МВД России
Санкт-Петербургский университет

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Материалы
международной научно-практической конференции

11–12 мая 2023 года

Санкт-Петербург
2023

План-график 2023, поз. 102
План НД 2023, п. 6 раздел IV

УДК 681.322
ББК 32.972.53
Б40

Б40 **Безопасность информационных технологий в правоохранительной сфере** [Электронный ресурс]: 11–12 мая 2023 г., Санкт-Петербург: материалы международной научно-практической конференции / сост.: Подружкина Т. А. – Электрон. дан. (1,62 Мб). – Санкт-Петербург: СПбУ МВД России, 2023. – 1 электрон. опт. диск. – Систем. требования: ПК с процессором Intel Core i3 и более; 512 Mb и более; CD/DVD – ROM дисковод; Microsoft Windows XP и выше; SVGA 800×600.16 bit и более; Internet Explorer; Adobe Acrobat Reader 8.0 и выше.

ISBN 978-5-91837-812-0
EDN: VBZZQD

В сборник включены статьи, отражающие содержание докладов и выступлений участников международной научно-практической конференции «Безопасность информационных технологий в правоохранительной сфере», состоявшейся в мае 2023 года в Санкт-Петербургском университете МВД России.

Все материалы публикуются в авторской редакции.

Издание представляет интерес для широкого круга исследователей в различных сферах науки, а также для практических работников правоохранительных органов.

УДК 681.322
ББК 32.972.53

Редакционная коллегия:
Подружкина Т. А.,
кандидат педагогических наук, доцент;
Гончар А. А.,
кандидат военных наук;
Лаур А. В.;
Молодых В. А.,
кандидат экономических наук, доцент;
Максимова Е. В.

© Санкт-Петербургский университет МВД России, 2023
© Коллектив авторов, 2023

ISBN 978-5-91837-812-0

СОДЕРЖАНИЕ

АНТОНОВА ЕКАТЕРИНА АЛЕКСАНДРОВНА

адъюнкт адъюнктуры
Санкт-Петербургский университет МВД России

ИСПОЛЬЗОВАНИЕ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В работе автор подчеркивает, что при раскрытии и расследовании преступлений важное значение отводится сбору и сохранению доказательственной информации с помощью научно-технических средств. Грамотное использование технико-криминалистических средств способствует эффективной работе правоохранительных органов.

Ключевые слова: криминалистическая техника, технико-криминалистические средства, информационная безопасность

Многие аспекты нашей деятельности сегодня переместились в цифровое пространство: мы общаемся с друзьями с использованием видеосвязи, совершаем покупки через приложения в смартфоне, для оформления жизненно необходимых документов обращаемся через сеть Интернет в те или иные организации, исполняем документы по своему виду деятельности с использованием компьютерной техники и так далее. В современном мире при всех жизненных ситуациях нас сопровождает интернет-пространство.

Государственные службы, коммерческие структуры собирают различные базы данных о нашей жизни, одних интересуют факты рождения, обучения, работы, других что покупает, куда ходит, как проводит досуг. Используя эти данные государственные структуры, могут планировать развитие различных сфер жизни нашего общества, коммерческие структуры анализировать спрос и предложение.

Совершая действия в цифровом пространстве, мы постоянно сталкиваемся с необходимостью использовать те или иные данные, которые могут быть, даже по истечении длительного срока, с нами идентифицированы, а затем и использованы.

В 1948 году появление новой науки «кибернетика» привело и к новому пониманию понятия «информация». Норберт Винер определил, что «информация — это не энергия и не материя, а обозначение содержания, полученного от внешнего мира в процессе приспособления к нему» [2]. Позднее информация начинает рассматривается как товар, кто владеет ей, тот имеет преимущество перед другими, а в мире материального, информация — равносильна прибыли.

С развитием информационных технологий, преступлений, совершенных в цифровой среде, становится все больше, о чем свидетельствуют статистические данные: «Сохраняется тенденция к увеличению количества на 28,7 % противоправных деяний в сфере информационно-телекоммуникационных технологий.

Их удельный вес в числе всех преступных посягательств возрос до 32,9 %, а по тяжким и особо тяжким — до 56,4 %. Больше совершено дистанционных мошенничеств и краж. Раскрываемость преступлений, совершенных в цифровом пространстве, составила 29,9 %, в том числе совершенных с использованием сети Интернет — 28,8 %, расчетных (пластиковых) карт — 35,7 %»[1].

«Основными тенденциями развития компьютерной преступности в последние годы является динамика ее постоянного роста, увеличение в ее структуре преступлений корыстной направленности (краж, мошенничеств и др.). При этом жертвами компьютерных преступлений все чаще становятся не обычные граждане, а банки, финансово-кредитные организации, крупные компании и корпорации, т. к. преступники используют возможность получить больший преступный доход при тех же ресурсно-временных затратах» [3].

Многие ученые считают, что политика государства, направленная на обеспечение прав и защиту интересов различных сфер деятельности общества, может обеспечить информационную безопасность граждан и страны в целом.

В этом направлении не маловажными аспектами могут быть как «...соблюдение условий всех видов информационной безопасности, разработка эффективных методов противодействия компьютерным и технологическим преступлениям» [4], так и разработка методик выявления и доказывания совершенных преступлений в области цифровых технологий, а также разработка технико-криминалистических средств для обеспечения информационной безопасности.

Так как преступления данной направленности совершаются с использованием технических средств, имеющих доступ к сети Интернет, то при производстве следственных действий: осмотрах, обысках, выемках обязательно изъятие мобильных средств коммуникации. С целью обнаружения электронных носителей информации, SIM-карт, записывающих устройств и прочих аналогичных объектов, целесообразно применять нелинейные локаторы серий: «Лорнет», *Orion*, «Люкс», *NR, BWS WH* или профессиональные детекторы нелинейных переходов *NR900EM* и др. [1].

Нельзя не отметить и важность сохранения информации, содержащейся на изъятых носителях, для этого хорошо подходит специальный чехол «Мешок Фарадея», который позволяет блокировать их функциональные свойства и не дает преступникам удаленно воздействовать на устройство.

Вся работа на месте преступления по обнаружению следов и объектов преступления направлена на получение информации, которая должна помочь как можно быстрей определить круг лиц совершивших преступление.

Развитие технико-криминалистических средств для обеспечения информационной безопасности правоохранительной деятельности

[1] Краткая характеристика состояния преступности в Российской Федерации за январь–август 2023 года // Министерство внутренних дел Российской Федерации.[Сайт]. URL: https://xn--b1aew.xn--p1ai/reports/item/41741442/ (дата обращения: 13.02.2024).

имеет свое собственное направление развития, способствующее расследованию противоправных деяний. Основной задачей на сегодняшний день при разработках технико-криминалистических средств становится их современность, мобильность, малая энергоемкость, простота в использовании и при всем при этом возможность обработки значительных объемов данных. Не только совершенствования технико-криминалистических средств обеспечения расследования информационных преступлений должно совершенствоваться, но и правового регулирования применения этих средств.

© Антонова Е. А., 2023

Библиографический список:

1. Багмет А. М.. Актуальные вопросы применения криминалистической техники для получения информации, содержащейся в мобильных электронных устройствах. // Вестник криминалистики. – 2013. – № 4. – С. 9–14.

2. Винер Н. Кибернетика и общество. – Москва, 1968. – С. 201.

3 Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: специальность 12.00.08: автореф. дис. … канд. юрид. наук /Евдокимов, Константин Николаевич. – Москва, 2022. – С. 25.

4. Манжуева О. М. Феномен информационной безопасности: сущность и особенности: специальность 09.00.01: автореф. дис. … д-ра филос. наук / Манжуева Оксана Михайловна. – Улан-Уде, 2015. – 383 с.

5. Грибунов О. П. Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института Министерства внутренних дел России. – 2017. – № 4 (83). – С. 137–142.

АРЧУКОВА АННА АЛЕКСЕЕВНА

адъюнкт адъюнктуры
Санкт-Петербургский университет МВД России

ИСПОЛЬЗОВАНИЕ ФУНКЦИОНАЛЬНЫХ ПРИЗНАКОВ ВНЕШНОСТИ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация. В данной статье рассматриваются способы, перспективные возможности и новые направления, использования информации о функциональных признаках внешности человека правоохранительными органами в процессе раскрытия и расследования преступлений.

Ключевые слова: криминалистическая идентификация, функциональные признаки внешности человека, внешний облик человека, искусственный интеллект

В настоящее время в связи с развитием технических средств, различных аппаратно-программных комплексов, распространение получает криминалистическая идентификация личности с помощью компьютерных технологий.

Данные технологии совершенствуют процесс исследования и помогают выполнять задачи, связанные с раскрытием и расследованием преступлений, с учетом достижений современной науки и техники. Ей, в частности, является система, в основе которой лежит сложный многоуровневый комплекс регистрации и учета параметров человека.

Известно, что человека индивидуализируют не только общефизические и анатомические признаки внешности, а также и функциональные особенности. Данные особенности проявляются в различных характеристиках движения и статики тела, таких как: походка, жестикуляция, мимика, осанка, привычки, умения и навыки, выработанные в процессе определённой деятельности и жизни человека. Данные элементы помимо общих признаков характеризуются индивидуальными особенностями каждого конкретного человека, которые и позволяют его идентифицировать, в том числе с помощью различных программных комплексов.

Идентификация человека по функциональным признакам внешности с помощью искусственного интеллекта является перспективным направлением, так как человек может изменить свою внешность с помощью различных средств (парик, очки, медицинская маска, балаклава) тогда идентификация по анатомическим признакам будет невозможна. А изменение функциональных признаков внешности на длительный период времени, например походки, является сложным в производстве процессом. Естественность поведения — обстоятельство, которое обусловливает невозможность фальсификации функциональных признаков внешности, поскольку они динамичны и индивидуальны.

Одной из проблем, требующей научного разрешения, является необходимость разработки концепции использования технологий искусственного интеллекта в деятельности

правоохранительных органов для проведения идентификации по функциональным признакам внешности.

Актуальность обусловлена Национальной стратегией развития искусственного интеллекта на период до 2030 года закрепленной Указом Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [1].

Согласно п. 5 Указа Президента «искусственный интеллект — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» [1].

При рассмотрении возможностей использования искусственного интеллекта для проведения идентификации и диагностики лиц, которые могут совершить преступление необходим определенный набор сведений для проведения данного исследования, который является совокупностью данных, прошедших предварительную подготовку (обработку) в соответствии с требованиями законодательства Российской Федерации об информации, информационных технологиях и о защите информации и необходимых для разработки программного обеспечения на основе искусственного интеллекта [1].

А. Ю. Гордеев отмечает, что увеличение эффективности габитоскопических исследований, к настоящему времени является наиболее перспективным направлением развития искусственных нейронных сетей, в ходе раскрытия и расследования [6, с. 128].

Необходимо определение правовых основ, целей, задач, принципов, механизмов реализации и основных направлений практического применения искусственного интеллекта в деятельности правоохранительных органов, а также в повышении эффективности идентификации человека по функциональным признакам внешности человека на основе использования данных технологий.

Использование аппаратно-программных комплексов в практике правоохранительных органов позволит оперативно решать идентификационные задачи в целях расследования, раскрытия и предупреждения преступлений, а также делает возможным отождествление без непосредственного контакта с интересующим правоохранительные органы человеком.

Из всего вышесказанного можно сделать вывод о том, что одним из наиболее сложных при производстве идентификации человека по функциональным признакам внешности человека и наиболее перспективным видится — использование различных автоматизированных комплексов. Так использование искусственного интеллекта, для проведения криминалистической идентификации по функциональным признакам внешности, может быть успешно использовано правоохранительными органами.

© Арчукова А. А., 2023

Библиографический список:

1. О развитии искусственного интеллекта в Российской Федерации: указ Президента Российской Федерации от 10 октября 2019 г. № 490 // Справочно-правовая система «Гарант». – URL: https://base.garant.ru/72838946 (дата обращения: 10.01.2024).

2. Булгаков В. Г. Возможности криминалистического исследования динамических признаков человека // Вестник криминалистики. – Москва: Спарк, 2006. – Вып. 1 (17).

3. Булгаков В. Г. Методология криминалистического исследования динамических признаков человека // Юристъ-Правоведъ. – 2011. – № 4 (47). – С. 13–16.

4. Писарев Д. Ю. Проблемы применения биометрических систем в расследовании преступлений: специальность 12.00.09: автореф. дис. … канд. юрид. наук / Писарев Дмитрий Юрьевич. – Краснодар, 2012. – 20 с.

5. Брюхомицкий Ю. А. Параметрические методы распознавания образов динамической биометрии // Известия ЮФУ. Технические науки. – 2011. – № 12(125). – С. 170-180. – EDN: OKIPGL.

6. Гордеев А. Ю. Перспективы развития и использования искусственного интеллекта и нейросетей для противодействия преступности в России (на основе зарубежного опыта) // Научный портал МВД России. – 2021. – № 1(53). – С. 123–135. – EDN: KNBLSY.

БАЙКОВ ВИКТОР МИХАЙЛОВИЧ

преподаватель кафедры криминалистических экспертиз и исследований
Санкт-Петербургский университет МВД России

ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ПРЕДУПРЕЖДЕНИЮ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Аннотация. В данной работе автор раскрывает, правовые вопросы взаимодействия общества и правоохранительных органов при работе по предупреждению правонарушений в цифровом пространстве, а так же вопросы подготовки сотрудников правоохранительных органов к работе с данным видом правонарушений.

Ключевые слова: информационно-цифровые технологии, правоохранительные органы, подготовка, информационная безопасность

Практически за последнее десятилетие наша жизнь изменилась коренным образом. Начало XXI века ознаменовалось бурным развитием информационно-цифровых технологий, которые изменили сущность и содержание общественных отношений, складывающихся между людьми, обществом и государством. У нас появилась возможность общаться на расстоянии, получать услуги не выходя из дома, оплачивать товары сидя за компьютером дома, врачи могут совершать сложные операции пациентам находясь в другом городе и список таких возможностей может быть довольно существенен. Вместе с тем, не смотря на все преимущества информационных технологий, так стремительно развивающихся за последнее время, существуют и риски совершения преступлений в этой среде, методы совершения которых, развиваются тоже, можно сказать, стремительно.

Проблема киберпреступности приобрела глобальный масштаб во всем современном мире, ущерб от деятельности хакеров достигает сотни миллиардов долларов, а незаконный финансовый оборот превышает триллионы долларов и такая ситуация продолжает прогрессировать. Информационная безопасность имеет огромное значение, как для отдельно взятого гражданина, так и для государственных структур, банковской и политической сферы, вооруженных сил, бизнеса, науке и медицине.

Данной проблеме уделяется огромное внимание со стороны государства. В своем выступлении на расширенном заседании коллегии МВД России по итогам работы ведомства за 2021 год. Президент Российской Федерации В. В. Путин, отмечал, что «В результате действий кибермошенников урон несут отечественные компании. С потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане во всё большем и большем количестве. Жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью»[1]. К сожалению ситуация

[1] Расширенное заседание коллегии МВД России по итогам работы ведомства за 2021 г. // МВД России [Сайт]. URL: http://www.kremlin.ru/events/president/transcripts/comminity_meetings/67795 (дата обращения: 13.05.2023).

не меняется в лучшую сторону, а рост преступлений, совершенных в цифровом поле только увеличивается. Так по данным МВД России за январь–август 2023 года «Сохраняется тенденция к увеличению количества — на 28,7 % — противоправных деяний в сфере информационно-телекоммуникационных технологий. Их удельный вес в числе всех преступных посягательств возрос до 32,9 %, а по тяжким и особо тяжким — до 56,4 %. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9 %, в том числе совершенных с использованием сети Интернет — 28,8 %, расчетных (пластиковых) карт — 35,7 %».[1]

В свою очередь данные Банка России за период с января по декабрь 2022 года свидетельствуют, что в этот период совершено 875 тыс. операций несанкционированного снятия денежных средств у клиентов на общую сумму 13 357, 77 млн руб. с использованием злоумышленниками 756 тыс. абонентских номеров с системой подмены номера и 5 217 интернет-сайтов, замаскированных под сервисы оказания различных услуг[2].

В этой связи государство предпринимает шаги по защите своих граждан и своего суверенитета.

«Эффективность защиты прав человека определяются достаточно универсальными критериями: прочностью конституционного правопорядка, защищенностью достоинства человеческой личности, гарантиями прав и свобод граждан, обеспечением социальной справедливости и солидарности»[1].

В настоящее время кроме социальной поддержки населения и улучшения уровня жизни граждан, что значительно снижает риски совершения преступлений гражданами, государства активно ведет работу по укреплению законности в правовом поле, совершенствуя законодательную базу, но стремительное развитие ситуации вокруг киберпространства требует решения все новые проблем в праве. Яркими примера может служить развитие робототехники, искусственного интеллекта, цифрового рубля и так далее.

В работе по укреплению законности и правопорядка активно принимают участие правоохранительные органы, к которым, как известно, относится и МВД России. Так, Указом Президента Российской Федерации от 11 октября 2022 г. в структуре МВД России было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России)[3].

Любые изменения в жизни общества требует от органов внутренних дел обновления и модернизации своей работы, современные же тенденции переноса значительной жизни общества в цифровую среду влияют не только на методы работы

[1] Краткая характеристика состояния преступности в Российской Федерации за январь–август 2023 года // МВД России [Сайт]. URL: https://xn--b1aew.xn--p1ai/reports/item/41741442/ (дата обращения: 13.05.2023).

[2] Обзор операций, совершенных без согласия клиентов финансовых организаций за период с января по декабрь 2022 г. // Банк России [Сайт]. URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 26.04.2023).

[3] В структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий // МВД России [Сайт]. URL: https://xn--b1aew.xn--p1ai/news/item/32844180/ (дата обращения: 05.08.2023).

правоохранительных органов, но и на средства. В сети интернет изменяется мышления и восприятия людей, логическое восприятие событий и их оценка, в виртуальном пространстве создаются сообщества, происходит общение, а частенько и совращение молодых неокрепших умов. В данном направлении борьба происходит в виртуальном мире, для ведения которой, необходимо высоко функциональное оборудование, отвечающее всем веяниям времени, а также знания и опыт работы с данным оборудованием. Это достаточно затратные процессы, но если мы хотим эффективно бороться с данными правонарушениями, необходимо не только приобретать такое оборудование, но и разрабатывать к нему определенной программное обеспечение, а это требует подготовки или найма на работу высококвалифицированных сотрудников.

В то же время сотрудники органов внутренних дел должны быть готовы работать с населением по вопросам цифровых-правовых отношений. Необходимо в образовательные программы подготовки всех категорий специалистов МВД России включать вопросы информационной безопасности граждан, а также эффективно использовать информационно-коммуникационные сети для профилактической работы с молодежью.

Невозможно одному ведомству работать с таким монстром как преступность в цифровом пространстве. Для достижения положительных результатов и улучшения уровня предупреждения цифровой преступности требуется комплексный подход, сотрудничества всех структур общества: между государственными органами, частными организациями и обществом в целом. Данное взаимодействие должно быть подробно разработано для разных структур и обязательно закреплено в праве и других нормативных документах.

© Байков В.М., 2023

Библиографический список:

1. Мецгер А. А. Профилактика правонарушений и защита прав человека в России // Закон и право. – 2022. – № 2. – С. 60–63.

2. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / Ю. В. Гаврилин, А. В. Аносов, В. В. Баранов [и др.]. – 2-е изд., перераб. и доп. – Москва: Академия управления МВД России, 2019. – 208 с.

3. Суходолов А. П. Проблемы противодействия преступности в сфере цифровой экономики / А. П. Суходолов, Л. А. Колпакова, Б. А. Спасенников // Всероссийский криминологический журнал. – 2017. – № 2. – С. 258–267.

4. Манжуева О. М. Феномен информационной безопасности: сущность и особенности: специальность 09.00.01: автореф. дис. … д-ра филос. наук / Манжуева Оксана Михайловна. – Улан-Уде, 2015. – 383 с.

ЕРМОЛИН ДАНИИЛ АЛЕКСАНДРОВИЧ

слушатель факультета подготовки сотрудников
для оперативных подразделений
Санкт-Петербургский университет МВД России

Научный руководитель:
АКИЕВ АРБИ РУСЛАНОВИЧ

начальник кафедры криминалистики
Санкт-Петербургский университет МВД России
кандидат юридических наук

МЕТОДИКА ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ СИСТЕМ И СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ, ФУНКЦИОНИРУЮЩИХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В данной статье рассматривается методика повышения эффективности защиты систем и сетей передачи данных, функционирующих в органах внутренних дел Российской Федерации. Описаны методы повышения эффективности защиты систем и сетей передачи данных, функционирующих в органах внутренних дел Российской Федерации.*

Ключевые слова: *системы и сети передачи данных, защиты систем и сетей передачи данных, криптографическая защита информации, защита информации в ОВД РФ, криптография, защита конфиденциальной информации*

В настоящее время, цифровизация проникает во все сферы жизни, и ее главная цель - улучшение качества жизни людей за счет использования новейших технологий. Государство тоже активно внедряет цифровые технологии в систему управления и экономики. В России многолетний курс на создание «Электронного правительства» начался еще в 2002 году, а сегодня его развитию посвящен нацпроект "Цифровая экономика". В этой связи, МВД России разработала программу цифровой трансформации для обеспечения более безопасных и эффективных условий работы ведомства. МВД России занимает лидирующее место в использовании цифровых технологий среди других государственных органов. Важная черта цифровой трансформации МВД России заключается не только в развитии информационной инфраструктуры, но и в охране информации, особенно чувствительной, получаемой и используемой в ходе оперативно-служебной деятельности, с помощью правовых, организационных и технических мер защиты.

Учитывая, что большинство служебной информации обрабатывается, хранится и передается через ведомственную компьютерную сеть, которая охватывает все отделения МВД России, особое внимание следует уделять защите систем и сетей передачи данных в ОВД. Необходимо

обеспечивать эффективную защиту чувствительной информации, передаваемой в сети, для предотвращения уязвимостей в ИС, а также возможных крупных атак на информационные ресурсы МВД России. Кроме того, служебная информация может быть скомпрометирована злоумышленниками в процессе передачи по каналам передачи данных, поэтому необходимо следить за эффективностью средств защиты информации для обеспечения безопасности систем и сетей передачи данных в ведомстве. Сотрудники подразделений информационных технологий, связи и защиты информации могут использовать методики по повышению эффективности защиты систем и сетей передачи данных в ОВД РФ для усовершенствования текущих систем защиты.

Подготовка к работе включала анализ информационно-технологической и коммуникационной инфраструктуры органов внутренних дел РФ, в том числе процесса ее цифровой трансформации, изучение структуры и способов подключения к ней оконечных устройств сотрудников МВД. Также были изучены особенности функционирования облачной инфраструктуры ИСОД МВД России и определены уязвимости систем и сетей передачи данных, анализировались нормативные требования к защите информации и приведены меры по обеспечению ИБ систем и сетей передачи данных. В ходе анализа были выявлены угрозы ИБ, такие как сетевые атаки и компрометация криптоключей, что требует постоянного внимания к данной проблеме и предприятия соответствующих мер. Кроме того, был изучен механизм определения базовых защитных мер в соответствии с характеристиками ИС, чтобы обеспечить надежную защиту информации.

ПОИБ ИСОД МВД России является сложной системой, где элементы тесно взаимодействуют друг с другом и любой пропущенный элемент может привести к уязвимости ИС для внутренних и внешних угроз. Средства защиты систем и сетей передачи данных играют важную роль в поддержании конфиденциальности информации в СПД.

Мною были созданы предложения относительно настройки конфигурации компонента *VipNet Administrator* и увеличения пропускной способности канала связи при применении программно-аппаратного комплекса *ViPNet Coordinator HW* в рамках стратегии повышения эффективности защиты систем и сетей передачи данных в сфере ОВД РФ.

В ходе анализа базовых настроек администрирования регионального сегмента ИСОД МВД России, удалось выявить ряд проблем, а именно:

1. Конфигурация компонента ЦУС *ViPNet Administrator* настроена «по умолчанию», а именно: пользователи с именем абонентского пункта и типы коллективов регистрируются автоматически, что в свою очередь способствует появлению проблем в дальнейшем администрировании сети.

2. Поскольку включение нового пользователя в коллектив регламентирует возможность данного пользователя расшифровать информацию ограниченного доступа, передаваемую своему коллективу или любому другому пользователю данного коллектива, создаются условия для реализации угрозы несанкционированного

ознакомления пользователя с информацией ограниченного доступа. К тому же, в коллективе зачастую за одним АРМ работает несколько пользователей, что также увеличивает вероятность угрозы.

3. В региональных сегментах отсутствуют сетевые группы, позволяющие снизить нагрузку криптографических преобразований и упростить администрирование сегментов сети, АРМ которых обрабатывают информацию одного уровня конфиденциальности.

4. В региональных сегментах отсутствуют скрытые коллективы, которые позволяют реализовать возможность руководителям подразделений МВД России иметь доступ к информации своих подчинённых.

5. В региональных сегментах реализована классическая полносвязная схема между всеми созданными типами коллективов, что создаёт предпосылки для максимальных нагрузок на подсистему шифрования трафика ViPNet Coordinator HW, на базе которого функционирует вся сеть.

6. При присоединении нового пользователя задается строгая привязка пользователей к своим абонентским пунктам через тип коллектива по правилу «1 пользователь — 1 коллектив», что в свою очередь накладывает определенные ограничения на сотрудников ОВД, которым в виду их должностного положения необходимо работать на нескольких АРМ.

7. В наименовании пользователей отсутствует персонификация

и наглядность (несмотря на персонализацию по подразделениям), которая позволила бы администратору сети осуществлять более эффективный и не требующий больших временных затрат аудит сети.

8. Отсутствуют возможности для быстрого масштабирования и модификации сети, а именно отсутствует возможность добавления, удаления, переименования большого количества пользователей, абонентских пунктов и типов коллектива.

Таким образом, проведенный анализ конфигурации настроек компонента *VipNet Administrator* в региональном сегменте обуславливает необходимость в разработке подходов по оптимизации параметров *VipNet*-сети.

Технические специалисты территориальных органов МВД России могут использовать это предложение, для улучшения защиты систем и сетей передачи данных в ОВД Российской Федерации, чтобы повысить уровень защищенности региональных сегментов ведомственности сети конфиденциальной связи.

© Ермолин Д. А., 2023

Библиографический список:

1. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 29.12.2022) // Собрание законодательства Российской Федерации (далее — СЗ РФ). – 2006. – № 31 (ч. I), ст. 3448.

2. О федеральной целевой программе «Электронная Россия» (2002–2010 годы): постановление Правительства Российской Федерации от 28 января 2002 г. № 65 (ред. от 09.06.2010) // СЗ РФ. – 2002. – № 5, ст. 531.

3. О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)»: распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р (ред. от 26.12.2013) // СЗ РФ. – 2010. – № 46, ст. 6026.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: приказ ФСБ России от 10 июля 2014 г. № 378 // Российская газета. — 2014. — 17 сентября.

5. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну: приказ ФАПСИ от 13 июня 2001 г. № 152 // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2001. – № 34.

6. Об утверждении новой Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел»: приказ МВД России от 8 июня 2006 г. № 420 // Организация правовой работы в системе МВД России: сборник правовых актов и методических документов. – Москва, 2006. – Т. II.

7. Бабкин А. Н. Моделирование и прогнозирование угроз информационной безопасности регионального сегмента ИСОД МВД России / А. Н. Бабкин, А. Ю. Куличенко, А. А. Широкий // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 79–88.

8. Единак В. В. Перспективы развития единой информационно-телекоммуникационной системы (ЕИТКС) органов внутренних дел / В. В. Единак, В. П. Писаренко; отв. ред. В. В. Воронин // Информационные технологии XXI века: сборник научный трудов. – Хабаровск: Тихоокеанский государственный университет, 2018. – С. 482–487.

9. Зарубин В. С. Варианты оптимизации защищенных телекоммуникационных сетей vipnet / В. С. Зарубин, С. В. Зарубин // Охрана, безопасность, связь. – 2022. – № 7-2. – С. 23–27.

10. Зарубин С. В. Некоторые аспекты защиты информации, передаваемой по каналам связи ИМТС МВД России / С. В. Зарубин, К. В. Колесов // Охрана, безопасность, связь. – 2020. – № 5-2. – С. 237–242

11. Куличенко А. Ю. Современное состояние защиты информации в телекоммуникационных сетях территориальных органов МВД России / А. Ю. Куличенко // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – № 6-2. – С. 178–182.

12. Зарубин С. В. Некоторые аспекты оптимизации настроек компонента планирования защищенной сети vipnet Administrator / С. В. Зарубин, Г. В. Перминов // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2019. – № 5-2. – С. 141–144.

13. Защита информации в ИСОД МВД России: учебное пособие / А. Н. Бабкин [и др.]. – Воронеж: Воронежский институт МВД России. – 2018. – 129 с.

14. Канавин С. В. К вопросу проведения комплексного исследования инженерной и телекоммуникационной инфраструктуры регионального сегмента ИМТС МВД России / С. В. Канавин, Н. С. Хохлов // Охрана, безопасность, связь. – 2022. – № 7-1. – С. 236–241.

15. Куватов В. И. Программно-аппаратная защита информации: Курс лекций / В. И. Куватов, О. Е. Чудаков, В. Н. Родин. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. – 192 с.

ЗУЕВ ЕВГЕНИЙ СЕРГЕЕВИЧ

преподаватель кафедры деятельности ОВД в особых условиях
Санкт-Петербургский университет МВД России

О ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Аннотация. *Исследованы особенности внедрения проекта «Приоритет 2030», развитие дополнительного образования по освоению программы «Цифровая кафедра». Рекомендована организация взаимодействия профильных образовательных учреждений, реализующих программы по изучению информационных технологий и информационных систем с ведомственными образовательными учреждениями МВД. Предложено создание волонтерского движения для предупреждения киберпреступлений.*

Ключевые слова: *информационная безопасность, кибервиктимность, волонтеры, информационные технологии, киберпреступность, реестр, цифровая кафедра*

Расширение спектра применения информационных технологий в России способствовал как количественному росту числа выявленных преступлений, так и появлению новых способов совершения преступлений. Нормативная правовая база не изменяется с такой же скоростью, как динамично изменяется сущность и структура преступности. В связи с чем правовые регуляторы общественных отношений нуждаются в качественной переработке и дополнениях. Можем утверждать, что преступность развивается вне территориальных рамок, преследует единственную, во многом разрушительную цель — получение сверхприбыли.

Утвердившимся явлением текущих событий явилось то, что если раньше криминальные элементы тянулись к объектам преступных посягательств, используя орудия преступления материального мира, то последняя тенденция гигантского роста трансграничной преступности демонстрирует нам все способы виртуального совершения преступлений.

Сотрудники правоохранительных органов в основном работают не с факторами, влияющими на преступность, а непосредственно с фактами преступной деятельности.

Для формирования информационного массива данных в интересах противодействия преступности, создания информационной модели для борьбы с киберпреступлениями необходимо детально проработать проблему преступности в данной сфере, разобраться с имеющим место быть смешением и пересечением различных понятий и терминов, отсутствием ясных представлений о стратегии борьбы и методики расследования данного явления.

По данным организации *Positive Technologies* за 2022 год увеличилось общее количество кибератак на 20,8 %. Отчасти это объяснялось ростом напряжения в киберпространстве. Предполагается, что мошенники расширяют свой бизнес, привлекают

новых исполнителей, используют для рутинных операций и обработки данных по заданному алгоритму виртуальных роботов (ботов).

По мнению Е. В. Пуляевой единое киберпространство можно определить как совокупность субъектов информационных отношений, информационных ресурсов, систем, технологий, устройств для обработки, хранения, воспроизведения информации [1].

Мы согласимся на данном этапе исследования с этой моделью киберпространства, объединенной одним общим признаком — возможностью открытого доступа к информационно-телекоммуникационным сетям.

Проблема кибервиктимности и многократное увеличение жертв преступлений, совершенных при помощи информационно-телекоммуникационных технологий требуют разработки программы для создания комплекса мер по защите населения. В этой связи интересен опыт государства Израиль и предложение о создании мирового кибершита.

Изучение передового зарубежного опыта и отечественной следственно-судебной практики дадут положительный результат. На наш взгляд, совместная работа сотрудников правоохранительных органов с психологами, лингвистами и другими специалистами над проблемой киберпреступности помогут снизить риски для наших граждан, хотя избавиться от угрозы вряд ли удастся.

По данным Центрального Банка России объем денежных потерь российских граждан от телефонного мошенничества в 2022 году составил 14,2 млрд рублей. При этом максимальная, единовременно похищенная сумма достигла 500 млн рублей. Под влиянием телефонных преступников в 2022 году российские граждане пытались оформить кредиты на 200 млрд рублей, а 83 % граждан России хотя бы раз сталкивались с попытками кибермошенничества.

Приказом МВД России «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации»[1] была создана так называемая «киберполиция». Задачи, возложенные на это подразделение, будут лишь увеличиваться, а расследуемые преступления усложняться, на наш взгляд. Сегодня назрела необходимость в помощи правоохранительным органам для борьбы с киберпреступностью.

Тщательное изучение влияние современных достижений науки и техники позволит использовать их во благо человечества, а нежелательные проявления исключить или минимизировать.

В этой связи интересен информационный модуль, выпущенный в 2019 году Управлением Организацией Объединенных Наций по наркотикам и преступности[2].

[1] Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: приказ МВД России от 29 декабря 2022 г. № 1110 // Справочно-правовая система «Гарант». URL: https://www.garant.ru/. – Докупент не публиковался.

[2] Серия университетских модулей. Киберпреступность. Модуль 5. Расследование киберпреступлений. URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_5_Cybercrime_Investigation_RU.pdf // (дата обращения: 01.09.2023).

Считаем необходимым учитывать рекомендации международных правоохранительных организаций при реализации профессиональных образовательных программ в учреждениях МВД России.

Развитие российской науки, внедрение научных разработок в повседневную жизнь, открытие новых технологий и их применение на блага общества — приоритетные задачи государства, определенные в Стратегии научно-технического развития Российской Федерации[1].

Финансирование развития науки, оценка труда ученых, применение полученных ими открытий в различных сферах деятельности — залог процветания нашего государства и улучшение уровня жизни его граждан.

В соответствии с Постановлением Правительства Российской Федерации «О мерах по реализации программы стратегического академического лидерства "Приоритет–2030"»[2] для вузов–участников программы разработан проект «Цифровые кафедры» проект «Цифровые кафедры» реализуется в рамках федерального проекта «Развитие кадрового потенциала ИТ-отрасли» национальной программы «Цифровая экономика Российской Федерации».

В качестве результата «обучающимся обеспечена возможность получения дополнительной квалификации по ИТ-профилю посредством обучения на «цифровой кафедре» образовательной организации высшего образования — участника программы стратегического академического лидерства «Приоритет-2030». Целью данного результата является обеспечение приоритетных отраслей экономики высококвалифицированными кадрами, обладающими цифровыми компетенциями. Показателем федерального проекта является «Количество обученных, получивших дополнительную ИТ-квалификацию на «цифровых кафедрах». Участниками проекта являются университеты-участники программы «Приоритет-2030» и университеты-кандидаты на вступление в программу «Приоритет-2030».

Мы считаем, что с учетом сложившейся криминогенной обстановки, изменения структуры преступности и увеличения способов совершения преступлений, образовательным учреждениям системы МВД так же необходимо участвовать в проекте «Цифровые кафедры». С учетом срока обучения по данному направлению, проект можно реализовывать в рамках профессиональной подготовки лиц, впервые принятых на службу в органы внутренних дел Российской Федерации. Сотрудники органов внутренних дел будут располагать актуальной и достоверной информацией, что поможет повысить эффективность в расследовании киберпреступлений.

Противодействие преступлениям, совершаемым с применением информационно-коммуникационных

[1] Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации»: постановление Правительства Российской Федерации от 29 марта 2019 г. № 377 (ред. от 09.12.2022) // Собрание законодательства Российской Федерации. 2019. № 15 (ч. III), ст. 1750.

[2] О мерах по реализации программы стратегического академического лидерства «Приоритет-2030»: постановление Правительства Российской Федерации от 13 мая 2021 г. № 729 // Собрание законодательства Российской Федерации. 2021. № 22, ст. 3823.

технологий, должно быть комплексным, адресным, основательно проработанным.

Учитывая то, что жертвами преступления становятся жертвы из различных социальных слоев населения, возрастных групп, имеющий различный уровень дохода, суммы накоплений, в разной степени владеющие информационно-коммуникационными абонентскими устройствами связи, на наш взгляд, необходимо реализовать программу социальной профилактики для населения. Привлечение студентов образовательных учреждений среднего и высшего образования, социальных работников поможет осветить проблему для различных категорий граждан и помочь в борьбе с преступностью.

Особую роль, на наш взгляд, для профилактики киберпреступлений нужно уделить работникам финансово-кредитных организаций. Ведь именно сотрудники банков выступают первичным звеном при оформлении финансовых документов, обслуживают физических лиц, выдают платежные средства (карты) и открывают счета.

Исключительно совместная работа, направленная на ознакомление населения и предупреждение о важности хранения персональных данных будет результативной.

Предлагаем для повышения информированности населения организовать волонтерское движение, разработать программу и формы взаимодействия с населением.

Предупреждение преступлений — задача государства, общества и каждого гражданина. Правоохранительные органы совместно с волонтерами смогут, на наш взгляд, повлиять на состояние киберпреступности.

© Зуев Е. С., 2023

Библиографический список:

1. Динамика институтов информационной безопасности. Правовые проблемы: сборник научных трудов / отв. ред. Т. А. Полякова, В. Б. Наумов, Э. В. Талапина. – Москва: ИГП РАН, 2018. – 264 с.

2. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) [Электронный ресурс]: сборник статей Международной научно-практической конференции. – Москва: Академия управления МВД России, 2018.

3. Оценка цифровой готовности населения России: доклад к XXII Апрельской международной научной конференции по проблемам развития экономики и общества, Москва, 13–30 апреля 2021 г. / Н. Е. Дмитриева (рук. авт. кол.), А. Б. Жулин, Р. Е. Артамонов, Э. А. Титов; Национальный исследовательский университет «Высшая школа экономики». – Москва: Издательский дом Высшей школы экономики, 2021. – 86 с.

4. Смушкин А .Б. Концепция дистанционной криминалистики: монография / под ред. докт. юрид. наук, проф. В. Б. Вехова. – Москва: Юрлитинформ, 2024. – 256 с.

КАЗАКОВ РОДИОН АЛЕКСЕЕВИЧ

курсант факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Санкт-Петербургский университет МВД России

Научный руководитель:
САВЕЛЬЕВА МАРИЯ ВЛАДИМИРОВНА

доцент кафедры теории и истории государства и права
Санкт-Петербургский университет МВД России
кандидат юридических наук, доцент

РАЗРАБОТКА ЦИФРОВОГО КОДЕКСА: ПРАВОСУБЪЕКТНОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. Этап цифровизации требует внедрения новых технических решений в правовой сфере. Наиболее насущным вопросом в российском обществе в настоящее время является разработка и внедрение цифрового кодекса, который, на наш взгляд, должен затрагивать вопросы применения искусственного интеллекта (далее – ИИ), защиты данных граждан, а также использование цифровых технологий в области оказания услуг и в процессе голосования. Нами поднимаются вопросы необходимости наделения ИИ правосубъектностью, будут выдвинуты позиции «за» и «против», будет предложена структура цифрового кодекса, а также предложены правовые нормы, с помощью которых будет осуществляться нормативно-правовое регулирование в данной области.

Ключевые слова: цифровой кодекс, правосубъектность, ИИ, правовое регулирование

Цифровой кодекс, как ранее указывалось в аннотации, должен охватывать достаточно широкий пласт интересов общества, что требует разработки правовых норм и технических условий, необходимых для его функционирования.

Приводя аргументацию «за» правосубъектность, считаем важным начать с того, что наделение искусственного интеллекта правосубъектностью позволит более продуктивно совершенствовать технологии, что, в свою очередь, создает необходимые условия для его применения в условиях автономии.

Рассуждая об ответственности, следует отметить, что наделенный правосубъектностью искусственного интеллекта (далее — ИИ) позволил бы разграничивать и определять лиц, его применивших. Это, конечно же, позволило бы облегчить процесс взыскания ущерба, усовершенствовало бы процесс защиты прав потребителей и третьих лиц, которые стали своего рода «жертвами» применения участниками правоотношений

ИИ. Для выявления использования ИИ предлагаем взять за основу функционал, применяемый порталом *antiplagiat.ru*, который способен определить сгенерированный материал и указать нам это. Совершенствуя данную систему, было бы вполне реальным определять участие ИИ не только на уровне составления текстовой информации, но и при другом применении ИИ. Для защиты интеллектуальной собственности, которая была создана с помощью ИИ, был бы полезен такой критерий, как «юридическая защита» [2].

Участие в регулировании систем, функционирующих автономно. Правосубъектность позволила бы нам предметно регулировать различного рода управляемые устройства, которые работают автономно. Так, например, в рамках правового поля возможно было разместить беспилотно пилотируемые летательные аппараты.

Выдвигая аргументы «против», считаем необходимым начать с того, что ИИ не наделен сознанием и не имеет представлений о том, что такое нравственная ответственность. Если говорить более предметно, то ИИ, в принципе, не способен к оценке своих действий с нравственной стороны.

Сложности в определении ответственности — это еще одна часть, которая позволяет выступить против правосубъектности. Здесь речь идет о юридической неопределенности, технической несовершенности программ по выявлению ИИ, что может привести к возникновению ошибок при определении ответственности [1].

Кроме того, использование искусственного интеллекта порождает между человеком и ИИ конкуренцию. Даже сейчас просматриваются ситуации, когда ИИ вытесняет человека с рынка труда.

Поговорим о структуре цифрового кодекса и совершенствовании нормативно-правовой базы, сущность которой описана в разделах представленного нами кодекса. Наш вариант типовой, схож с содержанием многих нормативно-правовых актов, однако ввиду содержания в цифровом кодексе условий использования ИИ и защиты данных пользователей будут сделаны некоторые акценты:

В качестве первого раздела мы предлагаем ввести раздел «Общие положения», который определяет основные понятия, применяемые настоящим кодексом, задачи, цели, особенности регулирования [3].

Второй раздел связан с использованием ИИ в различных общественных сферах. Речь идет о порядке создания, претворения в жизнь и получения определенных результатов от сгенерированных с помощью ИИ конечных продуктов. Кроме того, считаем важным рассмотреть в данном разделе вопросы ответственности и безопасности.

Третий раздел затрагивает безопасность и защиту данных пользователей, как участников общественно-цифровых отношений. Речь идет о составлении протоколов безопасности, подразумевающих собой информацию о порядке хранения, передачи, обработки данных пользователей.

Четвертый раздел посвящен электронному голосованию и сервису «Госуслуги». Речь идет о прозрачности использования данных систем, гарантий достоверности и подлинности. Применительно к Госуслугам

речь идет и способах защиты данных пользователей (в данном случае уклон делается в большей степени в сторону превенции, так как защиту данных раскрывает третий раздел).

Пятый раздел посвящен раскрытию государственных органов и должностных лиц, которые наделены правом предупреждать, пресекать нарушения в данной сфере, а также меры ответственности.

Цифровой кодекс является важной составляющей для совершенствования правой системы в эпоху всеобщей цифровизации. Данное внедрение позволило бы сделать существующую систему более гибкой, адаптивной к новшествам и удобной в использовании.

© Казаков Р. А., 2023

Библиографический список:

1. Цифровое право [Электронный ресурс]. – URL: https://dgtlaw.ru/analytic/otvetstvennost-iskusstvennogo-intellekta-v-pravovom-pole (дата обращения: 11.02.2024).

2. Социальный фонд России // GOV.RU [Сайт]. – URL: https://sfr.gov.ru/press_center/z_news/~2023/08/15/253461 (дата обращения: 11.02.2024)/

3. NAKED SCIENCE [Электронный ресурс]. – URL: https://naked-science.ru/article/sci/stephen-hawking-about-artificial-intelligence (дата обращения: 11.02.2024).

МАКАРЕНКО МАКСИМ АНАТОЛЬЕВИЧ

заместитель начальника кафедры уголовного процесса
Санкт-Петербургский университет МВД России,
кандидат юридических наук, доцент

СИСТЕМА КОНТРОЛЯ И НАДЗОРА ЗА ЗАКОННОСТЬЮ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ В УСЛОВИЯХ ЕГО ЦИФРОВИЗАЦИИ

Аннотация. *В статье рассматривается вопрос о необходимости совершенствования теоретических основ контроля и надзора уголовным преследованием, их нормативной регламентации, в условиях перехода на электронный формат. Уделено внимание зарубежному опыту внедрения цифровых технологий в уголовное судопроизводство.*

Ключевые слова: *прокурорский надзор, процессуальное руководство, процессуальный контроль, уголовное преследование, досудебное производство, цифровизация, цифровой формат*

В последние несколько десятков лет стремительным образом внедряются новые технологии, происходит глобальная цифровизация современной жизни практически во всех сферах её проявления. Это позволяет, прежде всего, улучшить и ускорить выполнение различных операций [1, с. 104]. Происходящие изменения не могли не коснуться и уголовного судопроизводства, однако до сих пор в России, как и раньше, материалы уголовных дел формируются на бумажной основе. При этом во многих государствах, в том числе и в некоторых, образованных на постсоветском пространстве, уголовно-процессуальная деятельность ведётся в цифровом формате. В этом отношении наиболее перспективен опыт Республики Казахстан.

Один из наиболее актуальных вопросов, обсуждаемых в научной среде, состоит в необходимости кардинальных изменений досудебного производства в связи с его переводом на электронный формат. Прежде всего, это касается отказа от стадии возбуждения уголовного дела. Обратим внимание на то, что такой отказ имел место в Казахстане. В этом отношении интересен опыт Киргизской Республики, уголовный процесс которой обходился без стадии возбуждения уголовного дела почти два года, но с принятием нового уголовно-процессуального закона от 28 октября 2021 г. она была возвращена и теперь действует в рамках цифрового формата досудебного производства.

Другой актуальный вопрос состоит в необходимости внесения корректировок в механизм функционирования контроля и надзора за законностью осуществления уголовного преследования. Имеются ввиду конечно же, такие его суплементарные, составляющие как прокурорский надзор и процессуальный контроль. Как в рамках того, так и в рамках

другого, в установленных законом пределах, осуществляется процессуальное руководство, которое может рассматриваться как правовое средство процессуального управления деятельностью лиц, осуществляющих расследование преступлений. Будучи объединёнными в единую систему, все названные составляющие требуют особой регламентации, отвечающей специфике производства в условиях цифрового пространства.

Прежде всего, опасно отстранение субъектов контроля и надзора, функционирующих в рамках досудебного производства, от реальной работы «в полях». Согласно УПК Республики Казахстан, где предусмотрен электронный формат производства по уголовным делам, прокурор вправе участвовать в осмотрах мест происшествий. Тогда как в России, где досудебное производство ведётся только в бумажном формате, таким правом он не обладает.

Преимущества цифрового формата состоят, прежде всего, в оперативности проверки руководителем органа расследования или прокурором процессуальных документов, их согласования или санкционирования, отмены, а также продления и установления процессуальных сроков. Наряду с экономией времени происходит экономия финансовых ресурсов, которые идут на распечатывание и пересылку материалов, порой — неоднократную.

Организационно-распорядительными актами Генеральной прокуратуры Российской Федерации предусмотрено ведение специальных книг учёта, поступающих в органы прокуратуры процессуальных решений и материалов [2; 3]. Если обратиться к статистическим данным, то за 2022 год прокурорами выявлено 5 217 038 нарушений законности, отменено 1 419 601 постановление об отказе в возбуждении уголовного дела, 387 214 — о приостановлении расследования, предъявлено 1 799 639 требований об устранении нарушений законности [3]. Суммарно в органы следствия и дознания направлено более 2 млн только основных актов прокурорского реагирования. Кроме того, немалый объём документооборота приходится на сами органы предварительного расследования в рамках функционирования правоотношений, складывающихся по поводу процессуального управления уголовным преследованием. Всё это происходит в бумажном формате, требуя привлечение значительных трудовых ресурсов, временных затрат и т. д.

Обращаясь к зарубежному опыту, отметим, что наряду с уголовно-процессуальным законом в Республике Казахстан действует Инструкция по организации надзора за законностью уголовного преследования, утверждённая Прокурором Республики 21 февраля 2023 г. № 65 [5], в которой детально регламентирована процессуальная деятельность прокуроров. В приложении № 3 к данной инструкции содержится детально разработанный алгоритм их действий по согласованию (утверждению) ключевых процессуальных решений (далее — КПР).

Алгоритм предусматривает, что руководитель органа прокуратуры в течение рабочего времени каждые 4 часа лично проводит мониторинг информационной системы единый реестр досудебных расследований (далее — ЕРДР) на предмет поступления

на согласование либо утверждение процессуальных решений от органа уголовного преследования. В течение одного часа с момента поступления КПР отписывается конкретному прокурорскому работнику (уполномоченному или процессуальному прокурору) для проверки его законности. Руководитель контролирует как сроки, так и законность, обоснованность принимаемых ими решений.

Проверка журнала надзора в информационной системе ЕРДР прокурорскими работниками производится каждые три часа. При поступлении от руководителя КПР в течение 9 часов проверяется его законность и обоснованность, а по уголовным делам, в рамках производства по которым задержан подозреваемый, — в более краткие сроки. Согласование КПР в системе ЕРДР происходит простым нажатием на кнопку «СОГЛАСОВЫВАЮ». Если же оно не согласуется прокурором, то он составляет мотивированное постановление об отказе в согласовании, которое подписывает электронной цифровой подписью.

Реформирование контроля и надзора, произошедшее в Российской Федерации в 2007 году, сместило акцент в единой системе, которую они в своей совокупности составляют, в сторону процессуального контроля. В результате не прокурор, а руководитель следственного органа согласует и утверждает ключевые решения следователей. Однако их копии подлежат обязательному направлению в органы прокуратуры на проверку, по результатам которой прокуроры их вправе отменить. Некоторые статистические данные по таким отменам приводились выше.

Следует понимать, что контроль и надзор уголовным преследованием при любом варианте соотношения полномочий осуществляющих их субъектов, будучи системой процессуального управления, может и должна быть переведена на цифровую платформу. В настоящее время проводится реализация Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года [6]. Учитывая неизбежность уже довольно скорого перехода российского досудебного производства на электронный формат, сейчас востребованы научные исследования, позволяющие подготовить законодательную базу и организационную составляющую к предстоящим преобразованиям.

Как видим, наряду с изучением зарубежного опыта важнейшее значение в современных условиях приобретает теоретическая разработка оптимальной правовой модели контроля и надзора за законностью уголовным преследованием. В цифровом пространстве она имеет свежие перспективы существенного совершенствования, будучи призванной стать более оперативной и эффективной системой. Они вполне достижимы, но, конечно же, требуют надлежащего нормативно-правового и организационного обеспечения. В неизменном виде действующая система контроля и надзора при переходе досудебного производства на цифровой формат оставаться не сможет.

© Макаренко М. А., 2023

Список литературы:

1. Скляр М. А., Кудрявцева К.В. Цифровизация: основные направления, преимущества и риски // Экономическое возрождение России. 2019. № 3 (61). С. 103–114.

2. Приказ Генеральной прокуратуры Российской Федерации от 17 сентября 2021 г. № 544 «Об организации надзора за процессуальной деятельностью органов предварительного следствия» // Законность. 2021. № 12.

3. Приказ Генеральной прокуратуры Российской Федерации от 19 января 2022 г. № 11 «Об организации надзора за процессуальной деятельностью органов дознания» // Законность. 2022. № 11.

4. Статистические данные об основных показателях деятельности органов прокуратуры Российской Федерации за январь-декабрь 2022 г. URL: https://epp.genproc.gov.ru/web/gprf/activity/statistics/ office/result?item=85327980.

5. Приказ Генерального Прокурора Республики Казахстан от 21 февраля 2023 г. № 65 «Об утверждении Инструкции по организации надзора за законностью уголовного преследования». URL: https://online.zakon.kz/Document/ ?doc_id=33556520&pos=6;-108#pos= 6;-108.

6. Приказ Генеральной прокуратуры Российской Федерации от 14 сентября 2017 г. № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Законность. 2017. № 12.

МАРТЫНЕНКО ИГОРЬ ВЛАДИМИРОВИЧ

аспирант юридического факультета
Санкт-Петербургский университет
технологий управления и экономики

СОВРЕМЕННЫЕ ПРОБЛЕМЫ РАЗВИТИЯ И ПРАВОВОГО РЕГУЛИРОВАНИЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Аннотация. *В статье дается определение электронной коммерции; говорится о причинах развития информационного общества и электронной коммерции; анализируется указ президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»; описываются различия между электронной коммерцией и электронной торговлей; определяются категории электронной коммерции; выделены проблемы связанные с правовым регулированием электронного бизнеса в России.*

Ключевые слова: *электронная коммерция, информационное общество, продажи товаров дистанционным способом, b2c-сервисы, защита прав потребителей в сфере электронной коммерции, электронная торговля*

В настоящее время стремительное развитие как информационно-телекоммуникационных технологий, так и товарно-денежных отношений, складывающихся в сети интернет, привело к активному росту дистанционной торговли в сети интернет, что в свою очередь обуславливает значимость правового регулирования электронной коммерции. Электронная коммерция на сегодняшний день вполне органично вписывается в экономическую систему Российской Федерации. Посредством интернета осуществляется рекламное продвижение, заключаются сделки продажи товаров и услуг, потребители получают возможность удаленно покупать товары или услуги, а коммерческие предприятия получают возможность для продвижения своего продукта до потребителя.

Постоянный рост и популяризация торговли в интернет-сегменте объясняется достаточно просто: покупка и продажа в виртуальном пространстве удобна всем участникам правоотношений. Потребитель получает возможность осуществлять покупки находясь в комфортных для себя условиях, например из дома, а также выигрывает время, не затрачивая его на дорогу до магазина и обратно, а продавец в свою очередь экономит средства на аренду торговых площадей необходимых для размещения товаров, а также может предложить свою продукцию неограниченному числу потенциальных покупателей. По указанным выше причинам электронная коммерция развивается впечатляющими темпами, привлекая интеллектуальные ресурсы и внедряя инновации в сфере электронной коммерции.

О значимости развития правоотношений в сфере электронной

коммерции говорит Президент Российской Федерации в своем указе «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1]. Согласно указу Стратегия определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. Согласно данной Стратегии, развитие цифровой экономики является одним из важнейших направлений, призванное обеспечить национальные интересы Российской Федерации. Там же дается понятие цифровой экономики, как хозяйственной деятельности, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг [2].

Поэтому важнейшим фактором развития информационного общества в Российской Федерации является цифровая экономика, ядром которой является электронная коммерция, как сфера, оказывающая на нее наибольшее влияние.

Большое значение при этом имеет разграничение таких понятий как «электронная коммерция» и «электронная торговля». Понятие электронной коммерции намного шире, чем понятие электронной торговли, причем последняя составляет лишь часть первой и представляет собой способ продажи и покупок товаров и услуг через Интернет. В то время как под электронной коммерцией понимается сфера экономики, включающая в себя все торговые, финансовые операции, которые осуществляются с помощью компьютерных сетей. Таким образом, электронная коммерция включает не только электронную торговлю, но и рекламу, и продвижение товаров, содействие связям сторон, обеспечение маркетинговых исследований рынка, электронные закупки и поддержку бизнес-процессов [5].

При этом при всей значимости электронной коммерции в развитии цифровой экономики в законодательстве отсутствует ее легальное определение. Все теоретические наработки правоведов нашли свое отражение в международных нормативно-правовых актах. Например, в разработанном ЮНСИТРАЛ «Типовом законе об электронной торговле» 16 декабря 1996 г. Дано следующее определение электронной коммерции: «сделки, заключаемые с помощью электронного обмена данными и других средств передачи данных, предусматривающих использование альтернативных бумажных форм и методов передачи

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203 / Собрание законодательство Российской Федерации. 2017. № 20, ст. 2901.

и хранения информации». Аналогичное определение дано в рамках Рабочей программы по электронной коммерции, принятой ВТО 25 сентября 1998 г. [6]. Однако, одно из самых оптимальных определений электронной коммерции дал А. И. Савельев, который определяет электронную коммерцию как совокупность отношений, возникающих в связи с заключением сделок посредством сети Интернет, а также при продвижении товаров, работ, услуг и иных объектов гражданских прав в сети Интернет.

С точки зрения субъектного состава участников электронной коммерции принято выделять следующие ее категории:

1) *Business-to-Consumer* (*B2C*);
2) *Business-to-Business* (*B2B*);
3) *Consumer-to-Consume* (*C2C*);
4) *Business-to-Government* (*B2G*) [4].

Business-to-Consumer (*B2C*) — это разновидность электронной коммерции, при которой предприятия продают свои продукты и услуги конечным потребителям или клиентам напрямую без посредников. Это позволяет компаниям участвовать в прямой коммерческой деятельности с потребителями, предоставляя последним более широкий доступ к продуктам и услугам первых.

Business-to-Business (*B2B*) — это такой вид рыночного взаимодействия, когда стороны юридические лица совершают обмен продуктами, услугами или информацией между собой. То есть сделка совершается между компаниями, а не между компанией и отдельным потребителем. Например, сделка между юридической компанией и клининговой компанией.

Consumer-to-Consumer (*C2C*) — интернет торговля между физическими лицами, когда одно частное лицо продает товары другому частному лицу. Чаще всего такие сделки совершаются при участии посредника в виде торговой онлайн-площадки. Это могут быть аукционные онлайн-платформы, платформы по предоставлению или обмену услугами в конкретной нише, социальные сети или мессенджеры.

Business-to-Government (*B2G*) — это продажа продукта государственным учреждениям. Так частные предприятия предоставляют различные виды услуг государственным учреждениям. Например, обеспечивают услуги ИТ-поддержки.

Наиболее популярная бизнес-модель в электронной коммерции — это модель B2C, то есть модель взаимоотношений интернет-магазина с покупателем. Поскольку в этом случае речь идет о продаже товара покупателю, такие взаимоотношения будут квалифицироваться как договор розничной купли-продажи с применением положений законодательства о защите прав потребителей.

Определение продажи товаров дистанционным способом дано в п. 2 ст. 497 Гражданского кодекса Российской Федерации[1] (далее — ГК РФ). При этом для договоров, заключенных в электронной форме, действуют правила договоров розничной купли-продажи. Так согласно ст. 437 ГК РФ, где речь идет

[1] Часть первая Гражданского кодекса Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательств Российской Федерации. 1994. № 32, ст. 3301.

о публичной оферте, продавец обязан заключить договор со всеми на равных условиях. Основное отличие электронного договора купли-продажи от обычного договора розничной купли-продажи заключается в удаленном способе его заключения [3].

В процессе осуществления взаимодействия между продавцом и покупателем в рамках электронной торговли, часто возникают проблемы, связанные с достоверностью той информации, которую продавец размещает на сайте. Нередко случаются ситуации, когда вследствие технической ошибки на сайте продавца может отображаться цена значительно меньше реальной стоимости товара.

Так, например, в конце октября — начале ноября 2021 г. Управление Роспотребнадзора по г. Москве получило огромное количество обращений по фактам отмены заказов маркетплейсом *Ozon.ru* в одностороннем порядке.

Дело в том, что в этот период на маркетплейсе *Ozon.ru* были неожиданно предложены существенные скидки, доходившие в некоторых случаях до 90 %, чем тут же воспользовались покупатели, оформив заказы на товары с этими скидками.

Покупатели, думая, что приобретают товар по акции, произвели оплату, однако через некоторое время получили уведомления от *Ozon.ru* о том, что их заказ отменен, а деньги будут возвращены. Дело в том, что на сайте произошел технический сбой, из-за чего цены на товар были существенно снижены, при этом сам продавец не знал о таком снижении [7].

Примечателен и другой случай сбоя на сайте продавца, в результате которого возникла аналогичная спорная ситуация. В июле 2021 года житель Волгограда осуществил покупку в ОАО «Торговый дом ЦУМ» 19 товаров с ценой от 19 до 129 рублей. Продавец направил на электронный адрес и номер телефона покупателя подтверждение заключения договора купли-продажи.

Однако позже покупателя уведомили о невозможности доставки заказанного товара, аннулировали заказ и предложили вернуть деньги. Покупатель не согласился с предложением Торгового дома и обратился в суд.

В суде Представитель продавца указал, на то, что на их сайте произошел технический сбой, из-за чего цены на товар стали отражаться некорректно и стоимость товаров упала в 846 раз относительно их действительной цены.

В результате суд первой инстанции встал на сторону Торгового дома и отказал в удовлетворении иска покупателя. В дальнейшем апелляционная и кассационная инстанции согласились с выводами суда первой инстанции и оставили решение без изменения. В итоге дело дошло до рассмотрения в Верховный Суд Российской Федерации, который отменил решения нижестоящих инстанций и отправил дело на новое рассмотрение.

В своем определении Верховный Суд Российской Федерации исходил из того, что предложение о продаже товаров на сайте продавца является публичной офертой и после оплаты Торговый дом должен был передать товар покупателю.

Верховный суд пришел к выводу, что соответствии с п. 12 Правил продажи товаров по договору розничной купли-продажи, утверждённых постановлением Правительства Российской Федерации 31 декабря 2020 г. № 2463, при дистанционном способе продажи товара продавец обязан заключить договор розничной купли-продажи с любым лицом, выразившим намерение приобрести товар на условиях оферты.

Фиксация цены происходит в момент заключения договора между покупателем и интернет-магазином, который определяется моментом оформления заказа с присвоением ему номера, который позволяет потребителю получить информацию о заключённом договоре розничной купли-продажи и его условиях. Изменить цену, объявленную в момент оформления заказа, продавец в одностороннем порядке не вправе [1].

Тем не менее, в результате повторного рассмотрения дела судом первой инстанции после возвращения его из Верховного Суда Российской Федерации покупателю повторно было отказано в удовлетворении исковых требований.

Таким образом, электронная коммерция является важнейшим элементом становления и развития цифровой экономики. При этом приведенные выше примеры свидетельствуют как о серьёзном развитии и значимости электронной коммерции в наши дни, так и об определенных проблемах, связанных с законодательным регулированием указанной сферы правоотношений. Стоит признать, что, несмотря на постепенное формирование правовой базы в российском законодательстве в области регулирования электронной коммерции, интенсивное развитие цифровой экономики на данный момент существенно опережает развитие законодательства.

© Мартыненко И. В., 2023

Библиографический список:

1. Определение Судебной коллегии по гражданским делам Верховного суда Российской Федерации от 06.06.2023 г. № 16-КГ23-6-К4 // Справочно-правовая система «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/407019844/ (дата обращения 15.10.2023).

2. Микаева А. С. Правовое регулирование электронной торговли в сети интернет \\ Новая Наука: от идеи к результату. – 2016. – № 12-3. – С. 203–205.

3. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. – 2-е изд., перераб. и доп. – Москва: Статут, 2016. – 640 с.

4. Умирзакова А. Д. Международно-правовое регулирование электронной коммерции / А. Д. Умирзакова, С. Н. Сабикенов // Казахский Национальный университет им. Аль-Фараби Казахстан: сборники конференций. – Алма-Ата: НИЦ Социосфера. 2015. – № 22. – С. 341–344.

5. Литвинова Д. В. Правовое регулирование электронной коммерции: отечественный и зарубежный опыт: монография / Д. В. Литвинова, Ю. К. Цареградская. – Москва: Проспект, 2023. – С. 8.

6. Управление федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по городу Москве [Электронный ресурс]. – URL: https://77.rospotrebnadzor.ru/index.php/napravlenie/zpp/10173-o-pravakh-potrebitelej-v-svyazi-s-odnostoronnej-otmenoj-zakazov-po-aktsii-09-11-2021 (дата обращения 15.10.2023).

ОГАРЬ ТАТЬЯНА АНДРЕЕВНА

начальник кафедры уголовного права
Санкт-Петербургский университет МВД России
кандидат юридических наук, доцент, полковник полиции

ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ ФОРМЫ ВИНЫ В ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. *В статье рассматриваются актуальные проблемы определения формы вины в преступлениях в сфере компьютерной информации путем анализа законодательства, уголовно-правовой доктрины и судебно-следственной практики.*

Ключевые слова: *преступления в сере компьютерной информации, формы вины, умысел, неосторожность*

Уголовная ответственность за преступления в сфере компьютерной информации появилась сравнительно недавно, соответствующая глава была включена лишь в Уголовный кодекс Российской Федерации (далее — УК РФ) 1996 года и в первоначальной редакции включала в себя только 3 статьи, предусматривающие ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

За период действия УК РФ 1996 года по настоящее время данная глава была дополнена двумя новыми статьями: в 2017 году была предусмотрена уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ), которая фактически объединила в себе три ранее существовавших преступления при совершении их в отношении нового объекта (критической информационной инфраструктуры), а также в 2022 году была предусмотрена ответственность за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274^2 УК РФ).

Изучение данных статистики за последние 4 года показывает, что при довольно большом количестве ежегодно регистрируемы преступлений в данной сфере (таблица 1) количество лиц, привлекаемых к уголовной ответственности крайне мало (таблица 2).

Такое несоответствие между количеством зарегистрированных преступлений и количеством лиц, привлеченных к уголовной ответственности может быть обусловлено различными факторами: как трудностями

при раскрытии и расследовании этих преступлений, которые могут совершаться из любой точки мира, так и трудностями при установлении в содеянном конкретных признаков состава преступления, образующих основание уголовной ответственности.

Таблица 1 – Количество зарегистрированных преступлений, предусмотренных ст. 272–273 УК РФ [10–13]

Статья / год	2019	2020	2021	2022
Ст. 272 УК РФ	2 420	4 105	6 392	9 308
Ст. 273 УК РФ	455	371	317	200

Таблица 2 – Количество осужденных по преступлениям, предусмотренным в главе 28 УК РФ «Преступления в сфере компьютерной информации» [6–9]

Статья / год	2019	2020	2021	2022
Ст. 272 УК РФ	85	84	133	179
Ст. 273 УК РФ	76	45	77	46
Ст. 274 УК РФ	0	0	0	1
Ст. 274^1 УК РФ	4	8	15	54
Ст. 274^2 УК РФ	—	—	—	—

Так как данная группа преступлений является сравнительно молодой то по ней, в отличие других видов преступлений, отсутствует многолетний опыт правоприменительной деятельности и сформировавшаяся судебная практика. Первые рекомендации относительно толкования признаков составов рассматриваемых преступлений были сформулированы в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утвержденных Генпрокуратурой России в 2014 году [5]. Данный документ содержит разъяснения по всем признакам составов преступлений, предусмотренных ст. 272–274 УК РФ.

Первые обобщения судебной практики были сделаны лишь в декабре 2022 года путем принятия Пленумом Верховного Суда Российской Федерации Постановления от 15.12.2022 г. № 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». В указанном постановлении был сделан ряд разъяснений, больше касающихся раскрытия содержания признаков объективной стороны рассматриваемых преступлений.

Вместе с тем, установление формы вины, при наличии которой закрепленное в уголовном законе деяние является преступлением, выступает важным обстоятельством для определения круга уголовно-наказуемых деяний, охватываемых то или иной нормой Особенной части Уголовного кодекса. Если преступление может быть совершено при наличии любой формы вины, то это максимально расширяет сферу применения конкретной нормы. При этом, возможность привлечения лица к уголовной ответственности при наличии той или иной формы вины зависит от степени общественной опасности запрещенного деяния. Так, умысел увеличивает степень общественной опасности любого деяния. Но если аналогичное деяние совершено по неосторожности, то степень его общественной опасности может не достигать уровня преступления. Так, например, причинение тяжкого вреда здоровью уголовно наказуемо при наличии любой формы вины, в то время как причинение легкого вреда здоровью является преступлением только при наличии умысла на его причинение.

Во многих статьях УК РФ отсутствует указание на конкретную форму вины, в таком случае возможность совершения преступления с той или иной формой вины устанавливается исходя из анализа диспозиции статьи каждого конкретного преступления, путем учета особенностей признаков объективной стороны (ее законодательная конструкция, способ или обстановка совершения преступления), наличия/отсутствия признака «заведомость», мотивов или целей. По отдельным группам преступлений в пленум Верховного Суда Российской Федерации в своих постановлениях дает разъяснения о возможности совершения преступления с той или иной формой вины при отсутствии указания на это в законе. Так в п. 4 постановления Пленума Верховного Суда Российской Федерации от 18.10.2012 г. № 21 «О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования» даны разъяснения относительно возможности совершения указанных преступлений с той или иной формой вины, при этом, для отдельных преступлений отмечается возможность совершения их как умышленно, так и по неосторожности, а для других только с неосторожной формой вины.

К сожалению, в принятом 15.12.2022 г. постановлении № 37, посвященном преступлениям в сфере компьютерной информации, единственное упоминание о признаках субъективной стороны имеется в п. 6, где указано, что в рамках каждого уголовного дела подлежат установлению не только общественно-опасные деяния, но также в наступившие последствия, «возможность наступления которых охватывалась *умыслом* лица», что не внесло ясности в рассматриваемый вопрос.

В преступлениях в сфере компьютерной информации законодатель

не указал форму вины, что послужило поводом для формирования разных подходов к ее определению в доктрине уголовного права и правоприменительной практике. В рамках подготовки указанной статьи нами были изучены имеющиеся суждения относительно формы вины, изложенные в методических рекомендациях Генеральной прокуратуры Российской Федерации, учебниках и комментариях к УК РФ, так как они содержат общепринятые положения и обобщения. Проведенное изучение показало отсутствие единообразия при определении формы вины в преступлениях в сфере компьютерной информации (таблица 3).

Таблица 3 – Подходы к определению формы вины в преступлениях, предусмотренных ст. 272–274 УК РФ

Статья УК РФ	Методические рекомендации [5]	Источник 1 [3]	Источник 2 [4]	Источник 3 [14]	Источник 4 [15]
272	Умысел и неосторожнос ть	Умысел и неосто-рожность	Умысел	Умысел	Умысел и неосто-рожность
273	Умысел	Прямой умысел	Прямой умысел	Прямой умысел	Прямой умысел
274	Умысел и неосторожность	Умысел и неосто-рожность	Неосторож-ность	Умысел	Умысел и неосто-рожность

Как видно, единообразный подход имеется только к определению форм вины в преступлении, предусмотренном ст. 273 УК РФ. Этому способствует законодательная конструкция объективной стороны рассматриваемого преступления. В соответствии со ст. 26 УК РФ формулировка интеллектуальных и волевых признаков неосторожной формы вины предполагает отношение лица к наступлению общественно опасных последствий, это позволяет сделать вывод о том, что такая форма вины возможна лишь в преступлениях с материальным составом, предполагающим наступление таковых. Соответственно, если у преступления формальная конструкция объективной стороны, то оно может быть совершено умышленно, причем умысел должен быть только прямой [1 с. 78; 2 с. 35]. Так как преступление, предусмотренное ст. 273 УК РФ имеет формальную конструкцию объективной стороны, то оно может быть совершено только с прямым умыслом.

Однако с определением формы вины в преступлениях, предусмотренных в ст. 272 УК РФ и ст. 274 УК РФ наблюдает отсутствие единообразия, так как это преступления имеющие материальную конструкцию объективной стороны, предусматривающую наступления общественно-опасных последствий. Так, неправомерный доступ к компьютерной информации (ст. 272 УК РФ) по мнению одной части авторов может быть совершен только умышленно, а другие полагают, что возможна любая форма вины. Формулировки деяния, как «неправомерный доступ к охраняемой законом информации»

свидетельствует о том, что лицо должно осознавать отсутствие разрешений и полномочий на доступ к информации и понимать, что она охраняется, что свидетельствует в пользу умысла. Проведенное изучение опубликованной судебной практики показало отсутствие приговоров по ст. 272 УК РФ, в которых упоминалась бы неосторожная форма вины, то есть к уголовной ответственности привлекают, как правило, при наличии умысла в отношении наступивших последствий. Однако, формулировка диспозиции не препятствует привлечению к уголовной ответственности при наличии неосторожной формы вины.

Что касается нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), то формулировка деяния скорее характера для неосторожных преступлений. Однако, указание на неосторожную форму вины в диспозиции рассматриваемой статьи отсутствует. Более того, по поводу данного преступления имеются прямо противоположные мнения, так есть авторы, которые полагают что это только умышленное преступление, в то время как другие относят его к преступлениям, совершенным только по неосторожности. Практически полное отсутствие правоприменительной практики по данной статье за последние 4 года не позволяет сделать значимых обобщений, и свидетельствует о том, что отсутствие единого мнения относительно формы вины в данном преступлении является причиной для непримененения данной нормы.

Таким образом, полагаем, что в целях повышения эффективности уголовно-правовой охраны компьютерной информации следует включить в Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 г. № 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» разъяснения относительно формы вины в преступлениях в сфере компьютерной информации.

© Огарь Т. А., 2023

Библиографический список:

1. Дуюнов В. К. Квалификация преступлений: законодательство, теория, судебная прутика: монография / В. К. Дуюнов, А. Г. Хлебушкин. – 6-е изд. – Москва: ИНФРА-М, 2021. – 481 с.

2. Кадников Н. Г. Квалификация преступлений и вопросы судебного толкования: монография. – Москва: Юриспруденция, 2019. – 336 с.

3. Комментарий к Уголовному кодексу Российской Федерации: в 4 т. / В. М. Лебедев [и др.]; отв. ред. В. М. Лебедев. – Москва: Юрайт, 2023. – Т. 3: Особенная часть. – 298 с.

4. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Т. К. Агузаров, А. А. Ашин, П. В. Головненков [и др.]; под ред. А. И. Чучаева. – Испр., доп. и перераб. – Москва: КОНТРАКТ, 2013. – 672 с.

5. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. // Генеральная Прокуратура Российской Федерации [Сайт]. – URL: https://epp.genproc.gov.ru/ru/web/gprf/documents?item=4900252 (дата обращения: 05.05.2023).

6. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лицах, в отношении которых вынесены судебные акты по уголовным делам за 2019 год // Судебный департамент при Верховном Суде Российской Федерации [Сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5259 (дата обращения: 18.04.2023)

7. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лицах, в отношении которых вынесены судебные акты по уголовным делам за 2020 год // Судебный департамент при Верховном Суде Российской Федерации [Сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения: 18.04.2023).

8. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лицах, в отношении которых вынесены судебные акты по уголовным делам за 2021 год // Судебный департамент при Верховном Суде Российской Федерации [Сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=6121 (дата обращения: 18.04.2023).

9. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лицах, в отношении которых вынесены судебные акты по уголовным делам за 2022 год // Судебный департамент при Верховном Суде Российской Федерации [Сайт]. – URL: http://www.cdep.ru/index.php?id=79&item=7649 (дата обращения: 18.04.2023).

10. Состояние преступности в Российской Федерации за январь–декабрь 2019 года // МВД России [Сайт]. – URL: https://xn--b1aew.xn--p1ai/reports/item/19412450 (дата обращения: 18.04.2023).

11. Состояние преступности в Российской Федерации за январь-декабрь 2020 года // МВД России [Сайт]. – URL: https://xn--b1aew.xn--p1ai/reports/item/22678184 (дата обращения: 18.04.2023).

12. Состояние преступности в Российской Федерации за январь–декабрь 2021 года // МВД России [Сайт]. – URL: https://xn--b1aew.xn--p1ai/reports/item/28021552 (дата обращения: 18.04.2023).

13. Состояние преступности в Российской Федерации за январь–декабрь 2022 года // МВД России [Сайт]. – URL: https://xn--b1aew.xn--p1ai/reports/item/35396677 (дата обращения: 18.04.2023).

14. Уголовное право России. Части Общая и Особенная: учебник / В. А. Блинников, А. В. Бриллиантов, О. А. Вагин [и др.]; под ред. А. В. Бриллиантова. – 2-е изд., перераб. и доп. – Москва: Проспект, 2015. – 1184 с.

15. Уголовное право. Особенная часть: учебник / Г. А. Агаев, Е. Н. Алешина-Алексеева, А. Г. Антонов [и др.]; Санкт-Петербургский университет МВД России. – Санкт-Петербург: Р-КОПИ, 2020. – 832 с.

ПРОУРЗИНА ОЛЬГА ЮРЬЕВНА

преподаватель–методист информационного центра
Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ ВНЕВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ЦЕЛЬЮ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Аннотация. *Исследованы особенности информационного обеспечения раскрытия и расследования преступлений в условиях межведомственного взаимодействия. Выявлена необходимость в интеграции межведомственных информационных систем и единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России). Предложена модель повышения квалификации сотрудников органов внутренних дел по изучению достижений научно-технического прогресса в сфере информационных технологий. Ожидаемый результат при реализации – сокращение трудозатрат при раскрытии и расследовании правонарушений.*

Ключевые слова: *информационное обеспечение, вневедомственные информационные системы, андрагогика, автоматизация труда*

Цифровизация современного мира, развитие глобальной информационно-телекоммуникационной компьютерной сети «Интернет», локальных информационных сетей и специализированных информационных систем представляет качественно новые ресурсы для развития человечества. Вместе с этим новые технологии и научные разработки порождают новые виды преступлений и представляют новые возможности для преступников. За последние десятилетия в нашей стране наблюдается увеличение количества преступлений, изменение структуры преступности, детерминант совершения преступления, в этих условиях формируется портрет современного преступника, вооруженного современными информационными технологиями, владеющего информационно-коммуникационными устройствами.

Интересным на наш взгляд является использование вневедомственных информационных систем в целях раскрытия, расследования и предупреждения преступлений. Рациональное использование сведений, получаемых из информационных систем, не относящихся к служебным ресурсам, должно успешно применяться для борьбы с преступностью.

Деятельность органов внутренних дел по выявлению, раскрытию и предупреждению преступлений имеет высокую значимость для обеспечения безопасности граждан и охраны государства, именно она выступает гарантом стабильности и правопорядка. Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года»[1] ставит своей целью как сохранение населения,

[1] О национальных целях развития Российской Федерации на период до 2030 года: указ Президента Российской Федерации от 21 июля 2020 г. № 474 // Собрание законодательства Российской Федерации (далее — СЗ РФ). 2020. № 30, ст. 4884.

здоровье и благополучие людей, так и цифровую трансформацию нашего государства.

В целях раскрытия и расследования преступлений сотрудники полиции используют криминалистически значимую информацию, получаемую из внешних информационных систем. Это позволяет раскрывать преступления в кратчайшие сроки и получать неоспоримые доказательства для расследования и осуществления правосудия.

В федеральном законе Российской Федерации «Об информации, информатизации и защите информации»[1] представлено следующее определение: «информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

В ст. 2 федерального закона «Об информации, информационных технологиях и о защите информации»[2] дается следующее определение основного термина: «информация — сведения (сообщения, данные) независимо от формы их представления».

Анализируя эти два определения, данные законодателем с интервалом в 11 лет для одного и того же объекта, можно утверждать, что сама по себе информация настолько широкое понятие, что любое толкование этого термина лишь ограничит его сущность. В настоящем федеральном законе также используется основное понятие информационных систем — как совокупности содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. На наш взгляд, это определение термина информационных систем не является полным и емким для отражения смысла и функциональных возможностей информационной системы.

Законопослушные граждане зачастую становятся жертвами мошенников, завладевших личными данными или информацией, ограниченного доступа. Социальная инженерия как маркер технологического развития общества в настоящее время приобрела негативные коннотации [1]. Для противодействия преступности, применяющей новейшие технологии в умелом сочетании с известными ранее способами совершения преступлений необходим ряд мер, для предупреждения данного вида преступлений. Мы считаем, что сегодня требуется разработка мер государственного и ведомственного регулирования для применения внешних информационных систем в деятельности сотрудников полиции.

Деятельность сотрудника органов внутренних дел по раскрытию, расследованию и предупреждению преступлений безотрывно связана с получением и применением актуальной, достоверной и значимой информацией. Исследование опыта работы сотрудников органов внутренних дел позволяет утверждать, что использование различных источников информации дает высокую эффективность при раскрытии и расследовании преступлений. Такими источниками являются не только служебные информационные системы.

[1] Об информации, информатизации и защите информации: федеральный закон от 20 февраля 1995 г. № 24-ФЗ (ред. от 10.01.2003) // СЗ РФ. 1995. № 8, ст. 609. – Утратил силу.

[2] Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 29.12.2022) // СЗ РФ. 2006. № 31 (ч. I), ст. 3448.

Информационное обеспечение правоохранительной деятельности позволяет принимать обоснованные тактические и процессуальные решения, успешно реализовывать полученные данные при построении тактики следственных действий.

На наш взгляд для обеспечения образовательной подготовки необходимо проводить систематическое обучение сотрудников правоохранительных органов по применению информационно-коммуникационных технологий и возможностям применения новых информационных массивов в борьбе с преступностью.

Мы считаем, что обучение по направлениям использования информационных технологий и информационно-коммуникационных устройств необходимо разрабатывать на базе профильных технических высших учебных заведений, с применением полигонов для тестирования и наглядной демонстрации возможностей современного оборудования. Однако содержание программы обучения для сотрудников правоохранительных органов необходимо составлять с учетом возраста слушателей, профиля служебной деятельности и базового образования. Андрагогика в современном мире развивается так стремительно, что в сочетании с профессионализмом профессорско-преподавательского состава мы получим положительные результаты.

Следственно-судебная практика свидетельствует о том, что число нераскрытых преступлений в России не снижается, а демонстрирует прямую зависимость от общего числа преступлений. Одной из важных причин недостаточного уровня раскрываемости преступлений является низкое качество информационного обеспечения процесса раскрытия и расследования преступлений. Последнее, являясь неотъемлемой частью криминалистического обеспечения, представляет собой многогранную деятельность, состоящую из подсистем правового, организационного, методического и технического характера [2]. Важную роль в повышении качества информационного обеспечения раскрытия и расследования преступлений играет, прежде всего грамотная организация деятельности по формированию, ведению и использованию сотрудниками правоохранительных органов информации, содержащейся в различных криминалистических учетах органов внутренних дел и сторонних информационных системах.

Примером одного из научных обоснованных решений может быть разработанная модель размещения доступа к вневедомственным информационным системам, интегрированная единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России).

Внедрение проекта «Экономика данных» в масштабах нашего государства должно быть организовано с учетом потребностей правоохранительных органов в целях борьбы с преступностью. В целях повышения эффективности работы органов внутренних дел считаем важным предложить создание унифицированных запросов и возможности направления в автоматическом режиме для получения информации из вневедомственных информационных систем. В целях раскрытия и расследования преступлений

сотрудники ОВД проводят трудоемкую работу по составлению тактики расследования, определения гипотез совершения преступлений, сбора достоверной и криминалистически значимой информации [3]. Возможность дистанционного получения сведений, содержащихся во вневедомственных информационных системах на основании типовых форм запросов значительно сэкономит время сбора информации во время проведения следствия и облегчит ознакомление с материалами дела для других сотрудников правоохранительных органов.

© Проурзина О. Ю., 2023

Библиографический список:

1. Оценка цифровой готовности населения России: доклад к XXII апрельской международной научной конференции по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Н. Е. Дмитриева (рук. авт. кол.), А. Б. Жулин, Р. Е. Артамонов, Э. А. Титов; Национальный исследовательский университет «Высшая школа экономики». – Москва: Издательский дом Высшей школы экономики, 2021. – 86 с.

2. Россинская Е. Р. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник Санкт-Петербургского университета. Право. – 2020. – № 3. – С. 745–759.

3. Смушкин А. Б. Об экосистеме предварительного расследования // Вестник Томского государственного университета. – 2023. – № 488. – С. 242–254.

РАХИМОВ ФАРИДУН ДАВЛАТАЛИЕВИЧ

адъюнкт адъюнктуры
Санкт-Петербургский университет МВД России

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО СОВЕРШЕНИЯ МОШЕННИЧЕСТВА В СФЕРЕ ИНВЕСТИЦИЙ

Аннотация. *Статья посвящена определению информационных технологий в качестве средства совершения мошенничества, содержанию отдельных ее элементов, и их отличия от информационно-телекоммуникационных технологий. В статье приводится ряд статистических сведений, благодаря которым объясняется рост распространения информационных технологий в качестве средства совершения мошенничества и популяризация инвестиций в качестве способа обмана при достижении преступного результата — хищения денежных средств.*

Ключевые слова: *мошенничество, инвестиции, информационные технологии, информационно-телекоммуникационные технологии, сеть «Интернет»*

Информационные технологии — это отличительная черта современного развивающегося общества и основное средство коммуникации, используемое в ключевых сферах жизнедеятельности. Показатели в сфере цифровой отрасли свидетельствуют о стабильной динамике использования информационных технологий в Российской Федерации (рисунок 1) [1].

Рисунок 1 – Состояние цифровой отрасли за 2020-2023 гг.

Отметим, что зона покрытия отдельных информационных технологий в процентном соотношении даже выше, чем общее количество населения Российской Федерации. Продолжающиеся процессы цифровизации общества закономерны с учетом темпов его развития и роста объема информации, потребляемого человеком. Глобальные изменения в сфере цифровой отрасли не могли не отразиться на регулирование рынка существующих в информационно-телекоммуникационной сети новых объектов экономических отношений. Вырастает оборот денежных средств с использованием платежных систем, он составил 3,3 трлн руб. в отчетном периоде за январь–декабрь 2023 г., снижается оборот наличных, увеличивается выпуск банковских карт, количество счетов, открытых учреждениями банковской системы [2]. Отмечается рост нетипичных форм цифровой валюты, не обеспеченных активами, при этом обладающими свойствами платежного средства, даже с возможностью их использования в иностранной юрисдикции, без участия в этих операциях третьих лиц.

Активное использовании участниками информационно-телекоммуникационных технологий (российскими гражданами, юридическими лицами, иностранными гражданами, в том числе, проживающими на территории Российской Федерации), новых объектов экономических отношений в цифровой среде привели к значительному росту популярности сферы инвестиций.

По данным поисковой системы «Яндекс» числовое значение запросов по слову «инвестиции» свидетельствует о популярности данного вопроса у российских пользователей сети «Интернет» (рисунок 2) [3].

для получения прибыли в краткосрочной и долгосрочной перспективе, появляются новые объекты экономических отношений и способы инвестирования в цифровые права. Отсутствие понимания у граждан о механизме их использования и сущности новых объектов экономических решений стали главными причинами распространения мошенничеств в сфере инвестиций с использованием информационных технологий в качестве средства совершения преступления — объекта, облечённого в форму, который осмысленно используется виновным для упрощения совершения им деяния.

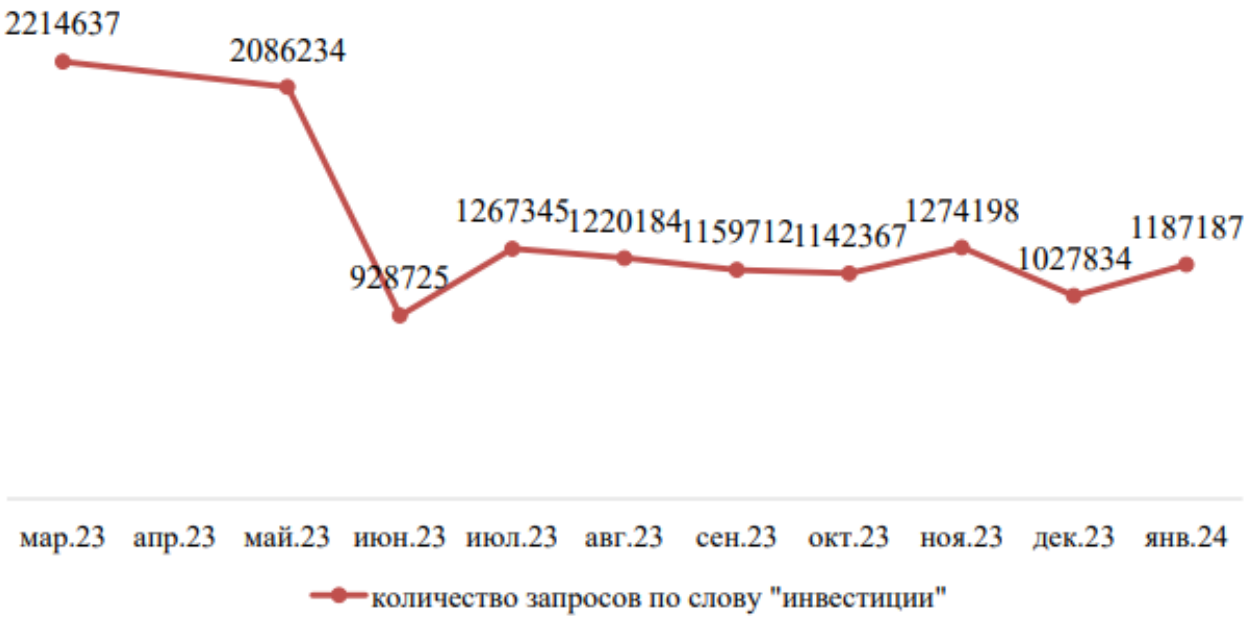

Рисунок 2 – Количество запросов по слову «инвестиции»

По данным поисковой системы «Гугл» слово «инвестиции» для граждан Республики Таджикистан и Российской Федерации по индексу популярности имеет стопроцентное значение. Помимо традиционных способов инвестирования с помощью вложения денежных средств в финансовые проекты, драгоценные метали, ценные бумаги, недвижимость,

Российское законодательство дает определение информационным технологиям как «*процессам, методам поиска, сбора, хранения, обработки, предоставления, распространения информации и способам осуществления таких процессов и методов*» [4]. Проводя сравнительный анализ с законодательством Республики Таджикистан, где под информационными

технологиями понимается «*совокупность средств вычислительной техники и телекоммуникаций, программных средств и методов их использования для поиска, обработки, хранения, передачи и получения информации*» [5], их определение для обоснования сущности данного термина кажется более удачным, потому что таким образом можно определить все многообразие элементов, из которого складывается понятие «информационные технологии», в виде совокупности информационных систем, технологических сетей, и средств вычислительной техники, с помощью которых осуществляется доступ к информации.

К ним можно отнести компьютеры, программное обеспечение, на котором функционирует ЭВМ, в том числе, операционную систему и приложения, коммуникации, а также сети локального и глобального предназначения для обеспечения информационных потребностей человека, доступа к информационным системам, удаленной работы с ними и информацией, передаваемой по линиям связи.

В. С. Володченко не случайно относит к информационным технологиям все ресурсы, с помощью которых осуществляется управление информацией: компьютеры, ноутбуки, планшеты, смартфоны, программное обеспечение, средства коммуникации [6]. Невозможно осуществить поиск новой информации и ее передачу на значительные расстояния, не используя для этого технические средства, обеспечивающие коммуникацию без прямого контакта с человеком.

С. Т. Гараев считает, что неоправданно сужать информационные технологии до коммуникативных технологий, связанных со связью и сетью «Интернет» [7]. Тем не менее, их наличие как раз и является главным условием для определения информационных технологий в качестве средства совершения мошенничества в сфере инвестиций. Вопрос только в том, какие объекты информационных технологий следует считать материальными (физическими), а какие идеальными (нематериальными) средствами, используемыми для упрощения совершения мошенничества.

Нам больше импонирует мнение А. А. Резник, что в качестве первых относятся электронно-вычислительная техника (компьютеры, ноутбуки, планшеты и т.п.), платежные инструменты (пластиковые банковские карты), средства связи (речь идет о смарт-картах, способных регистрироваться в мобильной сети, другими словами сим-карта); нематериальными средствами являются информационные системы, к которым относятся массивы информации, базы данных и т. п.; отдельная категория информационно-телекоммуникационных технологий, к которыми относятся электронная почта, сеть «Интернет», компьютерное программное обеспечение, с помощью которого осуществляется функционирование вычислительной техники и связи [8].

Говоря о цифровых активах, как о предполагаемом нематериальном средстве совершения мошенничества, не имеющей материальной формы, это набор числовых значений (единиц, кодов, записей), созданных с помощью вычислительных (цифровых) технологий, обладающих экономической ценностью, чаще всего не обеспеченных активами. Выбор цифровых активов в качестве сред-

ства совершения преступления, используемого как разновидность информационных технологий, обусловлено тем, что до сих пор не решен вопрос получения сведений о сторонах транзакций, из-чего информация о них анонимизирована. И. В. Колесов, комментируя сложившуюся ситуацию, называет это прямой предпосылкой для легализации добытых преступным путем денежных средств, и возможность беспрепятственно финансировать запрещенные формы деятельности, такие как терроризм и экстремизм [9].

На сегодняшний день мошенничество – один из наиболее распространённых видов преступлений против собственности и в структуре преступности в целом. Тем не менее, информационным центром МВД России не ведется отдельная статистика мошенничеств, совершенных в сфере инвестиций с использованием информационных технологий. Обусловлено это двумя причинами.

Во-первых, подобного рода мошенничество является лишь разновидностью основного состава мошенничества, в котором сфера инвестиций используется в качестве одного из способов обмана и злоупотребления доверием. Во-вторых, информационные технологии — понятие общее и использовать его только в качестве средства преступления было бы неверным.

Поэтому при формировании статистической отчетности ведется учет мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий, которые входят в понятие информационных технологий, наравне с другими средствами коммуникации, поиска и передачи информации, без разделения их на способы хищения денежных средства (рисунок 3) [10–12].

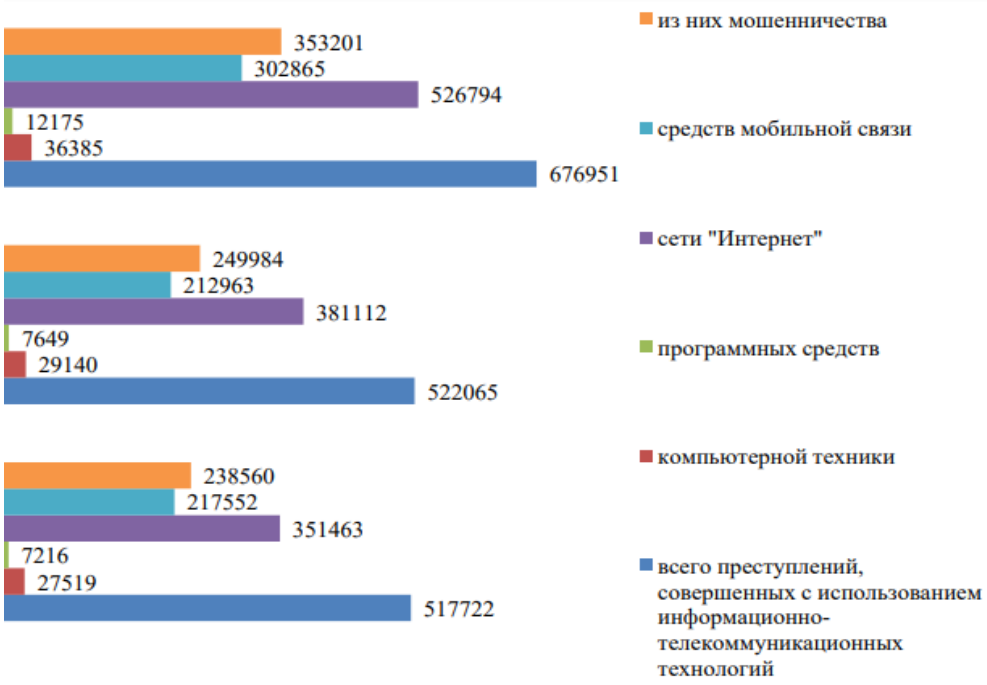

Рисунок 3 – Статистика мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий за 2020–2023 гг. в структуре общей преступности

Не случайно информационные технологии стали распространенным средством для совершения мошенничества в сфере инвестиций, потому что они обеспечивают сокрытие следов преступной деятельности, анонимность, отсутствие прямого контакта с жертвой, возможность воздействия на неопределенное количество людей даже с территории другого государства, а также минимальную подготовку и затраты средств на их приобретение. Таким образом, мошенничество сфере инвестиций, совершенное с использованием информационных технологий, является преступлениями латентными, трудно раскрываемым и расследуемым, что обусловлено разнообразием перечня доступных средств для облегчения совершения данного вида преступлений (смартфоны, ноутбуки, компьютеры, планшеты с выходом в глобальную сеть «Интернет», разнообразные платежные системы, цифровые активы, средства связи и платежа), с помощью которых любой может организовать инвестиционную деятельность, замаскированную под легальную схему получения денежных средств от процентов по прибыли, изначально не имея цели выполнить взятые на себя обязательства, сохраняя при этом анонимность, и не вступая в прямой контакт с жертвой.

© Рахимов Ф. Д., 2023

Список литературы:

1. Отчет о цифровизации в России // Datareportal [Сайт]. URL: https://datareportal.com/digital-in-the-russian-federation?utm_source=Global_Digital_Reports&utm_medium=Analysis_Article&utm_campaign=Digital_2024&utm_content=Digital_2024_Analysis_And_Review (дата обращения: 20.02.2024).

2. Статистика национальная платежной системы, период январь-декабрь 2023 г. // Банк России [Сайт]. URL: https://cbr.ru/statistics/nps/psrf/ (дата обращения: 20.02.2024).

3. Сервис подбора слов // Яндекс [Интернет портал]. URL: https://wordstat.yandex.ru (дата обращения: 20.02.2024).

4. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12.12.2023) // Российская газета. —2006. — 29 июля.

5. Закон Республики Таджикистан от 2001 года № 7 «Об информации». URL: https://ncpi.tj/wp-content/uploads/2020/02/18.Об-информатизации.pdf (дата обращения: 20.02.2024).

6. Володченко В. С. Понятие и квалификация информационных технологий / В. С. Володченко, Д. С. Ланцов и др. // Достижения науки и образования. 2020. № 12 (66). С. 41.

7. Гараев С. Т. Сущность информационно-коммуникационных технологий // Инновационная наука. 2016. № 6. С. 54/

8. Резник А. А. Понятие средства совершения преступления и его виды // Инновационная наука. 2020. № 3. С. 70.

9. Колесов И. В. Криптовалюта: возможности и угрозы / И. В. Колесов, Т. А. Стась // Финансовые исследования. 2018. № 4 (61). С. 173–174.

10. Статистика преступности за 2021 г. // МВД России [Сайт]. URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 20.02.2024).

11. Статистика преступности за 2022 г. // МВД России [Сайт]. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 20.02.2024).

12. Статистика преступности за 2022 г. // МВД России [Сайт]. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 20.02.2024).

СИМАКОВА ЕКАТЕРИНА АНДРЕЕВНА

курсант факультета подготовки сотрудников
для оперативных подразделений
Санкт-Петербургский университет МВД России

Научный руководитель:
БАДЗАГРАДЗЕ ТАТЬЯНА АЛЕКСАНДРОВНА

заместитель начальника кафедры криминалистики
Санкт-Петербургский университет МВД России
кандидат юридических наук, доцент

ОСОБЕННОСТИ ИЗЪЯТИЯ СВЕДЕНИЙ, СОДЕРЖАЩИХСЯ В ЭЛЕКТРОННЫХ СООБЩЕНИЯХ ИЛИ ИНЫХ ПЕРЕДАВАЕМЫХ ПО СЕТЯМ ЭЛЕКТРОСВЯЗИ СООБЩЕНИЯХ

Аннотация. *В рамках статьи рассматриваются особенности изъятия сведений, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях. В практике уголовного расследования такие данные могут иметь важное значение, поэтому процесс их изъятия должен быть выполнен в рамках соблюдения законодательства, регулирующего доступ к личной информации и защищающего конфиденциальность переписки. В статье освещаются правила и процедуры, которые необходимо соблюдать при проведении выемки электронных сообщений, а также важные аспекты, связанные с информационной безопасностью и защитой персональных данных.*

Ключевые слова: *осмотр и выемка электронных сообщений, изъятие данных, конфиденциальность переписки, персональные данные*

Уголовно-процессуальным кодексом Российской Федерации (далее — УПК РФ) регулируются основания и процедуры проведения следственного действия, такого как наложение ареста на почтовые отправления, их осмотр и выемка.

В 2016 году кроме «пакета Яровой», был принят федеральный закон № 375-ФЗ[1], который внес изменения в статью 185 УПК РФ. Согласно введенной в данную статью части 7: при наличии достаточных оснований, следователь по решению суда может провести осмотр и выемку электронных сообщений или иных сообщений, передаваемых по сетям электросвязи, если считает, что они содержат необходимые данные для уголовного дела [1].

Извлечение информации, содержащейся в электронных сообщениях, является одним из уголовно-процессуальных действий, которое может выполняться правоохранительными органами в ходе расследования преступлений. Этот процесс

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 6 июля 2016 г. № 375-ФЗ // Собрание законодательства Российской Федерации (далее — СЗ РФ). 2016. № 28, ст. 4559.

может быть особенно сложным из-за технологических и правовых ограничений, связанных с использованием электронной переписки в качестве доказательства.

Процедура выемки электронных сообщений предполагает получение согласия от владельца устройства, на котором хранятся эти сообщения. Если согласие отсутствует, то правоохранительные органы обращаются в суд с запросом на изъятие этих данных. В таком случае суд может вынести решение, что эти данные являются необходимыми для расследования преступления, и что их изъятие не нарушает законные права владельца. Анализ содержания ч. 7 ст. 185 УПК РФ позволяет сделать вывод, что после осмотра электронных сообщений следует проводить их выемку [2].

Однако, ввиду распространения современных технологий и широкого использования электронных сообщений, а также с учетом особенностей процедуры проведения, следует рассматривать выемку электронных сообщений как отдельное следственное действие.

Оценивая проблематику выемки электронных сообщений, В. Ф. Васюков отмечает, что закрепленный процессуальным законодательством порядок взаимодействия органов следствия с учреждением связи при наложении ареста на почтово-телеграфные отправления неприменим к возможным мероприятиям с участием операторов связи по аресту сообщений электронной почты [3].

Изъятие сведений, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях является сложным юридическим вопросом, связанным с защитой права на конфиденциальность переписки и соблюдением процедур, установленных законодательством. Также следует учитывать тот факт, что электронные сообщения могут содержать важную информацию для расследования уголовных дел, поэтому необходимо разработать специальные методики и технические средства для проведения выемки электронных сообщений в рамках уголовного процесса.

В большинстве стран существуют законы, регулирующие изъятие электронной переписки. Например, в США это *Electronic Communications Privacy Act* (*ECPA*), а в Европейском Союзе — Общий регламент по защите данных (*General Data Protection Regulation, GDPR*).

Изъятие информации с электронных носителей рассматривается на этапе проверки сообщения о преступлении, что обязывает дознавателя, орган дознания, следователя или руководителя следственного органа в течение трёх суток принять решение. Таким образом, изъятие электронных носителей при осмотре места происшествия до возбуждения уголовного дела при необходимости судебного решения буквально будет обязывать следователя приостановить производство осмотра. После этого следователю нужно будет: собрать необходимые материалы; утвердить ходатайство; обратиться с ним в суд и дождаться его рассмотрения.

Выемка электронных сообщений может быть выполнена с помощью различных технологий и методов, включая специальное программное обеспечение для извлечения данных, оборудование для считывания данных с жестких дисков и других носителей

данных, а также взлом компьютерных систем и устройств.

Кроме того, процесс выемки электронных сообщений может иметь негативные последствия для конфиденциальности и безопасности данных. Если процесс выемки не выполняется правильно, это то может привести к утечке конфиденциальной информации, такой как персональные данные или коммерческая тайны.

Одним из важных аспектов является вопрос защиты конфиденциальности переписки. Как правило, переписка между людьми защищена законодательством: Конституцией Российской Федерации[1] и федеральным законом «О персональных данных»[2], и может быть открыта только по указанию суда. Поэтому некоторые страны также требуют, чтобы изъятие электронных сообщений было согласовано с телекоммуникационным провайдером или другой компетентной организацией, отвечающей за хранение и передачу данных.

Также следует учитывать, что электронные сообщения могут содержать конфиденциальную информацию, которая не имеет отношения к делу, по которому проводится изъятие. В таком случае, должны применяться меры по защите конфиденциальной информации, например, её удаление или блокирование.

Важно отметить, что при изъятии сведений, содержащихся в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, необходимо учитывать особенности технологий, используемых для их передачи и хранения. Например, данные могут содержаться на удаленных серверах, расположенных за границей, и для их изъятия могут потребоваться специализированные инструменты и технологии.

В некоторых случаях, для изъятия сведений может потребоваться использование специализированного программного обеспечения, которое позволяет получать доступ к зашифрованным данным, или проведение компьютерной экспертизы для восстановления удаленных файлов или данных.

Изъятие электронных сообщений требует учета и других важных аспектов. Например, обеспечение информационной безопасности и защита персональных данных являются ключевыми задачами при проведении следственного действия. При этом необходимо строго соблюдать правила и процедуры, которые регулируют использование изъятой информации, чтобы предотвратить злоупотребление ею и неправомерное использование.

Помимо этого, при изъятии сведений из электронных сообщений необходимо учитывать временные рамки. Электронные сообщения могут содержать информацию о времени отправки и получения, а также о времени последнего доступа к ним. Эта информация может быть важна для установления времени совершения определенных действий или событий.

Изъятие информации, содержащейся на электронных носителях, должно быть оформлено в виде протокола в соответствии с правилами,

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // СЗ РФ. 2014. № 31, ст. 4398.

[2] О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 (ч. I), ст. 3451.

указанными в ст. 166 УПК РФ, и в таком случае, она будет относиться к таким доказательствам, как «иные документы» [4]. В протоколе следственного действия описываются отобранные электронные сообщения (вид сообщения, время получения, содержание и другие).

Необходимо соблюдать прозрачность и ответственность в процессе выемки электронных сообщений. В частности, необходимо убедиться, что люди, чьи данные будут изъяты, будут уведомлены об этом и будут иметь возможность обжаловать решение, если они считают, что это сделано неправомерно. Кроме того, необходимо развивать информационные технологии и методы защиты данных, чтобы снизить риск утечки данных и нарушений конфиденциальности.

Процесс выемки электронных сообщений является сложным и требует соблюдения определенных правил и процедур для гарантии законности и надлежащего использования изъятых данных. Кроме того, существуют правила, регулирующие хранение электронных данных, которые должны выполняться после выемки электронных сообщений.

В целом, процесс выемки электронных сообщений требует соблюдения законодательства, использования соответствующих технологий и методов. Правильная и законная выемка данных может стать важным следственным действием в расследовании уголовного дела.

© Симакова Е. А., 2023

Библиографический список:

1. Смешкова Л. В. Осмотр и выемка электронных сообщений / Л. В. Смешкова, О. И. Петров // Борьба с правонарушениями в сфере экономики: правовые, процессуальные и криминалистические аспекты: сборник материалов международной научно-практической конференции. – Новосибирск, 2020. – С. 114–117.

2. Архипова Н. А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. – 2018. – № 6. – С. 132–135.

3. Васюков В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. – 2019. – № 2. – С. 8–12.

4. Удовиченко В. С. Особенности изъятия информации с электронных носителей в досудебном производстве / В. С. Удовиченко, С. А. Сорокина // Алтайский юридический вестник. – 2021. – № 2 (34). – С. 133–138.

5. О проблеме изъятия электронных носителей информации в рамках следственных действий [Электронный ресурс]. – URL: https://www.advgazeta.ru/mneniya/o-probleme-izyatiya-elektronnykh-nositeley-informatsii-v-ramkakh-sledstvennykh-deystviy/.

СОРОКИН АНДРЕЙ РОМАНОВИЧ

слушатель факультета подготовки
сотрудников для оперативных подразделений
Санкт-Петербургский университет МВД России

Научный руководитель:
ЛАУР АЛЕКСАНДР ВЛАДИМИРОВИЧ

преподаватель кафедры криминалистики
Санкт-Петербургский университет МВД России

СОВРЕМЕННОЕ СОСТОЯНИЕ СЕРВИСОВ КОМПЬЮТЕРНОЙ РАЗВЕДКИ В СЕТИ ИНТЕРНЕТ И ИХ ВОЗМОЖНОСТИ. РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО ИХ ИСПОЛЬЗОВАНИЮ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Аннотация. *В данной статье рассматривается современное состояние сервисов компьютерной разведки в сети Интернет и их возможности, а также предлагаются рекомендации по использованию этих сервисов в деятельности органов внутренних дел.*

Ключевые слова: *информационная безопасность, компьютерная разведка, сервисы разведки в сети Интернет*

С развитием информационных технологий и распространением Интернета возникает все большая потребность в использовании сервисов компьютерной разведки. Эти сервисы могут быть использованы для различных целей, от слежки за конкурентами до борьбы с киберпреступностью и терроризмом. Одним из наиболее активных пользователей таких сервисов являются правоохранительные органы.

Сервисы компьютерной разведки включают в себя различные инструменты для сбора, анализа и интерпретации данных в сети Интернет. Эти сервисы включают в себя программное обеспечение для мониторинга социальных сетей, поисковых систем и других источников информации в Интернете. Они также могут включать в себя средства для отслеживания трафика и перехвата электронной почты.

Сервисы компьютерной разведки могут быть использованы для различных целей, включая обеспечение безопасности в Интернете, расследование преступлений, борьбу с киберпреступностью и терроризмом, а также слежку за конкурентами в бизнесе.

Сервисы компьютерной разведки могут быть разделены на две основные категории: открытые и закрытые. Открытые сервисы доступны для всех пользователей Интернета и могут быть использованы без ограничений. Закрытые сервисы, с другой стороны, доступны только определенным пользователям, которые

прошли специальную процедуру аутентификации.

Сервисы компьютерной разведки могут использоваться как для пассивного, так и для активного сбора информации. Пассивный сбор информации включает в себя мониторинг социальных сетей и поисковых систем, а также анализ трафика. Активный сбор информации включает в себя перехват электронной почты и взлом компьютерных систем.

Сервисы компьютерной разведки также могут быть использованы для анализа и интерпретации информации. Некоторые сервисы используют алгоритмы машинного обучения для анализа больших объемов данных и выявления скрытых связей между ними. Другие сервисы могут проводить анализ данных на основе определенных ключевых слов или фраз.

Рекомендации по использованию сервисов компьютерной разведки в деятельности органов внутренних дел (далее — ОВД):

Сервисы компьютерной разведки могут быть важным инструментом для деятельности правоохранительных органов. Однако, использование таких сервисов должно осуществляться в соответствии с законодательством, чтобы не нарушать права и свободы граждан.

Рекомендуется проводить обучение сотрудников ОВД по использованию сервисов компьютерной разведки. Это поможет избежать ошибок при использовании этих сервисов и снизит риск нарушения законодательства.

Также необходимо разработать стратегию использования сервисов компьютерной разведки в деятельности ОВД. Эта стратегия должна включать в себя четкие правила использования сервисов компьютерной разведки и определение границ использования этих сервисов.

Важно также проводить мониторинг использования сервисов компьютерной разведки сотрудниками ОВД. Это позволит выявить неправомерное использование этих сервисов и принять меры для предотвращения нарушений законодательства.

Сервисы компьютерной разведки становятся все более распространенными и доступными в Интернете. Эти сервисы имеют широкий спектр возможностей и могут использоваться как для защиты, так и для нарушения прав и свобод граждан.

Однако, правоохранительным органам следует использовать сервисы компьютерной разведки только в рамках закона и с соблюдением прав и свобод граждан. Для этого необходимо проводить обучение сотрудников ОВД по использованию этих сервисов, разрабатывать стратегию и правила их использования, а также мониторить их использование для предотвращения нарушений законодательства.

В будущем, сервисы компьютерной разведки, вероятно, будут продолжать развиваться и улучшаться, и правоохранительным органам следует следить за этими тенденциями и адаптировать свою деятельность в соответствии с новыми возможностями и вызовами.

© Сорокин А. Р., 2023

Библиографический список:

1. Павлова О. Н. Информационная безопасность: угрозы и методы защиты / О. Н. Павлова, А. В. Безуглов. – Москва: КНОРУС, 2019. – 192 с.

2. Павлова О. Н. Кибербезопасность и информационные технологии. – Москва: Юрайт, 2019. – 174 с.

3. Радаев А. А. Информационная безопасность: защита информации от несанкционированного доступа. – Москва: Форум, 2019. – 272 с.

4. Леонов Н. А. Кибербезопасность: защита от компьютерных атак / Н. А. Леонов, М. Ю. Гладков. – Москва: Питер, 2020. – 320 с.

5. Баринов А. В. Информационная безопасность предприятия: угрозы и защита – Москва: Эксмо, 2021. – 288 с.

6. Акопян А. Г. Кибербезопасность и защита информации: учебное пособие – Москва: Юрайт, 2021. – 292 с.

7. Лебедев В. С. Кибербезопасность: защита информации в условиях сетевой атаки / В. С. Лебедев, Д. Ю. Шейнин. – Москва: Проспект, 2021. – 352 с.

ТИХОНОВ ТИМУР АНДРЕЕВИЧ

слушатель факультета подготовки сотрудников
для оперативных подразделений
Санкт-Петербургский университет МВД России

ПРИМЕНЕНИЕ МЕТОДОВ КОМПЬЮТЕРНОЙ РАЗВЕДКИ ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ С ЧАСТНЫХ ОНЛАЙН-КАМЕР НАРУЖНОГО НАБЛЮДЕНИЯ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В данной статье рассматривается тема применения методов компьютерной разведки для получения информации с частных онлайн-камер наружного наблюдения в деятельности ОВД Российской Федерации. Описаны методы компьютерной разведки, которые можно и нужно применят для решения и упрощения задач, поставленных перед органами внутренних дел.*

Ключевые слова: *компьютерная разведка, методы и средства компьютерной разведки, онлайн-камеры, компьютерная разведка ОВД, получение компьютерной информации*

В XXI веке информационные технологии развиваются быстро, предоставляя человеку новые возможности во многих областях его жизни. Основу современных информационных технологий составляют средства обработки информации и информационно-телекоммуникационные сети, включая Интернет. Огромное количество информации хранится на серверах в Интернете, часть которой доступна общественности. Для поиска и использования этой информации используются компьютерные методы. Сегодня большинство людей получают информацию из открытых источников.

Компьютерная разведка (далее — КР) — это специальная деятельность, которая проводится как открыто, так и скрытно, и направлена на получение информации из информационных и телекоммуникационных сетей. Нормативно-правовая база позволяет органам внутренних дел (далее — ОВД) использовать методы КР в своей работе. При этом цель ОВД — получение открытой информации, которая помогает предотвращению, выявлению и раскрытию преступлений, а также защите прав, свобод и безопасности граждан и общества в целом, а также отслеживанию оперативной обстановки на определенной территории.

В Интернете функционируют множество онлайн-устройств, таких, как серверы, персональные компьютеры, смартфоны, роутеры, телевизоры, принтеры, сканеры, датчики, а также онлайн-камеры видеонаблюдения, которые взаимодействуют друг с другом. Онлайн-камера видеонаблюдения — это видеокамера, которая передает цифровой видеопоток через сеть Интернет, используя IP-протокол. У каждой онлайн-камеры есть свой уникальный IP-адрес. Обычно они используются для личного использования, но также

доступны для всех пользователей сети, при наличии правильных учетных данных.

Органы внутренних дел имеют возможность использовать аппаратно-программный комплекс (далее — АПК) «Безопасный город», который включает в себя огромное количество онлайн-камер видеонаблюдения, расположенных в общественных местах, особенно там, где происходит массовое скопление людей, таких как вокзалы, станции метро, улицы и площади. Важно отметить, что лишь камеры, установленные по заказу городской администрации и местных жилищно-коммунальных хозяйств, включены в АПК «Безопасный город». Тем не менее, в настоящее время существует значительное количество частных онлайн-камер видеонаблюдения, которые устанавливаются физическими и юридическими лицами для удовлетворения своих потребностей. Такие камеры транслируют видеопоток в интернет, и владельцы таких камер делятся данными для доступа с другими пользователями сети.

Для получения информации с онлайн-камер сотрудники ОВД могут использовать официальный запрос к физическому или юридическому лицу, однако этот метод не всегда возможен и результативен, так как не всегда можно установить владельца камеры и запись может быть удалена, а также может возникнуть отказ владельца предоставить доступ. Кроме того, данный метод неприменим для проведения негласного ОРМ. Применение методов КР позволит сотрудникам ОВД более эффективно и оперативно получать информацию с онлайн-камер в рамках проведения ОРМ и следственных действий, а также использовать свое право на получение информации.

Компьютерная разведка возникла совсем недавно и активно развивается, а также использоваться как сотрудниками правоохранительных органов, так и заинтересованными гражданами. КР — это процесс получения информации из информационно-телекоммуникационной сети Интернет посредствам применения специализированных методов и средств.

Основным нормативным правовым актом, регулирующим компьютерную разведку, является Конституция Российской Федерации[1]. В ч. 4 ст. 29 говорится: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

Помимо этого, в федеральном законе «Об информации, информационных технологиях и о защите информации»[2] в п. 1 и 2 ст. 3 говорится: «правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах: свободы поиска, получения, передачи, производства

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // Собрании законодательства Российской Федерации (далее — СЗ РФ). 2014. № 31, ст. 4398.

[2] Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 28.06.2022) // СЗ РФ 2006. № 31 (ч. I), ст. 3448.

и распространения информации любым законным способом».

В ч. 1 ст. 8 говорится, что «граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим федеральным законом и другими федеральными законами».

Основным нормативным правовым актом, регулирующим деятельность органов внутренних дел, является федеральный закон «О полиции»[1]. В п. 1 ст. 11 закреплено, что «полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру».

В федеральном законе «Об оперативно-розыскной деятельности»[2], поскольку информация, полученная с онлайн-камер сотрудниками оперативных подразделений ОВД, являющихся субъектами ОРД, при проведении отдельных ОРМ (в частности, ОРМ «Получение компьютерной информации») может выступать в качестве объекта ОРМ.

Онлайн-камера представляет собой видеокамеру, которая использует IP-протокол для передачи цифрового видеопотока по интернету. Она имеет собственный IP-адрес и транслирует видеопоток на локальный регистратор или персональный компьютер. В зависимости от модели и количества камер они могут подключаться к разному оборудованию по разным интерфейсам. Камеры могут быть аналоговыми или цифровыми. Они работают по стеку протоколов *TCP/IP*.

Работа по получению информации с частных онлайн-камерами наружного наблюдения можно разделить на три ключевых этапа:

1) поиск онлайн-камер в сети;

2) получение к ним доступа;

3) просмотр видеопотока.

Самый первый этап — это поиск онлайн-камер в сети.

Существуют два способа поиска онлайн-камер:

– ручное сканирование адресного пространства;

– использование поисковых систем с указанием текстовых шаблонов.

Современные технологии позволяют устанавливать онлайн-камеры для личных и профессиональных нужд, однако не все пользователи понимают принципы их работы и защиты информации. Часто люди не меняют стандартные логины и пароли, используемые при входе и настройке устройства, а также не обновляют программное обеспечение камеры, что делает их уязвимыми для злоумышленников. Из-за этого частные камеры могут стать объектом интереса для злоумышленников, которые смогут получить доступ к данным и использовать их против владельца. В связи с тем, что существует множество камер, имеющих стандартные логины и пароли, которые известны многим людям, использование

[1] О полиции: федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 21.12.2021) // СЗ РФ. 2011. № 7, ст. 900.

[2] Об оперативно-розыскной деятельности: федеральный закон от 12 августа 1995 г. № 144-ФЗ (в ред. от 01.07.2021) // СЗ РФ. 1995. № 33, ст. 3349.

обновленного программного обеспечения и изменение логинов и паролей является обязательным для обеспечения безопасности.

© Тихонов Т. А., 2023

Библиографический список:

1. Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р (ред. от 05.04.2019) // Справочно-правовая система «Гарант». URL: http://www.garant.ru/hotlaw/federal/303815/ (дата обращения: 15.06.2022).

2. Алябьев А. А., Лагуточкин А. В. Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет // ППД. – 2013. – № 1. – URL: https://cyberleninka.ru/article/n/problemy-osuschestvleniya-operativno-rozysknyh-meropriyatiy-v-informatsionnom-prostranstve-seti-internet (дата обращения: 15.06.2022).

3. Дубоносов Е. С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения // Известия Тульсого государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – URL: https://cyberleninka.ru/article/n/operativno-rozysknoe-meropriyatie-poluchenie-kompyuternoy-informatsii-soderzhanie-i-problemy-provedeniya (дата обращения: 03.03.2023).

4. Лагуточкин А. В., Ковтун Ю. А. О нормативно-правовом совершенствовании деятельности оперативных подразделений в условиях современного вызова цифровых технологий // Вестник Белгородского юридического института МВД России. – 2021. – № 4. – URL: https://cyberleninka.ru/article/n/o-normativno-pravovom-sovershenstvovanii-deyatelnosti-operativnyh-podrazdeleniy-v-usloviyah-sovremennogo-vyzova-tsifrovyh (дата обращения: 15.06.2022).

5. Олифер В., Олифер Н., Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – 6-е изд. – Санкт-Петербург: Питер, 2020. – 1008 с.

6. О «Безопасном городе» // АПК «Безопасный город» [Сайт]. – URL: https://apkbg.info/about/ (дата обращения: 27.05.2022).

7. Павлюков В. В. Практические способы получения и использования результатов оперативно-розыскного мероприятия "получение компьютерной информации» // Вестник Костромского государственного университета. – 2020. – № 3. – URL: https://cyberleninka.ru/article/n/prakticheskie-sposoby-polucheniya-i-ispolzovaniya-rezultatov-operativno-rozysknogo-meropriyatiya-poluchenie-kompyuternoy (дата обращения: 15.06.2022).

8. Петроченков С. Д. Информационные технологии как современный фактор развития оперативно-розыскной деятельности // Научный компонент. – 2020. – № 3 (7). – URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-kak-sovremennyy-faktorrazvitiya-operativno-rozysknoy-deyatelnosti (дата обращения: 15.06.2022).

ТУРЧИН ДЕНИС АНДРЕЕВИЧ

слушатель факультета подготовки сотрудников
для оперативных подразделений
Санкт-Петербургский университет МВД России

Научный руководитель:
АКИЕВ АРБИ РУСЛАНОВИЧ

начальник кафедры криминалистики
Санкт-Петербургский университет МВД России
кандидат юридических наук

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ МВД РОССИИ

Аннотация. *В данной статье рассматривается один из методов защиты информации от несанкционированного доступа на объектах информатизации МВД России по техническим каналам утечки информации.*

Ключевые слова: *методы защиты информации, несанкционированный доступ, технические каналы утечки информации, техническая защита информации*

Согласно федеральному закону «Об информации, информационных технологиях и о защите информации»[1] защита информации реализуется путем применения совокупности трех мер, а именно: правовых, организационных и технических. В рамках данной работы внимание будет уделено именно техническим мерам, поскольку в ходе проведения преддипломной практики была выявлена новая угроза — строительство высокоэтажного здания в непосредственной близости к зданию территориального органа МВД России, что создает угрозу несанкционированного получения различных сведений по виброакустическим каналам утечки информации.

Для обеспечения надежной защиты информации от несанкционированного доступа, а именно от утечки информации по виброакустическим каналам, необходимо выбрать наиболее подходящее техническое средство защиты информации. Мною были выбраны следующие критерии для выбора средств защиты информации:

– устройства должны обеспечивать защиту от утечки информации по виброакустическому каналу связи;

– устройства должны иметь актуальную лицензию ФСТЭК;

– устройства должны иметь полную информацию о себе в доступных источниках.

В ходе поиска в Государственном реестре сертифицированных средств защиты информации были выбраны 22 средства защиты информации, но в виду того, что у 14 устройств

[1] Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 28.06.2022) // СЗ РФ 2006. № 31 (ч. I), ст. 3448.

не было актуальной лицензии или доступной информации в открытых источниках, был сделан выбор в пользу оставшихся восьми средств защиты информации.

Ими стали:

– генератор шума «ЛГШ-408»;

– система виброакустической защиты «Камертон-5»;

– система активной акустической и вибрационной защиты «ШТОРМ-10»;

– система виброакустической защиты «Гамма СВАЗ-01»;

– генератор акустических и виброакустических помех «Вуаль»;

– система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б;

– система «Шорох-5Л»;

– система акустических и виброакустических помех «БУРАН».

Выбор наиболее подходящего средства защиты информации осуществлялся по следующим пунктам:

– обеспечение защиты по виброакустическим каналам связи;

– обеспечение защиты через оптико-электронные каналы связи;

– возможность использование в выделенных помещениях до 1 категории включительно;

– наличие актуального сертификата;

– наличие доступной рабочей документации на изделие.

В ходе анализа и сравнения восьми средств защиты информации от несанкционированного доступа по виброакустический каналам связи было выбрано устройство — система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б, так как она соответствовала всем установленным пунктам выбора необходимого нам средства:

– устройство обеспечивает защиту информации по виброакустическим каналам связи;

– устройство обеспечивает защиту по оптико-электронным каналам связи;

– устройство можно использовать в выделенных помещения до 1 категории включительно;

– устройства имеется актуальный сертификат ФСТЭК (до 20.09.2024);

– устройство имеет в открытом доступе наиболее полную рабочую документацию по настройке и установке в выбранное помещение.

Для установки и настройке системы активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б необходимо изучить: руководство по эксплуатации ЮДИН 665230.010-01 РЭ и руководство по эксплуатации ЮДИН 665230.010 РЭ. Оба документа доступно и полно раскрывают все нюансы работы с данным средством защиты информации.

В результате анализа множества технических средств для защиты информации от утечки по виброакустическим каналам связи мною было выбрано одно устройство, удовлетворяющее все критерии отбора — система активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б. Технические специалисты территориальных органов МВД России могут использовать данное устройство для защиты объектов информатизации от несанкционированного доступа и утечки информации по виброакустическим каналам связи.

© Турчин Д. А., 2023

Библиографический список:

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 28.05.2019) // Зарегистрировано в Минюсте России. – 2013. – 31 мая. – № 28608. – Справочно-правовая система «Гарант». – URL: https://www.garant.ru.

2 Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств: приказ МВД от 31 декабря 2014 г. № 1152 (ред. от 06.02.2018) // Справочно-правовая система «Гарант». – URL: https://www.garant.ru.

3. О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: приказ МВД России от 9 ноября 2018 г. № 755 // Справочно-правовая система «Гарант». – URL: https://www.garant.ru.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 (ред. от 14.05.2020) // Зарегистрировано в Минюсте России. – 2013. – 14 мая. – № 28375. – Справочно-правовая система «Гарант». – URL: https://www.garant.ru.

5. Меры защиты информации в государственных информационных системах: методический документ (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.). // Справочно-правовая система «Гарант». – URL: https://www.garant.ru/.

6. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации Государственный реестр сертифицированных средств защиты информации: руководящий документ (утв. Решением Государственной технической комиссии при Президенте Российской Федерации 30 марта 1992 г.) (ред. от 14.05.2020) / Справочно-правовая система «Гарант». – URL: https://www.garant.ru/.

7. ГОСТ Р 78.36.052-2015. Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к первой категории (Методические рекомендации). – Москва: НИЦ «Охрана», 2015. – 192 с.

8. Руководство по эксплуатации ЮДИН.665230.010-01 РЭ. – URL: http://www.cbi-info.ru/files/sonata-av3m.pdf.

9. Куватов В. И. Программно-аппаратная защита информации: курс лекций / В. И. Куватов, О. Е. Чудаков, В. Н. Родин. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2020. – 192 с.

ЧЕРНЫШЕВА МАРИЯ ИГОРЕВНА

слушатель факультета подготовки
сотрудников для оперативных подразделений
Санкт-Петербургский университет МВД России

Научный руководитель:
БАДЗАГРАДЗЕ ТАТЬЯНА АЛЕКСАНДРОВНА

заместитель начальника кафедры криминалистики
Санкт-Петербургский университет МВД России
кандидат юридических наук, доцент

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ СПЕЦИАЛЬНЫХ И БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ТО МВД РОССИИ

Аннотация. *В статье рассмотрена проблема защиты специальных и биометрических персональных данных, обрабатываемых в информационных системах ТО МВД России. Описана разработка системы защиты, включающая в себя расчет уровня информационного риска с использованием соответствующей формулы. Результаты расчетов могут быть использованы для определения приоритетов в области информационной безопасности и для принятия решений по разработке и внедрению соответствующих мер по защите информации.*

Ключевые слова: *информационная безопасность, персональные данные, система защиты, информационный риск, МВД России*

Современные информационные технологии играют важную роль в обеспечении безопасности граждан и правопорядка. Однако, при использовании информационных систем в ТО МВД России, существует риск несанкционированного доступа к специальным и биометрическим персональным данным, что может привести к серьезным последствиям. Для того чтобы обеспечить безопасность обработки данных, необходимо разработать систему защиты, которая учитывает все возможные угрозы и риски.

Одним из ключевых аспектов при разработке системы защиты является определение уровня информационного риска. Уровень информационного риска — это степень вероятности потери или утечки информации, а также возможный ущерб, который может быть нанесен организации в результате реализации угрозы.

Формула для расчета уровня информационного риска выглядит следующим образом:

$$R = P_{нсд} \times (K_{пом} + K_{сп} + K_{итз} + (K_{ао}/3 + K_{по}/3 + K_{кс}/3)) \times S_{у}, \quad (1)$$

где: R — уровень информационного риска;

$P_{нсд}$ — вероятность реализации несанкционированного доступа к информации подразделения;

$K_{пом}$ — коэффициент степени недостаточности правовых и организационных мер;

$K_{сп}$ — коэффициент степени уязвимости сотрудников подразделения;

$K_{итз}$ — коэффициент степени уязвимости инженерно-технической защищенности подразделения;

$K_{ао}$ — коэффициент степени уязвимости аппаратного обеспечения;

$K_{по}$ — коэффициент степени уязвимости программного обеспечения;

$K_{кс}$ — коэффициент степени уязвимости каналов связи и каналов передачи данных;

$S_{у}$ — предполагаемый ущерб от реализации угрозы.

Давайте подробнее рассмотрим каждый из параметров в формуле.

$P_{нсд}$ — вероятность реализации несанкционированного доступа к информации подразделения. Для оценки этого параметра, необходимо проанализировать все возможные угрозы и применить методы анализа рисков. Чем выше вероятность несанкционированного доступа, тем выше уровень информационного риска.

$K_{пом}$ — коэффициент степени недостаточности правовых и организационных мер. Этот коэффициент оценивает степень защищенности информационной системы от угроз, связанных с недостатком правовых и организационных мер. Например, это может быть отсутствие политик и процедур по управлению доступом к информации, недостаточная квалификация персонала, отсутствие обучения сотрудников по вопросам безопасности информации.

$K_{сп}$ — коэффициент степени уязвимости сотрудников подразделения. Этот коэффициент оценивает степень уязвимости информационной системы в связи с возможными ошибками, допущенными сотрудниками подразделения. Например, это может быть использование слабых паролей, отсутствие двухфакторной аутентификации, фишинговые атаки.

$K_{итз}$ — коэффициент степени уязвимости инженерно-технической защищенности подразделения. Этот коэффициент оценивает степень защищенности информационной системы от угроз, связанных с возможными недостатками инженерно-технических средств защиты. Например, это может быть недостаточная защищенность сетевых портов, недостаточное обновление программного обеспечения, уязвимости в операционной системе.

$K_{ао}$ — коэффициент степени уязвимости аппаратного обеспечения. Этот коэффициент оценивает степень уязвимости информационной системы в связи с возможными недостатками аппаратного обеспечения. Например, это может быть использование устаревшего оборудования, которое не поддерживает современные методы шифрования.

$K_{по}$ — коэффициент степени уязвимости программного обеспечения. Этот коэффициент оценивает степень уязвимости информационной системы в связи с возможными недостатками программного обеспечения. Например, это может быть использование устаревших версий программного обеспечения, которые имеют известные уязвимости.

$K_{кс}$ — коэффициент степени уязвимости каналов связи и каналов передачи данных, учитывает вероятность

риска, связанного с возможным несанкционированным доступом к информации в процессе ее передачи по сети. Это включает в себя уязвимости, связанные с сетевыми протоколами, конфигурацией сетевого оборудования, недостаточной защитой от сниффинга (перехвата) трафика и другими факторами.

S_y — предполагаемый ущерб от реализации угрозы, определяется в соответствии с потенциальными последствиями утечки или несанкционированного доступа к конфиденциальной информации. Это может включать потерю имущества, нарушение конфиденциальности, нарушение репутации организации и другие негативные последствия.

Таким образом, формула для расчета уровня информационного риска может быть использована при разработке системы защиты специальных и биометрических персональных данных обрабатываемых в информационных системах ТО МВД России. Результаты расчетов могут быть использованы для определения приоритетов в области информационной безопасности, а также для принятия решений по разработке и внедрению соответствующих мер по защите информации.

© Чернышева М. И., 2023

Библиографический список:

1. Бабаев А. А. Анализ уязвимостей системы информационной безопасности / А. А. Бабаев, А. В. Шутов // Проблемы защиты информации. – 2019. – № 1 (27). – С. 32–37.

2. Камалов А. Х. Проблемы защиты информации в информационно-телекоммуникационной инфраструктуре / А. Х. Камалов, А. В. Лямина // Вестник Башкирского государственного университета. – 2022. – № 1. – С. 72–77.

3. Литвинова Е. А. Разработка системы защиты информации в организации / Е. А. Литвинова, Н. В. Белоусова // Международный журнал прикладных и фундаментальных исследований. – 2020. – № 4-1. – С. 90–92.

4. Маслова Е. Н. Организация системы защиты персональных данных в государственных учреждениях / Е. Н. Маслова, О. С. Чеснокова // Информационные технологии в науке, управлении, социальной сфере и медицине. – 2023. – № 1 (11). – С. 28–33.

5. Савченко А. В. Анализ уязвимостей системы информационной безопасности на основе метода анализа иерархий / А. В. Савченко, А. А. Жуков // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – № 1 (119). – С. 54–59.

Научное электронное издание

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Материалы
международной научно-практической конференции

11–12 мая 2023 года

Составитель:
Подружкина Т. А.,
кандидат педагогических наук, доцент

Публикуется в авторской редакции

Дизайн обложки
Шеряй Александр Николаевич

Системные требования: ПК с процессором Intel Core i3 и более; 512 Mb и более; CD/DVD — ROM дисковод; Microsoft Windows XP и выше; SVGA 800×600 .16 bit и более; Internet Explorer; Adobe Acrobat Reader 8.0.

978-5-91837-812-0

EDN: VBZZQD

Подписано к использованию 20.12.2023.
Объем 3,84 усл. авт. л. Заказ № 158/23. Тираж 100 экз.
Санкт-Петербургский университет МВД России
198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1