя собой главнейшую задачу, которая актуальна как среди отдельных пользователей и компаний, так и всего государства в целом. В современном мире по-разному обособляют перспективы кибербезопасности, но среди ключевых следует выделить: во-первых, усовершенствование работоспособности искусственного интеллекта.

Из-за того, что его потенциал практически не имеет границ, то в его основу можно внедрить различные техники, которые будут направлены исключительно на предотвращение кибератак. Искусственный интеллект в современном обществе направлен на создание мощнейших, эффективных и менее затратных инструментов в антивирусных программах, необходимых для обнаружения и дальнейшего предотвращения вредоносных угроз. Также его деятельность направлена на анализ громоздких объемов данных, обрабатывая их во много раз быстрее и эффективнее, чем человек, дополнительно выявляя подозрительную активность.

Искуственный интеллект помогает различным компаниям принимать оперативные, логичные и обоснованные решения, повышая качество продукции и услуг, во многом снизив затраты на обработку информационных данных. Показательным примером может служить опыт применения искуственного интеллекта при обеспечении защиты своих клиентов со стороны коммерческих организаций от вишеров (мошенничество по телефону). Сервисом предложенной платформы является технология «Нейрощит» (Новая технология Тинькофф Мобайла, предназначенная для защиты абонентов от злоумышленников в период реального времени), в основе которой находится искусственный интеллект, позволяющий выявлять и беспрепятственно пресекать попытки киберпреступления, когда происходит телефонный звонок, полностью анализируя и сопоставляя глобальное количество технических характеристик неизвестного входящего звонка. Немаловажным достоинством данной технологии является то, что через анализ технической информации, которая содержится в звуковой волне, можно безусловно обнаружить злоумышленника, пытавшегося завладеть конфиденциальной информацией. С каждым днем сценарии, заложенные в основу киберугрозы, интерпретируются, безостановочно совершенствуются, обучаясь на всех входящих данных.

Во-вторых, основной акцент нужно сделать на законотворческом процессе в Российской Федерации. А именно на безопасности в киберпространстве, которая урегулирована законами и иными нормативными правовыми актами, главной целью которых является защита информации пользователей от несанкционированного доступа злоумышленников. Обновление нормативной базы, ее совершенствование в процессе цифровизации представлены как важнейшая задача в сфере обеспечения информационных систем от возможных киберугроз. С изменением общего миропорядка возникает необходимость применения адекватных мер, направленных на обеспечение защиты коммерческих и государственных организаций. В этой связи Указом Президента Российской Федерации было определено требование с 1 января 2025 года о недопущении использования программных продуктов и систем из недружественных стран [4].

В-третьих, следует уделить особое внимание усовершенствованию общественного сознания в области кибербезопасности, а именно повысить уровень образовательной активности и подготовленности среди населения. Стоит отметить работу средст массовой информации, проводящих разъяснительную работу в доступной форме для широкого круга пользователей, будь то новостная лента либо информационные очерки или анимированные развлекательные сюжеты мультфильмов.

Таким образом, кибербезопасность остается важнейшим звеном в обеспечении нашей защищенности в информационной сфере. Не нужно отрицать того, что окружающий нас мир постоянно меняется, преобразуясь вместе с техническим прогрессом, но именно своевременное выявление новейших угроз, вклады в разработку технологий и образование позволяют на несколько шагов опережать злые намерения киберпреступников. Кибербезопасность касается не только государства, но и каждого гражданина, который отвечает за свое будущее. Развитие этой области имеет огромное значение для общей безопасности цифрового мира.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ганиев С.К., Худойкулов З.Т., Насруллаев Н.Б. Основы кибербезопасности. – Ташкент: Excellent polygraphy, 2021. – 224 с.
2. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (последняя редакция) [Электронный ресурс] // СПС «КонсультантПлюс».
3. Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research [Электронный ресурс]. – URL: https://blog.checkpoint.com (дата обращения: 12.05.2024).
4. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс] // СПС «Гарант».
5. Прокопенко А.Н., Жукова П.Н., Страхов А.А. Основные тренды в сфере кибербезопасности в России на современном этапе // Математические методы и информационно-технические средства: материалы XIX Международной научно-практической конференции, Краснодар, 22 июня 2023 года. – Краснодар: Краснодарский университет МВД России, 2023. – С. 233–240.
6. Агаев М.М., Куриленко Ю.А. Виды фишинговых атак и способы противодействия / Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел: сборник материалов Всероссийской научно-теоретической конференции, Ростов-на-Дону, 22 апреля 2022 года. – Ростов-на-Дону: Ростовский юридический институт МВД России, 2022. – С. 95–98.
7. Комардина А.А., Меняйло Д.В., Меняйло Л.Н. Применение информационных технологий и возможностей цифровизации в деятельности сотрудника ОВД / Экономическая безопасность: правовые, экономические, экологические аспекты: сборник научных трудов 6-й Международной научно-практической конференции, Курск, 9 апреля 2021 года. – Курск: Юго-Западный государственный университет, 2021. – С. 184–187.
8. Куриленко Ю.А., Любаева Д.С. Мошенничества в сфере компьютерной информации / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей X Всероссийской научно-практической конференции, Белгород, 19 мая 2023 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – С. 125–128.

АКТУАЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕДЕНИИ НЕКОТОРЫХ ОПЕРАТИВНО-РАЗЫСКНЫХ МЕРОПРИЯТИЙ

Челядинов Д.В.,
кандидат технических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье раскрыто теоретическое представление об основных аспектах применения технических средств и информационных технологий, направленных на проверку правдивости показаний опрашиваемых лиц с использованием комплексов психофизиологических исследований. Рассмотрены и проанализированы некоторые варианты тактических приемов по проведению оперативно-разыскного мероприятия «опрос» с применением соответствующих аппаратно-программных комплексов, в том числе в негласной форме дистанционным способом. Статья содержит вывод о том, что эффективность применения комплексов психофизиологических исследований будет определена только в процессе практического применения сотрудниками оперативных подразделений правоохранительных органов. Автором высказываются конкретные предложения по совершенствованию деятельности органов внутренних дел в рассматриваемой сфере.

Ключевые слова: технические средства, комплекс психологических исследований, дистанционное применение, программное обеспечение, мобильные устройства, оперативно-разыскные мероприятия.

TOPICAL ISSUES OF THE USE OF INFORMATION TECHNOLOGY IN CARRYING OUT SOME OPERATIONAL INVESTIGATIVE ACTIVITIES

Chelyadinov D.V.,
Candidate of Technical Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: this article reveals a theoretical understanding of the main aspects of the use of technical means and information technologies aimed at verifying the veracity of the testimony of the interviewees using complexes of psychophysiological studies. Some variants of tactical techniques for conducting an operational search event «survey» with the use of appropriate hardware and software complexes, including in an unspoken form by remote means, are considered and analyzed. The article concludes that the effectiveness of the use of complexes of psychophysiological research will be determined only in the process of practical application by employees of operational units of law enforcement agencies. The author makes specific proposals to improve the activities of the internal affairs bodies in this area.

Keywords: technical means, complex of psychological research, remote application, software, mobile devices, operational investigative measures.

В современном обществе довольно остро стоит вопрос об актуализации всевозможных технических средств при получении достоверной и качественной информации в рамках осуществления оперативно-разыскной деятельности, которые в дальнейшем могут кардинально изменить методику предупреждения, выявления и раскрытия противоправных деяний. Это стало значимым фактором, влияющим на целесообразность создания и применения различных комплексов психофизиологических исследований, в том числе беспроводных. Беспроводные технические средства применяются дистанционно и, как правило, негласно для объекта исследования, соответственно объект не осознает то, что в отношении него проводятся какие-либо мероприятия [1].

Таким образом, бесконтактный комплекс психофизиологических исследований представляет собой техническое устройство, не требующее закрепления считывающих датчиков на теле испытуемого, принцип работы которого реализует сложный алгоритм, оценивающий множество невербальных и физиологических признаков человека.

Существует множество разработок в сфере применения бесконтактных комплексов психофизиологических исследований, рассмотрим некоторые из них.

Одним из направлений бесконтактных психофизиологических исследований является определение правдивости ответов на поставленные вопросы по голосу. Принцип работы такого комплекса основан на сложном алгоритме, который оценивает десятки невербальных признаков речи – изменение тембра и громкости голоса, темп речи, количество запинок и другие. Можно отметить, что эта технология уже прекрасно себя зарекомендовала, пройдя тщательную проверку. С ее помощью было успешно проведено значительное количество судебных экспертиз, подтвержденных классическим «детектором лжи» и последующими оперативно-разыскными мероприятиями [2].

Несмотря на достаточно корректную работу, программное обеспечение новых комплексов психофизиологических исследований продолжает дорабатываться и совершенствоваться. Разработчики данных устройств сегодня активно занимаются совершенствованием технологий бесконтактной проверки правдивости показаний, а одним из наиболее приоритетных направлений является использование данного рода технических средств в автоматическом режиме. Если это удастся сделать, то затраты времени на подготовку сотрудников по работе с «детектором лжи» существенно сократятся. Кроме того, сам процесс использования прибора станет намного проще.

Если говорить о долгосрочной перспективе, то разработчики планируют довести свое творение до варианта мобильного приложения. При этом уточняется, что пользоваться комплесом без специальных навыков все равно не получится. Оказывается, для корректной работы устройства необходимо правильно проводить интервью с испытуемым. Так что целевая его сфера использования – это правоохранительная деятельность и в частности при проведении оператив-

но-разыскных мероприятий в рамках осуществления оперативно-разыскной деятельности правоохранительными органами [3].

Разработчики данных устройств нацелены на дальнейшее внедрение выше указанных программ непосредственно в планшеты, смартфоны и иные мобильные устройства, однако ввиду сложности алгоритма работы с ними, для лица, которое станет применять такого типа оборудование, будет предусмотрено прохождение дополнительного обучения, необходимого для получения специальных навыков обращения с бесконтактными комплексами психофизиологических исследований.

Принцип работы этих инновационных устройств схож с обычным «детектором лжи»: прибор сравнивает, как меняются реакции человека в состоянии эмоционального напряжения. Вместо датчиков, выводящих данные на комплекс психофизиологических исследований, требуется лишь видеокамера и ноутбук с криптоключом, который помогает запустить программу.

Программы отслеживают значительное количество ключевых точек на лице и грудной клетке: движение бровей, точки носа и глаз, мимических мышц на лице – вокруг рта, на лбу, под глазами, которые работают почти бесконтрольно, то есть программы работают с данными, недоступными невооруженному глазу. Затем они считывают информацию, обрабатывают ее и выдает прогноз: с какой достоверностью испытуемый в данный момент лжет или говорит правду [4].

Для того чтобы собрать необходимое количество данных, требуется минимум двадцать секунд беседы с человеком по каждому отдельному вопросу. При этом испытуемый может не подозревать о проверке, если используется обычная веб-камера, установленная на расстоянии одного метра и не привлекающая внимания.

Как один из вариантов дальнейшего развития подобного оборудования является использование таких особенностей человеческого организма, как повышенное потоотделение при неправдивых ответах на вопросы у опрашиваемого лица. Новейшие разработки предполагают сканирование потовыводящих каналов с помощью субтерагерцового излучения.

В заключение следует отметить, что эффективность и практичность данных технических средств в рамках осуществления оперативно-разыскной деятельности будет определена только в процессе практического применения беспроводных устройств.

Наиболее целесообразно было бы внедрение и использование такого рода приборов в территориальных подразделениях МВД России на районном уровне, так как для их применения не требуется добровольное согласие испытуемого лица на прохождение теста, и оперативно-разыскное мероприятие «опрос» проходит дистанционно в негласной форме.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анищенко Л.Н., Турецкая А.В. Программно-аппаратный комплекс для бесконтактной оценки психофизиологического состояния человека // Биомедицинская радиоэлектроника. – 2018. – № 10. – С. 61–67.

2. Мадянов А.В., Васильева Н.Ю., Болховитина С.Н. Использование методов профайлинга и верификации в ходе предварительного расследования // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3. – Ч. 2. – С. 329–333.

3. Молчанов А.Ю. Альтернативность и релевантность контрольного вопроса. – Москва: Центр прогрессивных технологий детекции лжи, 2019.

4. Свободный Ф.К. Практика применения полиграфа в процессе расследования преступлений: мнения работников следственных подразделений // Психопедагогика в правоохранительных органах. – 2020. – № 3. (82). – С. 279–285.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЕДИНОЙ СИСТЕМЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ МВД РОССИИ

Чиненов А.В.,
кандидат юридических наук;
Рзгоян К.Т.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: системы электронного документооборота в последние годы прочно вошли в нашу жизнь. В процессе внедрения систем электронного документооборота возникает ряд существенных проблем. Одной из основных проблем является обеспечение информационной безопасности при использовании электронных документов. Необходимо отметить принятие в декабре 2016 года новой Доктрины информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 [1]. Одним из национальных интересов в информационной сфере Доктрина назвала обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры. Поскольку общегосударственные и министерские системы электронного документооборота относятся к информационной инфраструктуре, то вопросы обеспечения их функционирования приобретают особую важность. В этой связи представляется актуальным исследование правовых аспектов обеспечения безопасности информации при организации электронного документооборота в МВД России.

Ключевые слова: безопасность, защита информации, информационно-аналитическое обеспечение.

ENSURING INFORMATION SECURITY IN THE UNIFIED SYSTEM OF INFORMATION AND ANALYTICAL SUPPORT FOR THE ACTIVITIES OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Chinenov A.V.,
Candidate of Law;
Rzgoyan K.T.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: electronic document management systems have become firmly established in our lives in recent years. In the process of implementing electronic document management systems (EDMS), a number of significant problems arise. One of the main problems is ensuring information security when using electronic documents. It is necessary to note the adoption in December 2016 of the new Information Security Doctrine approved by Presidential Decree № 646 dated 05.12.2016. One of the national interests in the information sphere, the Doctrine called ensuring the sustainable and uninterrupted functioning of the information infrastructure. Since the national and ministerial electronic document management systems relate to the information infrastructure, the issues of ensuring their functioning are of particular importance. In this regard, it seems relevant to study the legal aspects of information security in the organization of electronic document management in the Ministry of Internal Affairs of Russia.

Keywords: security, information protection, information and analytical support.

Правовое регулирование информационной безопасности в интегрированной среде обеспечения деятельности (далее – ИСОД) МВД России осуществляется в основном секретными приказами МВД России. Поэтому в рамках данной статьи некоторые вопросы информационной безопасности не могут быть рассмотрены.

Создаваемая с 2011 года в министерстве единая система информационно-аналитического обеспечения деятельности МВД России построена по принципам облачных технологий и использует единую технологическую платформу. Информационная поддержка оперативно-служебной деятельности сотрудников органо внутренних дел осуществляется в режиме клиент – сервер. Это означает, что каждый сотрудник осуществляет самостоятельный вход в ИСОД МВД России и вне зависимости от того, где этот вход осуществлен, сотруднику доступны определенные возможности.

В ходе построения ИСОД МВД России было принято решение об объединении различных сервисов в одну систему, в том числе системы электронного документооборота. Информационная безопасность обеспечивается не каждому сервису отдельно, а для всей системы в целом. Для обеспечения безопасности информации создана подсистема обеспечения информационной безопасности (далее – ПОИБ).

ПОИБ предназначена для решения задач обеспечения информационной безопасности как внутри ИСОД, так и при взаимодействии с внешними системами

других органов государственной власти. Единая техническая политика по обеспечению информационной безопасности в Системе проводилась с учетом моделей угроз и нарушителей, согласованных с ФСБ России и ФСТЭК России [2].

К компонентам подсистемы информационной безопасности относятся антивирусная защита, анализ защищенности, обнаружение вторжений, защита информации от несанкционированного доступа, криптографическая защита информации, управление событиями информационной безопасности и обеспечение информационной безопасности демилитаризованной зоны. Под демилитаризованной зоной ИСОД МВД России понимается пограничный сегмент, выполняющий функции разделения внешней сети (сети Интернет) и внутренней (ИМТС) при использовании общедоступных сервисов ИСОД.

В 2016 году началась реализация комплекса поэтапных мер импортозамещения оборудования ИСОД и перевода ведомственной информационно-телекоммуникационной платформы на отечественные средства вычислительной техники:

– серверы – на базе процессора «Эльбрус»;

– терминальные станции – на базе процессора «Байкал»;

– операционные системы «Эльбрус», «Циркон», «Астра Линукс».

Подсистема обеспечения информационной безопасности ИСОД МВД России включает в себя:

1. Сервис управления доступом к информационным системам и ресурсам ИСОД МВД России (СУДИС). Сервис обеспечивает: управление доступом пользователей в систему, управление доступом пользователей к сервисам ИСОД, управление доступом сервисов ИСОД к другим сервисам ИСОД, единую точку входа в сервисы ИСОД.

2. Антивирус «Касперский» обеспечивает защиту от вредоносного программного обеспечения и защиту от почтового спама. Комплекс мероприятий, направленных на противодействие DDOS-атакам, приводящих к отказу в обслуживании, например, интернет-портала и других публичных ресурсов МВД России обеспечивается средствами «Лаборатории Касперского».

3. ViPNet Client обеспечивает защиту информации при ее передаче по каналам связи и защиту от сетевых атак на уровне АРМ. ViPNet Client позволяет обмениваться информацией по открытым каналам связи с использованием шифрования.

ViPNet Client – это специализированный программный комплекс криптографической защиты (СКЗИ) для стационарных и мобильных АРМ, сертифицированный в ФСБ России.

4. КриптоПРО позволяет осуществлять идентификацию пользователей по электронной подписи (доступ в систему, доступ к сервисам ИСОД МВД России) и производить подписание электронных документов в Сервисе электронного документооборота.

Для обеспечения информационной безопасности в МВД России в целом и при использовании систем электронного документооборота, в частности, были созданы подразделения информационных технологий, связи и защиты информации.

На уровне министерства создан Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации (ДИТСиЗИ МВД России), который выполняет функции головного подразделения Министерства в области: совершенствование информационных и телекоммуникационных технологий, разработка и развитие автоматизированных информационных систем, систем и средств связи, противодействия техническим разведкам, технической защиты информации, радиоэлектронной борьбы, использование электронной подписи, межведомственного информационного взаимодействия [3].

Кроме того, обеспечением безопасности информации в МВД России занимается Главный центр связи и защиты информации МВД России, который является главным администратором компьютерной сети Министерства и Удостоверяющим центром МВД России (выдает сотрудникам квалифицированные электронные подписи – ruToken).

Разработкой программного обеспечения ИСОД МВД России занимается научно-производственное объединение «Специальная техника и связь», которое обеспечивает функционирование Центра разработки, поддержки, внедрения и администрирования компонентов ИСОД МВД России.

Таким образом, следует отметить, что МВД России в соответствии с обоими группами правовых актов является обладателем информации и оператором информационной системы. Поскольку системы электронного документооборота МВД России содержат персональные данные, то на них распространяются требования обеспечения безопасности персональных данных.

Как законодательство, так и нормативные правовые акты МВД России требуют обеспечения конфиденциальности информации, защиты ее от несанкционированного доступа, невозможность полного уничтожения информационных ресурсов и их быстрое восстановление после внешнего вмешательства.

Механизм обеспечения информационной безопасности в ИСОД состоит из пяти составляющих: сервиса управления доступом к информационным системам и ресурсам ИСОД МВД России, антивируса «Касперский», специализированного программного комплекса криптографической защиты ViPNet Client, средств криптографической защиты информации КриптоПРО и электронных ключей, выдаваемых каждому сотруднику для доступа в систему.

Министерство самостоятельно обеспечивает безопасность информации в своих информационных системах, в том числе путем выдачи электронных ключей квалифицированной электронной подписи. В настоящий момент продолжается подключение подразделений министерства к Всероссийской системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – № 50. – Ст. 7074.

2. Приказ МВД России от 15.06.2021 № 444 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» (ред. от 16.11.2022) [Электронный ресурс] // СПС «КонсультантПлюс».

3. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2011. – № 16.

4. Моисеев Н.А., Новоселов Н.Г., Серегин М.В., Чиненов А.В. Современная информационная среда как объект оперативно-разыскной деятельности // Евразийский юридический журнал. – 2018. – № 6 (121). – С. 316–318.

РОЛЬ СТАТИСТИЧЕСКИХ ДАННЫХ В ПРОГНОЗИРОВАНИИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Ярош Д.А.,
Емельянова О.В.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: история свидетельствует, что без статистических данных невозможны управление государством как социальным органом, разработка программ социально-экономического развития, в том числе и в области социально-правового контроля над правонарушениями. Особое значение статистический анализ и прогнозирование правонарушений приобрело в настоящее время в связи со снятием ограничений на публикацию данных правовой статистики. Это открывает новые возможности для статистиков в объективном анализе и прогнозировании правонарушений и играет важную роль в государственной деятельности, связанной с применением юридических мер воздействия, предупреждения и профилактики правонарушений.

Ключевые слова: информация, статистические данные, статистика, полиция, преступления, преступник, динамика преступлений.

THE ROLE OF STATISTICS IN PREDICTING CRIMINAL ACTIVITY

Yarosh D.A.,
Emelyanova O.V.
(Kikot Moscow University the Ministry of Internal Affairs of Russia)

Abstract: history shows that without statistical data it is impossible to manage the state as a social body, to develop programs for socio-economic development, including in the field of social and legal control over crime. Statistical analysis and forecasting of offenses has now acquired particular importance in connection with the

lifting of restrictions on the publication of legal statistics. This opens up new opportunities for statisticians in the objective analysis and forecasting of offenses and plays an important role in government activities related to the application of legal measures to influence, prevent and prevent offenses.

Keywords: information, statistical data, statistics, police, crimes, criminal, crime dynamics.

Вокруг нас за день происходит множество событий, встреч, разговоров, мы ведем рабочие переписки, тратим время на просмотр различных видео и фото, то есть можно сказать получаем информацию в различных видах и формах. Также получая определенный спектр информации, мы можем делиться ею со своими близкими, друзьями, знакомыми, различными службами, органами государственной власти и местного самоуправления и другими субъектами нашей жизни.

Каждый человек понимает и анализирует информацию по-своему. Кому-то удобно воспринимать информацию слушая другого человека, ведя диалог, они могут рассматривать проблему с различных сторон. Также люди могу получать информацию читая книги, электронные научные статьи. Интересуясь определенной информацией, люди развиваются ипонимают точнее для себя ту или иную проблему общества. При получении информации человек проводит тщательный ее анализ, чаще всего это происходит автоматически, с помощью когнитивных функций мозга, которые помогают понять и осмыслить ее. Благодаря данной функции головного мозга люди развиваются и расширяют свое мировоззрение, а также могут строить теории, прогнозировать социальные проблемы, выстраивать причинно-следственную связь [5]. Решение данных проблем и задач является важным вызовом для любой страны, ведь при их решении нужно задействовать большое количество людей. Но не каждый гражданин может понимать и анализировать объем той или иной проблемы и для этого государство чаще всего использует статистические данные, для более полного и точного рассмотрения проблемы.

Из-за особенностей своих деталей следует обратить особое внимание на три основных типа представления статистической информации [3]. Это представляет особую важность для обеспечения удобного доступа к данным статистики для всех заинтересованных лиц.

1. Текстовая.
2. Табличная.
3. Графическая.

Текстовая форма применяется при малом количестве цифровых данных.

Статистическая презентация данных в виде числовой насыщенности описания изучаемых явлений, представленная в таблицах, приобрела широкое распространение за счет высокой информативности. Этот подход стал эффективной альтернативой математическим таблицам, которые применяются для анализа предоставленной информации.

Данные о социально-экономических явлениях представлены в табличной форме с разделением на строки и колонки, что обеспечивает структурированное и

организованное изложение информации. Такой статистический формат позволяет лучше понять зависимости между данными и ясно интерпретировать их.

Работа сотрудников полиции включает в себя охрану общественного порядка, предупреждение и пресечение преступлений, защиту прав собственности граждан и все, что способствует общественному благополучию. Эти задачи подразумевают обеспечение безопасности жизни, здоровья, свободы и законных интересов как граждан России, так и иностранных граждан, лиц без гражданства. Можно сказать, что работа полиции состоит в обработке большого количества информации о преступлениях, административных правонарушениях и происшествиях. То есть полиция играет важную роль в сборе информации, но для чего именно она это делает? Наша страна, Россия, очень широка и просторна, по этому очень сложно следить за ее безопасностью без статистических данных. В России на данный момент восемьдесят девять субъектов, и в каждом из них полиция ведет учет преступлений и преступников, а также разграничивает их по степени тяжести на особо тяжкие, тяжкие, средние и легкие. Представляя статистику по зарегистрированным и выявленным преступлениям, Министерство внутренних дел Российской Федерации показывает свою эффективность и полезность обществу. А также может отражать социальные проблемы и неравенства, помогая государству обратить внимание на данные проблемы и незамедлительно приступить к их решению.

Далее посмотрим на практике, как полиция работает с графической формой статистических данных (см. рис. 1) [1].

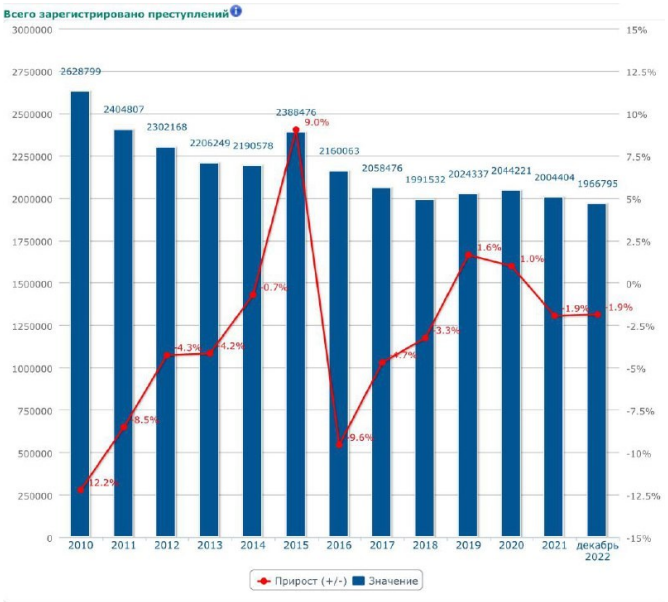


Рисунок 1. Всего зарегистрировано преступлений

На данном графике представлена динамика зарегистрированных преступлений. Анализируя данную диаграмму, можно увидеть, что динамика зарегистрированных преступлений постоянно то возрастает, то убывает. Давайте разберемся почему такое может быть. Анализируя статистические данные, представляемые МВД России, помогают определить социальное, экономическое со-

стояние страны. Предыдущие кризисы, как правило, сопровождались колебаниями в валовом внутреннем продукте (далее – ВВП).

В 2015 году в России произошел экономический спад на фоне накопленной нестабильности. Например, ВВП в 1997 году увеличился на 1,4% после пятилетнего спада с 1992 по 1996 год, когда он снижался на 9,4%. В период с 2012 по 2014 год экономика также демонстрировала негативную динамику, но с некоторым ростом, спровоцированным государственными расходами, налогообложением и действиями силовых структур. Рост ВВП составил 3,4% в 2012 году, затем снизился до 1,3% в 2013 году и далее до 0,6% в 2014 году, указывая на то, что кризис в этот раз был более длительным. В 2008 году ВВП России рос на 7,5% каждый год в течение пяти лет. В тот период инвестиционный климат был на пике дважды: в октябре 1997 года индекс РТС достиг 571.6 пункта, который вернулся к этим значениям только в сентябре 2003 года, и в мае 2008 года, достиг максимума в 2 498 пунктов, недостижимого в ближайшем будущем. Ранее происходившие нестабильные события также имели внешние причины. Кризис в азиатских странах в августе 1997 года сказался на России. Связь между внутренними проблемами и глобальными финансовыми потрясениями стала очевидной в 2008 году.

Сегодняшнее состояние развитых стран характеризуется ростом фондовых индексов и обсуждением повышения процентных ставок финансовыми институтами, что является предвестником новых экономических вызовов, которые могут возникнуть к 2017–2019 годам и помешать мировому экономическому восстановлению России, если ожидаемые изменения начнут происходить в течение будущих 3–4 лет. Поэтому 2015 год стал кризисом с причинами, явно определенными национальными [4].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Количество преступлений, зарегистрированных в отчетном периоде [Электронный ресурс]. – URL: https://www.fedstat.ru/indicator/36224 (дата обращения: 20.04.2024).

2. Официальная статистика [Электронный ресурс]. – URL: https://rosstat.gov.ru/folder/10705 (дата обращения: 20.04.2024).

3. Тепляшин П.В., Молоков В.В. Структура преступности в Российской Федерации: статистический анализ и криминологическая характеристика // Алтайский юридический вестник. – 2023. – № 1 (41). – С. 89–97.

4. Федотов А.А. Социальное неравенство и уровень преступности: межрегиональный анализ // Экономика и бизнес: теория и практика. – 2019. – № 9. – С. 208–211.

5. Жукова П.Н., Дрога А.А. Статистические приемы и методы исследования и прогнозирования в рамках преподавания дисциплины «Правовая статистика»: электронные методические рекомендации. – Белгород, 2022.

6. Чернышов В.В., Абовян Э.П. Факторный анализ экономической преступности в России // Евразийский юридический журнал. – 2022. – № 9 (172). – С. 296–299.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ГЕОЛОГИЧЕСКОЙ ИНФОРМАЦИИ

Савотченко С.Е.,
доктор физико-математических наук, доцент
(Российский государственный геологоразведочный университета имени Серго Орджоникидзе),
(Московский технический университет связи и информатики);
Захаров В.А.,
аспирант
(Российский государственный геологоразведочный университета имени Серго Орджоникидзе);
Акапьев В.Л.,
кандидат педагогических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье раскрывается понятие географической информации и предлагается оригинальная система классификации данного вида информации на общедоступную и конфиденциальную. Проводится анализ нормативно-правовой базы, регулирующей оборот геологической информации.

Ключевые слова: географическая информация, конфиденциальная геологическая информация, общедоступная геологическая информация, недропользователи.

LEGAL REGULATION OF THE PROTECTION OF CONFIDENTIAL GEOLOGICAL INFORMATION

Savotchenko S.E.,
Doctor of Physical and Mathematical Sciences, Associate Professor
(Sergo Ordzhonikidze Russian State University for Geologicfl Prospecting named after),
(Moscow Technical University of Communications and Informatics);
Zaharov V.A.,
graduate student
(Sergo Ordzhonikidze Russian State University for Geologicfl Prospecting named after);
Akapyev V.L.,
Candidate of Pedagogical Sciences;
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article reveals the concept of geographical information and proposes an original system for classifying this type of information into publicly available and confidential. The analysis of the regulatory framework governing the turnover of geological information is carried out.

Keywords: geographical information, confidential geological information, publicly available geological information, subsurface users.

Закон Российской Федерации «О недрах» является нормативным правовым актом, регулирующим вопросы защиты геологической информации. В соответствии с данным законом, геологическая информация представляет собой совокупность сведений о геологическом строении недр, процессах, происходящих в них, местонахождении и состоянии полезных ископаемых, других свойствах недр. Данная информация классифицируется на общедоступную и конфиденциальную.

Общедоступная геологическая информация – это сведения, которые могут быть получены любыми заинтересованными лицами в установленном порядке. К такой информации относятся, в частности, данные государственного кадастра месторождений и проявлений полезных ископаемых, а также сведения из государственного баланса запасов полезных ископаемых.

Конфиденциальная геологическая информация -– это сведения, доступ к которым ограничен в интересах обеспечения национальной безопасности, охраны коммерческой тайны недропользователей, а также в иных предусмотренных законодательством случаях. Данная информация является государственной собственностью и подлежит обязательному учету, хранению и использованию.

Согласно Закону Российской Федерации «О недрах», геологическая информация, полученная в процессе геологического изучения недр, находится в государственной собственности. Это означает, что государство осуществляет права владения, пользования и распоряжения такой информацией. Недропользователи, проводящие геологоразведочные работы, обязаны предоставлять полученные результаты в государственный фонд геологической информации.

Порядок учета, хранения и использования геологической информации регламентируется положениями Закона Российской Федерации «О недрах» и иными нормативными правовыми актами. Так, все сведения о недрах подлежат государственному учету и ведению в специальном государственном реестре. Доступ к конфиденциальной геологической информации имеет ограниченный круг лиц, определяемый уполномоченными органами. Использование такой информации возможно только в рамках и в порядке, установленном законодательством.

Федеральный закон «Об информации, информационных технологиях и о защите информации» является одним из основополагающих нормативно-правовых актов, регламентирующих вопросы защиты конфиденциальной информации, в том числе и в сфере недропользования.

Закон устанавливает ряд требований к обеспечению защиты конфиденциальной информации. Лица, получившие доступ к конфиденциальной информации, обязаны не раскрывать третьим лицам и не распространять данную информацию без согласия ее обладателя. Обладатель конфиденциальной инфор-

мации должен принимать правовые, организационные и технические меры для ее защиты.

Ответственность за нарушение режима конфиденциальности информации предусмотрена как гражданским, так и уголовным законодательством. Так, согласно Гражданскому кодексу Российской Федерации, лица, незаконно использующие конфиденциальную информацию, обязаны возместить причиненные убытки. Уголовный кодекс Российской Федерации устанавливает ответственность за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Приказ Минприроды России «Об утверждении Порядка представления геологической информации о недрах заинтересованным лицам» является важным нормативным актом, регулирующим вопросы доступа к геологической информации, в том числе конфиденциального характера.

Согласно данному Порядку, доступ к геологической информации о недрах предоставляется заинтересованным лицам на основании их письменных заявлений. При этом устанавливаются определенные условия и процедура предоставления доступа. В частности, Порядок предусматривает, что доступ к геологической информации предоставляется в зависимости от ее отнесения к общедоступной или конфиденциальной. Общедоступная информация предоставляется любым заинтересованным лицам, в то время как доступ к конфиденциальной информации ограничен.

Для получения доступа к конфиденциальной геологической информации заявитель должен обосновать необходимость ее получения и подтвердить наличие соответствующих полномочий. Уполномоченный орган рассматривает заявление и при наличии оснований принимает решение о предоставлении доступа к запрашиваемой информации.

Приказом также определен перечень сведений, относящихся к конфиденциальной геологической информации. К ним относятся:

- материалы геологоразведочных работ, содержащие сведения о местонахождении, качестве и количестве запасов полезных ископаемых;
- данные о результатах поисковых, оценочных и разведочных работ на участках недр;
- сведения о технологиях и методах геологического изучения недр, обеспечивающих получение конкурентных преимуществ при проведении геологоразведочных работ;
- прогнозные оценки перспектив нефтегазоносности и рудоносности недр.

Правовой режим конфиденциальной геологической информации в Российской Федерации предусматривает определенные критерии, которым должна соответствовать информация, чтобы быть отнесенной к категории конфиденциальной.

Основными критериями отнесения геологической информации к конфиденциальной являются:

1. Наличие коммерческой ценности информации для правообладателя. Конфиденциальная геологическая информация обладает определенной коммерческой ценностью для предприятий, осуществляющих геологическое изучение недр, разведку и разработку месторождений полезных ископаемых. Данная ин-

формация может содержать сведения о запасах, ресурсах, качественных характеристиках полезных ископаемых, технологиях и методиках геологоразведки, что представляет собой ценный актив для компаний-недропользователей. Утрата контроля над такой информацией может повлечь для правообладателя значительные экономические потери.

2. Информация должна быть ограничена в доступе и не являться общедоступной. Доступ к конфиденциальной геологической информации, как правило, имеет ограниченный круг лиц – сотрудники организаций-правообладателей, государственные органы, осуществляющие контроль и регулирование недропользования, и иные лица, имеющие соответствующие полномочия и разрешения.

3. Правообладатель конфиденциальной геологической информации должен предпринимать меры по ограничению доступа к ней, ее учету и контролю за использованием.

Стоит отметить, что данные критерии закреплены в Федеральном законе «О коммерческой тайне» и имеют общий характер для любой конфиденциальной информации, в том числе и геологической. Вместе с тем, Закон Российской Федерации «О недрах» и иные подзаконные акты содержат дополнительные или уточняющие требования к отнесению той или иной геологической информации к категории конфиденциальной. Так, Постановление Правительства Российской Федерации от 11.02.2005 № 69 детализирует виды сведений, которые относятся к конфиденциальной геологической информации, в том числе - информация о количестве, качестве и способах разработки запасов полезных ископаемых, технико-экономических параметрах месторождений, геологическом строении участков недр и т.д.

Виды конфиденциальной геологической информации:

1. Технико-экономические показатели разработки месторождений полезных ископаемых К этой категории относятся сведения, содержащиеся в технико-экономических обоснованиях (проектах) кондиций для подсчета запасов полезных ископаемых, проектах разработки месторождений, а также других технико-экономических и проектных документах.

2. Информация о запасах и ресурсах полезных ископаемых. К конфиденциальной информации относятся сведения о количестве, качестве и геологических особенностях разведанных запасов полезных ископаемых на месторождениях.

3. Сведения о методиках и технологиях геологического изучения недр. К конфиденциальной информации отнесены данные о применяемых методиках и технологиях проведения геологоразведочных работ, включая поисковые, оценочные и разведочные работы.

4. Информация о результатах геологоразведочных работ

К конфиденциальной геологической информации относятся сведения, содержащиеся в материалах геологического изучения недр. Это могут быть данные о геологическом строении участков недр, результатах поисковых, оценочных и разведочных работ, а также иные сведения, полученные в ходе геологоразведки.

Помимо указанных, к конфиденциальной геологической информации могут быть отнесены и иные виды сведений, доступ к которым ограничен в соответствии с законодательством. Например, это могут быть данные о запасах и

качестве попутных полезных ископаемых, информация об экологических параметрах месторождений, сведения о новых технологических решениях в сфере разведки и разработки месторождений.

Важно отметить, что законодательство Российской Федерации устанавливает определенные исключения из режима конфиденциальности геологической информации. Так, Закон Российской Федерации «О недрах» предусматривает, что сведения, необходимые для государственного регулирования отношений недропользования, не могут быть отнесены к конфиденциальной информации.

Режим доступа к конфиденциальной геологической информации в Российской Федерации предусматривает ряд ограничений и специальный порядок предоставления доступа к данной информации. Кроме того, законодательство закрепляет права и обязанности владельцев и пользователей конфиденциальной геологической информации.

Таким образом, анализ нормативно-правовой базы, регулирующей оборот геологической информации, показал, что в Российской Федерации сформирована развитая законодательная основа, определяющая правовой режим данного вида информации, порядок ее использования, хранения и защиты. Вместе с тем, востребованность геологической информации в различных сферах и необходимость ее эффективного использования требуют постоянного совершенствования мер по обеспечению конфиденциальности и безопасности. Результаты исследования могут быть использованы для совершенствования нормативно-правого регулирования защиты конфиденциальной геологической информации с учетом современных реалий глобализации с одной стороны, и недружественного отношения ряда зарубежных стран с другой, с целью повышения эффективности обеспечения информационной безопасности в сфере недропользования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Агафонов В.Б. Право собственности на геологическую информацию: дис. ... канд. юрид. наук. – Москва, 2003. – 196 с.

2. Василевская Д.В. Административно-правовой режим недропользования в Российской Федерации: проблемы теории и практики: дис. ... канд. юрид. наук. – Москва, 2015. – 211 с.

3. Салиева Р.Н. Документированная геологическая информация: гражданско-правовой аспект получения и использования: дис. ... канд. юрид. наук. – Москва, 2004. – 175 с.

4. Закон Российской Федерации от 21.02.1992 № 2395-1 «О недрах» (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс».

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с изм. и доп., вступ. в силу с 01.03.2022) // СПС «КонсультантПлюс».

6. Постановление Правительства Российской Федерации от 11.02.2005 № 69 «О государственной геологической информации» (с изм. и доп.) // СПС «КонсультантПлюс».

СОДЕРЖАНИЕ

НАУЧНОЕ ИЗДАНИЕ

Проблемы информационного обеспечения деятельности правоохранительных органов

Сборник статей 11-й Международной научно-практической конференции
24 мая 2024 года

Редактор ***М.К. Козырева***
Комп. верстка ***И.Ю. Чернышева***

Подписано в печать 2024 г., Формат 60х90/16
Усл. печ. л. 15. Тираж 27 экз. Заказ 64

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-583-9