Следственное управление Следственного комитета РФ по Липецкой области

Липецкий филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ»

ФГБОУ ВО «Липецкий государственный технический университет»

СОВРЕМЕННЫЕ ВЫЗОВЫ И МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

СБОРНИК
материалов всероссийской научно-практической конференции с международным участием
приуроченной ко Дню образования Следственного комитета Российской Федерации

17 января 2025 года

Липецк – 2025

УДК 343.3 (063)
ББК 67.408.135л0
С56

Рецензенты:
д-р юрид. наук, профессор, профессор кафедры уголовного права и криминологии, Заслуженный юрист Российской Федерации, академик Академии педагогических и социальных наук, член-корреспондент Академии Российской словесности, академик Международной славянской академии наук, образования, искусств и культуры *Ю.И. Голик;*
д-р. юрид наук, доцент, ведущий научный сотрудник сектора административного права и административного процесса ИГП РАН *Т.В. Щукина*

Современные вызовы и механизмы противодействия киберпреступности: сборник материалов всероссийской научно-практической конференции с международным участием (г. Липецк, 17 января 2025 г.) / под общ. ред. В.А. Брусенцевой, Е.В. Шаповалова. – Воронеж: НАУКА-ЮНИПРЕСС, 2025. – 220 с.
ISBN 978-5-4292-3279-9

Материалы сборника научных трудов участников всероссийской научно-практической конференции «Современные вызовы и механизмы противодействия киберпреступности», состоявшейся 17 января 2025 г. в г. Липецке, посвящены рассмотрению вопросов повышения эффективности противодействия киберпреступности, её выявлению, раскрытию и расследованию. В сборнике представлены исследования представителей органов государственной власти, правоохранительных органов, профессорско-преподавательского состава, докторантов, аспирантов и специалистов.

Сборник предназначен для широкого круга читателей: ученых, специалистов-практиков, аспирантов, студентов.

Опубликованные материалы представлены в авторской редакции.

УДК 343.3 (063)
ББК 67.408.135л0

ISBN 978-5-4292-3279-9



© Коллектив авторов, 2025
© Липецкий филиал РАНХиГС, 2025
© НАУКА-ЮНИПРЕСС, 2025

СОДЕРЖАНИЕ

Абубакирова Г.М.
Современные вызовы кибермошенничества с использованием криптоволют и цифровых активов **7**

Анютина А.А.
Сравнительный анализ способов выявления, расследования и раскрытия киберпреступлений в российском и зарубежном праве 11

Anyanova E.S.
Cybersecurity at sea 14

Бардачевский Р.И.
О необходимости оптимизации уголовно-процессуальных инструментов, направленной на повышение оперативности изъятия средств совершения киберпреступлений 21

Бодров Н.Ф., Лебедева А.К.
Криминалистическое противодействие распространению дипфейков 23

Бородин Д.В.
Тестирование веб-приложений на базе CMS «1С-Битрикс: Управление сайтом» для предупреждения киберпреступлений. 27

Брусенцева В.А.
Современные угрозы безопасности несовершеннолетних в сети Интернет 32

Галкин Д.В.
Цифровые технологии в расследовании преступлений, связанных с автомобильным транспортом. 37

Говорухин Д.С.,
Совершенствование деятельности органов внутренних дел в сфере борьбы с преступлениями, совершенными с использованием информационно-коммуникационных технологий 42

Голубовский В.Ю.
Противодействие современным киберугрозам 51

Дук Ю.И.
Киберпреступность в России: пути противодействия 54

Дягилев А.А., Раскатов Р.А.
Противодействие вовлечению несовершеннолетних в противоправную деятельность с использованием сети Интернет 62

Егоров В.А.
Компетенция уголовно-исполнительных инспекций при проведении электронного мониторинга в отношении поднадзорных лиц 66

Захарова А.Д.
Международно-правовое регулирование правового статуса ребенка, в условиях современных вызовов и угроз 74

Зиганшин Т.Р.
Возможности применения специальных знаний при производстве расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий 81

Зуев С.В.
Администрирование в цифровом уголовном процессе как высшая форма организации работы органов расследования и суда 88

Изотова В.Ф.
Проблемы противодействия несанкционированному распространению персональных данных в киберпространстве 92

Иовлева А.С.
Применение меры пресечения в виде запрета определенных действий при расследовании киберпреступлений 97

Клементьева Е.С., Мишуков Я.О.
Новые подходы в уголовно-правовой охране права на неприкосновенность частной жизни в интернет-пространстве 102

Климов А.С.
Особенности совершенствования уголовного законодательства, предусматривающего ответственность за киберпреступления . . . 108

Кочкина М.С.
Предупреждение онлайн-груминга несовершеннолетних в сети Интернет 112

Корнев А.С.
К вопросу выявления, раскрытия и расследования преступлений, совершенных с помощью искусственного интеллекта 114

Кузнецов А.А.
Понятие цифровых доказательств 117

Кунц Е.В.
Стратегия по предотвращению преступлений в кибепространстве 123

Левашова О.В.
Проблемы и перспективы совершенствования норм уголовного законодательства о кибербезопасности 126

Матвеев А.В.
Роль органов внутренних дел Российской Федерации в противодействии киберпреступности 138

Пестрецов И.О.
Способ противодействия киберпреступности в условиях прекращения уголовного дела и уголовного преследования в отношении участника СВО 143

Польшиков А.В., Пучнина М.Ю.
Противодействие вовлечению в проституцию несовершеннолетних посредством использования сети Интернет 148

Скобелин С.Ю.
Криминалистическая характеристика преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием информационных технологий 152

Солодина С.А.
О некоторых вопросах использования азартных игр в сети «Интернет» для отмывания денежных средств, приобретенных преступным путем 160

Соломонова В.В.
Киберпреступность в современной России: масштабы и последствия 164

Татаринова А.С.
Предупреждение преступности в сфере информационно-телекоммуникационного пространства 168

Тетерина М.Н.
Правовые аспекты кибербезопасности в банковском секторе 171

Толочко А.В., Толочко Н.С.
Современные информационно-коммуникационные технологии в образовательном процессе как средства противодействия киберпреступности 176

Уздемир А.Н.
Основные риски и предупреждение кибератак в банковском секторе 181

Утегенова Г.А.
Интерактивные развлечения как фактор, способствующий семейно-бытовому насилию: анализ и меры предупреждения 186

Утузикова Т.А.
Профилактика и предупреждение киберпреступлений среди молодежи: роль государственной молодежной политики 192

Фалахеева А.Г.
Особенности участия защитника по уголовным делам в отношении отдельных категорий лиц 196

Хайрусов Д.С.
Некоторые аспекты криминалистической профилактики деятельности «телефонных» мошенников и подстрекателей 203

Чеботарев Д.Д., Кузнецова Н.Н.
К вопросу о применении искусственного интеллекта при противодействии киберпреступности 206

Шагунова В.М.
Особенности расследования преступлений в сфере экономической деятельности, совершаемых в киберпространстве 210

Шаповалов Е.В.
Киберпреступность: проблемы практики расследования 215

Абубакирова Г.М., аспирант
Кыргызская Республика, Юридического институт Кыргызского
Национального университета имени Ж. Баласагына,
г. Бишкек

СОВРЕМЕННЫЕ ВЫЗОВЫ КИБЕРМОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ КРИПТОВОЛЮТ И ЦИФРОВЫХ АКТИВОВ

Аннотация

Статья посвящена анализу современных вызовов, связанных с кибермошенничеством, использующим криптовалюты и цифровых активов. Рассмотрены основные схемы кибермошенничества, такие как фейковые криптовалютные биржи, фиктивная техподдержка, фальшивые криптоинвестиции и криптошантаж, их влияние на экономическую безопасность пользователей и защиту персональных данных. Предложены меры профилактики, включая усиление правового регулирования, повышение финансовой грамотности и внедрение современных технологий аутентификации. Особое внимание уделено необходимости разработки строгих законов для стран Содружества Независимых Государств.

Ключевые слова: кибермошенничество; криптовалюты; цифровые активы; цифровая безопасность; правовое регулирование.

Криптовалюта представляет собой современную электронную платежную систему, которая работает без участия банков или посредников для подтверждения транзакций [1]. Она основана на одноранговой сети, обеспечивающей возможность мгновенных переводов между пользователями в любой точке мира и в любое время. Криптовалюта активно используется для различных целей, включая бизнес, торговлю, инвестиции и покупки в интернете. Также, ее можно обменивать на обычные деньги, приобретать, хранить и тратить с помощью криптографических кошельков.

Криптовалюта представляет собой уникальный вид цифровой валюты, который отличается от традиционных валют рядом ключевых особенностей [2]. Криптовалюта обладает рядом уникальных характеристик, которые отличают ее от традиционных финансовых систем. Она адаптивна и может эффективно функционировать как в масштабных, так и в локальных операциях. Создаваясь исключительно из программного кода, криптовалюта является виртуальной и не имеет физической формы. Ее децентрализация гарантируется одноранговой сетью, что исключает контроль со стороны центральных органов власти. Кроме того, криптовалюта полностью цифровая и существует исклю-

чительно в электронном формате. Благодаря открытому исходному коду разработчики имеют возможность создавать новые криптовалюты без значительных финансовых вложений, что стимулирует инновации в этой области [3].

Хотя криптовалюта обладает рядом уникальных особенностей, однако она имеет и значительные уязвимости. Поскольку криптовалюты хранятся в цифровых кошельках, они подвержены риску взлома и кибермошенничества. Вышеуказанные характеристики делают криптовалюту инновационным инструментом, который предоставляет новые возможности для финансового взаимодействия, но одновременно создает сложности в регулировании и использовании. В результате криптовалюта становится важным объектом научного исследования, особенно в области правового регулирования и обеспечения безопасности пользователей в цифровой среде.

На сегодняшний день существует множество известных видов кибермошенничества, связанных с использованием криптовалют. Рассмотрим наиболее распространенные из них.

Фиктивная техподдержки – одна из самых распространенных форм кибермошенничества, при которой злоумышленники выдают себя за представителей службы поддержки [4]. Пользователи попадают в ловушку, нажимая на фальшивые всплывающие окна или посещая поддельные сайты. Кибермошенники убеждают жертв, что их устройство якобы неисправно и требует немедленного ремонта, угрожая возможным повреждением. Взамен предлагают оплатить «устранение проблемы» или заработать криптовалюту, хотя на самом деле неисправности не существует. Оплата производится методами, которые сложно отследить и не обеспечивают защиты потребителей. Часто кибермошенники также получают доступ к устройству жертвы и крадут конфиденциальные данные, включая банковские реквизиты, пароли и личную информацию, что приводит к значительным финансовым и репутационным потерям.

Фейковые криптовалютные биржи представляют собой серьезную угрозу для пользователей, поскольку их деятельность связана с кибермошенничеством, включая кражу средств, отказ в выводе активов и использование фишинговых схем [5]. Такие платформы маскируются под настоящие, используя поддельные URL-адреса, которые визуально похожи на оригинальные, что затрудняет их распознавание. Злоумышленники создают фишинговые сайты, собирая конфиденциальные данные пользователей, включая пароли и финансовую информацию. Данные поддельные биржи отказывают в выводе средств, взимают завышенные комиссии или напрямую крадут криптовалюту пользователей.

Подобная деятельность не только подрывает доверие к криптовалютным платформам, но и нарушает права пользователей, включая их финансовую и информационную безопасность.

Криптошантаж - представляет собой форму кибермошенничества, при которой злоумышленники требуют перевести деньги на их криптовалютный адрес под угрозой раскрытия компрометирующей информации [6]. Чаще всего в таких письмах утверждается, что у кибермошенников есть данные о посещении пользователем порнографических сайтов или что его устройство заражено вирусом. Вымогатели требуют выкуп, угрожая раскрыть личные данные, если жертва не предоставит приватные ключи или не переведет средства в криптовалюте. Одним из примеров является вредоносная программа MyloBot, которая заражает устройства, рассылает шантажирующие письма и требует выкуп в биткоинах. Если пользователь ответит на письмо, перейдет по ссылке или откроет вложение, злоумышленники могут получить доступ к его устройству и данным. Этот вид киберпреступлений становится особенно опасным, когда кибермошенники делают свои угрозы максимально убедительными, используя страх и манипуляции для достижения своих целей.

Кибермошенничество с фальшивыми криптоинвестициями является одним из распространенных видов киберпреступлений, связанных с криптоактивами. Злоумышленники убеждают людей инвестировать в поддельные криптопроекты, обещая высокую прибыль и подкрепляя свои заявления фальшивыми отзывами [7]. После внесения средств инвесторы теряют свои деньги, так как средства исчезают. Кибермошенники предлагают программы с гарантированной доходностью или платформы для майнинга, которые на деле не имеют никакой реальной ценности. Для усиления доверия они убеждают жертв в перспективности неизвестных монет и предлагают приобрести поддельный проект. Часто злоумышленники отправляют ссылки на сайты, содержащие вредоносное ПО, чтобы получить доступ к личным данным, паролям и кошелькам пользователей. Также жертвам могут направлять письма с просьбой перезагрузить криптоинвестиционный счет, угрожая блокировкой аккаунта. После перехода по таким ссылкам кибермошенники получают доступ к конфиденциальной информации, что приводит к значительным финансовым потерям.

На основании вышеизложенного необходимо отметить, что конфиденциальность пользователей в социальных сетях стремительно уменьшается, что делает данную проблему одной из ключевых в условиях цифровой эпохи. Социальные сети, благодаря их широкой популярности и доступности, становятся удобной площадкой для кибер-

мошенников, которые используют их для продвижения различных схем, включая кибермошенничество с использованием криптоактивов. Киберпреступники часто применяют несанкционированные изображения известных личностей, таких как знаменитости и успешные бизнесмены, чтобы создать иллюзию легитимности и вызвать доверие у потенциальных жертв. Это подрывает не только безопасность пользователей, но и их уверенность в цифровой среде. Угроза усугубляется отсутствием строгих правовых норм, направленных на предотвращение подобных действий, а также недостаточным уровнем цифровой грамотности у многих пользователей. Таким образом, проблема требует комплексного подхода, включающего разработку эффективных законодательных мер, усиление защиты персональных данных и проведение просветительских мероприятий, направленных на повышение осведомленности пользователей о рисках и способах защиты.

В заключение следует подчеркнуть, что минимизация рисков, связанных с использованием криптовалют, требует от пользователей соблюдения базовых мер безопасности. Во-первых, важно проверять подлинность приложений перед их использованием, начиная с отправки небольших сумм для тестирования. Во-вторых, рекомендуется регулярно менять пароли, включать двухфакторную аутентификацию и не передавать данные криптокошелька третьим лицам. В-третьих, переходя по ссылкам, необходимо проверять наличие протокола «https», свидетельствующего о безопасности ресурса. Осведомленность инвесторов и соблюдение этих простых, но эффективных мер помогут предотвратить финансовые потери и обеспечить защиту личных данных. Однако, учитывая растущие угрозы кибермошенничества, особенно на территории стран Содружества Независимых Государств, требуется срочное принятие строгих правовых норм, регулирующих использование криптоактивов и направленных на противодействие мошенническим схемам в цифровой среде.

Список цитируемой литературы:

1. Криптовалюта [Электронный ресурс]. – Википедия: свободная энциклопедия. – URL: https://ru.wikipedia.org/wiki/Криптовалюта (дата обращения: 07.12.2024)
2. Осипова, В.С. Цифровая валюта. Отличие криптовалюты от цифровой валюты/ В.С. Осипова // Almanac Crimea. Economics, innovation. Региональные и международные исследования. – 2024. – № 42. – С. 113–119.
3. Пашкова, В.Д., Иваницкий, Д.К. Особенности регулирования криптовалют в международной практике / В.Д. Пашкова, Д.К. Иваницкий //

Международный научный журнал «Вестник науки». – 2023. – № 5 (62). – Т. 1. – С. 68–74.
4. Ложная техподдержка. [Электронный ресурс]. – Энциклопедия «Касперского». Глоссарий. — URL: https://encyclopedia.kaspersky.ru/glossary/technical-support-scam/ (дата обращения: 10.12.2024)
5. DexCoyote Foundation. Остерегайтесь фейковых криптовалютных бирж: как избежать мошенничества. [Электронный ресурс]. – URL: https://www.binance.com/ru/square/post/725218 (дата обращения: 10.12.2024)
6. Rabotnik сел за криптошантаж, Dropbox упустил секретные ключи и другие события кибербезопасности [Электронный ресурс]. – URL: https://forklog.com/news/rabotnik-sel-za-kriptoshantazh-dropbox-upustil-sekretnye-klyuchi-i-drugie-sobytiya-kiberbezopasnosti (дата обращения: 10.12.2024)
7. Инвестиционное мошенничество. Генеральный прокурор Нью Йорка. [Электронный ресурс]. – URL: https://ru.ag.ny.gov/resources/individuals/investing-finance/investment-fraud (дата обращения: 11.12.2024)

Анютина А.А., магистр
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Научный руководитель – Соловьева В.В. д-р ист. наук, профессор
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПОСОБОВ ВЫЯВЛЕНИЯ, РАССЛЕДОВАНИЯ И РАСКРЫТИЯ КИБЕРПРЕСТУПЛЕНИЙ В РОССИЙСКОМ И ЗАРУБЕЖНОМ ПРАВЕ

Аннотация

Целью данного исследования выступает изучение вопросов, связанных с анализом российского и международного законодательного регулирования кибертеррористических преступлений. В статье рассматривается анализ способов выявления кибепреступлений, связанных с высоким ростом угроз на данные, находящиеся на хранении и использовании в киберпространстве. Также в статье будет проведен сравнительный анализ правовых систем России и мира, направленных на борьбу с кибермошенниками и защиту данных в сети «Интернет».

Ключевые слова: преступление, киберпреступность, сеть «Интернет», мошенничество, злоумышленник, компьютерная безопасность, уголовное законодательство, международные акты по кибербезопасности.

Следует отметить, что в современной системе в 1950-х и 1990-х годах кибератак не существовало в том виде, в каком мы знаем их сегодня. Это относительно новые явления, которые появились с развитием технологий и оцифровкой общества. Однако в целом информационная безопасность в то время не была серьезной проблемой, поскольку использование компьютеров и Интернета все еще было относительно ограниченным. Однако имели место некоторые инциденты, связанные с безопасностью, и киберпреступности, которые сыграли важную роль в развитии информационной безопасности и повышении осведомленности о проблеме.

Современное уголовное законодательство сталкивается со значительными вызовами в отношении киберпреступности или киберпреступного поведения, учитывая быстрое развитие технологий и использование Интернета. Киберпреступность включает в себя незаконные действия, совершаемые в виртуальной среде, такие как онлайн-мошенничество, несанкционированный доступ к компьютерным системам, кибер-саботаж или распространение незаконного контента. В последнее время наблюдается значительный рост кибератак, краж личных данных и утечек данных с использованием передовых технологий, чтобы получить доступ к конфиденциальной информации и причинить вред отдельным лицам и организациям [2, С. 44].

В современном уголовном праве киберпреступность охватывает широкий спектр видов деятельности. С одной стороны, это преступления, связанные с существенным нарушением личной или корпоративной неприкосновенности, такие как: посягательства на целостность хранилищ информации и использование незаконно полученной цифровой информации для шантажа компании или частного лица. Другая часть преступлений такого рода связана с тем, что отдельные лица из корпораций или государственных структур намеренно изменяют данные либо для получения прибыли, либо в политических целях. На другом конце спектра находятся преступления, которые связаны с попытками нарушить реальное функционирование Интернета. Они варьируются от рассылки спама, взлома и атак на определенные веб-сайты с использованием служб безопасности до кибертерроризма, использования Интернета для организации общественных беспорядков и даже смертей.

Примеры киберпреступлений включают доступ к компьютерным системам, кражу данных или личных данных, онлайн-мошенничество,

онлайн-домогательства и другие виды преступлений, связанные с использованием технологий, фишинг (получение личной информации мошенническими методами), атаки программ-вымогателей (блокирование или шифрование данных с требованием выкупа), кражу личных данных (мошенническим путем получение и использование личной информации другого лица) или DDoS-атак (отказ в обслуживании). Эти преступления часто трудно обнаружить и отследить, поскольку преступники могут действовать из любой точки мира и использовать изощренные методы, чтобы скрыть свои следы. Современная система уголовного права основана на идее о том, что преступления должны караться мерами наказания, соразмерными их тяжести, и что правосудие должно применяться объективно и беспристрастно.

В последние годы криминальные системы по всему миру начали адаптироваться к новым угрозам, исходящим от киберпреступности. Были разработаны новые законы и правила борьбы с киберпреступностью, и правоохранительные органы начали расширять свои возможности по расследованию киберпреступлений и судебному преследованию за них.

Согласно Всемирному индексу киберпреступности за 2024 год, Россия является страной происхождения большинства киберпреступлений. За ними следуют Украина и Китай. В пятерку также входят США и Нигерия. В то же время российские хакеры оказались лидерами рейтинга, в том числе по сложности используемых технологий.

В России предусмотрена уголовная ответственность за киберпреступления (глава 28 УК РФ «Преступления в сфере компьютерной информации»). За рубежом подход к борьбе с киберпреступностью может отличаться. Например, в Германии эта проблема широко решается на государственном уровне с целью обеспечения общей цифровой среды, безопасности государства в информационном пространстве и безопасности экономики страны. Япония разработала собственную классификацию киберпреступлений, которая позволяет определить определенный вид преступности в секторе высоких технологий [1, С. 144].

В Соединенных Штатах штат быстро адаптирует свое законодательство к быстро меняющейся ситуации в преступном мире и постоянно ужесточает наказания за нарушения закона в этой области. В РОССИИ система уголовных санкций более мягкая: например, статья 159.6 УК РФ предусматривает максимальное наказание в виде ограничения свободы на срок до полутора лет и в соответствии с Кодексом США за это преступление, ущерб от которого составляет до полутора лет, за мошенничество в сфере компьютерной информации в особо крупном размере [3, С. 48].

Список цитируемой литературы:

1. Морозов, Н. А. Борьба с компьютерной преступностью / Н.А. Морозов // Общество и право. – 2014. – № 2. – С. 141-145.
2. Несмеянов, А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий / А. А. Несмеянов // Вестник Восточно-Сибирского института МВД России. – 2014. – № 4. – С. 43-48.
3. Рудик, М.В. Обзор уголовного законодательства западноевропейских стран и США в сфере создания с целью использования, распространения или сбыта вредных программных или технических средств / М. В. Рудик // Вестник КРУ МВД России. – 2015. – № 2. – С. 48-50.

Anyanova E.S., Candidate of Legal Sciences, LL.M,
Dr.iur (University of Hamburg, Germany)
legal adviser of the Limited Liability Company «BALTTORG»,
Kaliningrad

CYBERSECURITY AT SEA

Abstract

The threat of cyber-attacks is very acute. The purpose of this paper is to examine the need of the amendment of rules of international law required for the cyber resilient shipping.

Although some research is being conducted in this area, maritime cybersecurity has not been deeply investigated. This paper presents a detailed analysis of legal documents and research published on the law of cyber security for maritime industry highlighting security problems and challenges. The proposals of documents on cyber security and recommendations for maritime cyber risk management are discussed.

Keywords: maritime industry; shipping; cybersecurity; ports.

Introduction

The importance of cybersecurity is consistently emphasized. For example, as it is stressed by the scientists, cybersecurity is increasingly regarded as one of the fundamental problems of most countries [SHAISULTANOV et al., p. 258].

Cyber incidents damage ship operations, cause financial losses. Maritime cyber risk is a potential threat to damage shipping-related operations, safety or security systems, their information. The average maritime cyber incident takes approximately two months to resolve [DNV CYBER, 2024/2025, p. 21].

This paper will present the problem of cybersecurity threat for shipping. First, it explores cybersecurity concepts, cybersecurity risks and basics of the cyber risk management. Second, it assesses cyber attacks examples.

Then it will explore cyber security concept under the principles of international law addressing cyber attacks in shipping. In this study juridical methodology and tools help the analysis of legal concepts of information and communication technology [ARANHA, 2011, p. 11], especially the concept of maritime cyber security.

Finally, a series of recommendations are made for maritime cyber risk management.

CYBERSECURITY THREAT FOR SHIPPING

Cyber security means a security concept used to protect the cyber environment, organisation and user [CODE OF PRACTICE CYBER SECURITY FOR SHIPS, 2017]. Cyberthreats cover threats of cyber criminality, cyber espionage, cyber terrorism [SENARAK, 2021], phishing attacks redirecting legitimate payments.

Not being prepared for a cyber incident may result in the information systems being damaged. It may even have implications on the environment when the dangerous goods are transported [THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, VERSION 4, 2023].

CYBER ATTACKS EXAMPLES

The number of reported incidents of cyberattacks on the maritime industry increased in the last years. For example, in 2021 the U.S. Port of Houston was attacked. In March 2023, a malware attack targeted the Port of Antwerp-Bruges in Belgium [DUNLEVIE, 2023]. In 2023 the website of the port of Rotterdam was targeted in a cyberattack. Several Dutch ports including Amsterdam and Groningen were targeted by distributed-denial-of-service attacks (DDoS): the port of Amsterdam's website stopped its work, the work of Groningen Seaports was disrupted.

A hacker group with ties to China known as Mustang Panda attacked with USB sticks containing malware plugged into computers on numerous ships [Norwegian and Greek freighters, vessels in the Netherlands and Greece) [SUPPLYCHAINBRAIN, 2024].

In July 2017, the Danish shipping company in container transport "MAERSK" was attacked by the "NotPetya" ransomware. This malware had already attacked the Dutch company TNT Express in June 2017. The 'NotPetya' attack on Maersk caused loss approximately $300 million [DNV CYBER, 2023, p. 8].

In 2020 the Geneva HQ of shipping major like Mediterranean Shipping Company was attacked by a malware. As a result of this attack its customer website did not function for several days.

French container shipping major CMA CGM was also attacked by cyber-criminals in 2020 and 2021. In 2020 the cyber-attack of the Iran's Shahid Rajaee port in the Strait of Hormuz created traffic jams of delivery trucks and delays in shipments.

In 2022 Sea-Invest, one of the largest Belgian-based port terminals has shut down all operations due to a hacking attack.

In 2022 a Singapore shipbuilder Sembcorp Marine was attacked by an unauthorized user, who gained access to the IT network through third-party software [ANYANOVA, 2024, p. 73].

The website and internal computer system of the Port of Lisbon were disrupted in December 2022 and did not work for several days after a cyberattack.

Norwegian shipping classification society *Det Norske Veritas* [DNV CYBER, 2024/2025] was attacked by a ransomware attack in 2023 [MARITIME CYBERSECURITY ATTACKS ON THE RISE - MARPOINT, 2023]. The IMO was also attacked in 2020 and 2023. The Port of Los Angeles is constantly attacked by ransomware, malware and spear-phishing attacks.

The attack on a manufacturer of navigation systems Voyager Worldwide in April 2024 disabled the company's systems, that caused delays and unauthorized changes to their navigation routes (approximately 40 million cyberattack attempts each month) [DUNLEVIE, 2023].

On April 6, 2024, a coordinated cyber attack targeted several key maritime ports and vessels, causing widespread disruption. The attackers deployed ransomware and malicious software to cripple port operations and manipulate Automatic Identification Systems (AIS) on multiple ships, leading to substantial delays, misrouted cargo. The incident resulted in losses exceeding $500 million.

Major shipping companies like Maersk and CMA CGM had to reroute vessels and suspend certain operations temporarily. The Port of Rotterdam and the Port of Singapore faced disruptions in its cargo handling systems, which delayed the unloading and loading of vessels for several days.

The incident highlighted that many of these systems went outdated and are highly vulnerable to cyber threats.

Due to these incidents prevention of cyberattack became very important [SENARAK, 2021]. After the number of such incidents increased, the companies started to take offline e-commerce platforms and data centres [DNV CYBER, 2023, p. 8].

INTERNATIONAL LAW ADRESSING MARITIME CYBER ATTACKS

Documentary part of international law on cybersecurity in shipping is scarce. The issue of cyber security is a gap in the security of ships and port facilities.

Cybersecurity for the maritime industry is particularly addressed at international level since 2017 by means of such documents as guidelines and recommendations. However, there is no mandatory requirements.

The IMO's Guidelines on maritime cyber risk management were adopted in 2017 [IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2, 2022] and put into effect in 2021 in order to combat cyber threats in the shipping industry based on the International Safety Management (ISM) Code [PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023].

These guidelines recognize that all organizations in the shipping industry shall refer to Member Governments' and Flag Administrations' requirements and relevant international or industry standards and best practices (e.g. The Cybersecurity Framework 2.0 of the National Institute of Standards and Technology, ISO/IEC 27001 standard for information security management systems) in order to address the most relevant security measures.

The Resolution MSC.428(98) adopted by the Maritime Safety Committee (MSC) on 16 June 2017 concerns Maritime Cyber Risk Management in Safety Management Systems [IMO RESOLUTION MSC.428(98)].

Additional guidance and standards include the Guidelines on Cyber Security Onboard Ships. The document was produced and supported by the International Chamber of *Shipping* (*ICS*), the International Union of *Marine* Insurance e.V. (*IUMI*), Baltic and International *Maritime* Council (BIMCO), the Oil Companies International *Marine* Forum (*OCIMF*), the International Association of Indepedent Tanker Owners (*INTERTANKO*), the International Association of Dry Cargo Shipowners (*INTERCARGO*), International Ship Managers' Association (INTERMANAGER), the World *Shipping* Council (*WSC*), the Superyacht Builders Association (*SYBAss*).

The Cybersecurity Guidelines for Ports and Port Facilities were developed by the International Association of Ports and Harbors (IAPH) in 2021 [IAPH CYBERSECURITY GUIDELINES, 2023].

In order to ensure the security of port facilities against attacks from within the cyber domain, it is proposed to use the ISPS Code. The ISPS Code requires ports to design a Port Facility Security Assessment (PFSA) to identify possible threats and countermeasures and a Port Facility Security Plan (PFSP) to identify for different security levels the measures to be put

in place and the actions to be undertaken. The risk management activities in the ISPS Code cover mostly physical risks. The ISPS Code has two parts: a mandatory Part A and a recommendatory Part B. There are no cybersecurity provisions in Part A. Part B contains some regulations on computer systems and networks.

COUNTER MEASURES

Cyber security means a security concept used to protect the cyber environment, organisation and user [CODE OF PRACTICE CYBER SECURITY FOR SHIPS, 2017].

It is necessary to apply a risk management approach [IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT. MSC-FAL.1-Circ.3-Rev.2, 2022], since IT technologies are constantly changing.

The counter-measures shall be aimed at reducing the risk of unauthorised access to the ship including its cyber-physical systems. The protection from unauthorised access includes measures to check any removable media or portable devices that will be connected to the system for malware (for example, software updates on USB memory sticks or diagnostic software on laptops or tablet devices). Access to systems consoles, displays, etc. shall be password protected.

It is also proposed to develop new cybersecurity guidelines for maritime domain with the participation of the IMO. Sometimes the proposals are made to amend the ISPS Code and to cover cybersecurity standards for ports and port facilities [PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023].

In order to promote the cyber security management, the proposal was made to designate the cyber security officer (CySO). This CySO shall be responsible for all security aspects of cyber-enabled systems on the ship, i.e. both the IT and communications systems. The CySO should also be responsible for the development of the CSA/CSP and implementing the CSP.

Such position of CySO is introduced in certain places. For example, in the Rotterdam port the Port Security Officer has recently also been appointed Cyber Resilience Officer. However, this position is not required by the ISPS Code.

The International Maritime Cyber Security Organisation (IMCSO) was established in order to improve cybersecurity for the shipping [New Maritime Cybersecurity Body Launched, 2024[.

Some states (for example, Turkey, Bulgaria, Ukraine) conclude cybersecurity intelligence sharing agreements with each other [DUNLEVIE, 2023].

CONCLUSION

Nowadays the maritime industry has become increasingly vulnerable to cyber threats. This paper argues that recent examples from the shipping industry have demonstrated that cyber incidents have the potential to disturb ship operations and cargo management and cause significant financial losses, reputational damage.

The numerous cyber-attacks demonstrated the vulnerability of the maritime industry, for example, a cyberattack in 2020 at the Shahid Rajaee port in the Strait of Hormuz (created traffic jams of delivery trucks and delays in shipments), a cyberattack in 2017 with the "NotPetya" ransomware at the shipping company in container transport (the Danish "MAERSK") (damaged its information technology systems for several weeks), cyberattacks in the early 2020s at the shipping majors like Cosco, MSC and CMA CGM (took e-commerce platforms and vital data centres offline), a cyberattack in January 2023 at Norwegian shipping classification society DNV (a ransomware on the servers of its software), cyberattacks in 2022 and 2023 at the Port of Los Angeles (ransomware, malware and spear-phishing incidents). In 2022 maritime cybersecurity incidents occurred at Singapore shipbuilder Sembcorp Marine (an unauthorized access to the network), the Port of Lisbon (a cyberattack on the port's website and internal computer system).

The numerous proposals to amend the international legal instruments including the ISPS Code regarding the cybersecurity requirements are made. It is necessary to build cybersecurity rules into functional processes and training.

References

1. Anyanova, E. Maritime Cyber Security. Law, State and Telecommunications Review, v. 16, n. 2, p. 69–82, 2024. DOI: 10.26512/lstr.v16i2.47018.
2. Aranha, M. Hermeneutical Model for Identification of Juridical Variables in the ICT Comparative Research. SSRN Electronic Journal. May 2, 2011. Available at: http://dx.doi.org/10.2139/ssrn.2079096
3. Code of Practice Cyber Security for Ships. [s.l.]: The UK Department for Transport, 2017. Available at: https://www.gov.uk/.
4. DNV CYBER (Eds.) Maritime cyber priority, 2023. Available at: https://www.dnv.com/. 2024.
5. DNV CYBER (Eds.) Maritime cyber priority, 2024 / 2025. Available at: https://www.dnv.com/. 2024.
6. Dunlevie, T. Anticipating the Next Black Sea Shipping Crisis. Available at: https://centerformaritimestrategy.org/publications/anticipating-the-next-black-sea-shipping-crisis/. June 27, 2023.

7. IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0. IAPH. November 11, 2023.
8. IMO Resolution MSC.428(98). Maritime cyber risk management in safety management systems, 16 June 2017.
9. Maritime cyber risk. The IMO. Available at: https://www.imo.org/.
10. Maritime cybersecurity attacks on the rise - MARPOINT, 2023. Available at: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise
11. MarineLink (Eds.) New Maritime Cybersecurity Body Launched, 2024. Available at: https://www.marinelink.com/
12. Port cybersecurity: incorporating the IAPH's new guidelines into the ISPS code | Center for international maritime security, 2023. Available at: https://cimsec.org/incorporating-the-iaphs-new-cybersecurity-guidelines-into-the-international-ship-and-port-facility-security-code/.
13. Senarak, C. (2021). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. The Asian Journal of Shipping and Logistics, 37 (4), 345–360.
14.Shaisultanov, S.; Akimzhanov, T.; Abdrakhmanov, B.; Bazarlinova, A.; Bazarlinova A. Combating Internet Fraud through Operative-search Measures. The Law, State and Telecommunications Review, v. 16, no. 2, p. 257-275, October 2024.
15. SupplyChainBrain (Eds.) Chinese Hackers Targeting Ships Across Europe With Malware on USB Sticks, July 11, 2024. Available at: https://www.supplychainbrain.com/articles/40018-chinese-hackers-targeting-ships-across-europe-with-malware-on-usb-sticks.
16. The guidelines on cyber security onboard ships, Version 4, 2023. Available at: https://www.imo.org/.
17. THE IMO. IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2. [s.l.: s.n.], 2022.

Бардачевский Р.И., канд. юрид. наук, доцент, доцент кафедры ФГБОУ ВО «Уфимский университет науки и технологий», Институт права, г. Уфа,
следователь по особо важным делам отделения по расследованию киберпреступлений и преступлений в сфере высоких технологий третьего следственного управления Главного следственного управления Следственного комитета Российской Федерации, подполковник юстиции, г. Москва

О НЕОБХОДИМОСТИ ОПТИМИЗАЦИИ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ИНСТРУМЕНТОВ, НАПРАВЛЕННОЙ НА ПОВЫШЕНИЕ ОПЕРАТИВНОСТИ ИЗЪЯТИЯ СРЕДСТВ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация

В статье на основании приведенного анализа алгоритма расследования киберпреступления автором указывается на необходимость принятия мер по повышению оперативности изъятия устройств, посредством которых преступники воздействуют на информационную среду

Ключевые слова: расследование киберпреступлений; киберкриминалистика; применение компьютерной техники при совершении преступлений

В современном мире информационные технологии стали неотъемлемой частью нашей жизни. Они используются в различных сферах деятельности, от бизнеса до государственного управления. Однако вместе с развитием информационных технологий растёт и число киберпреступлений, которые представляют серьёзную угрозу для общества. Киберпреступления могут включать в себя широкий спектр деяний, таких как хакерские атаки, мошенничество, кража личных данных, распространение вредоносного программного обеспечения и другие. Тем самым, все киберперступления совершаются посредством компьютерной техники.

В фундаментальном исследовании обоснованно отмечено, что с применением компьютерной техники преступление совершается посредством реализации алгоритма: преступник-устройство-среда-устройство [3].

Следовательно, для изобличения киберпреступника необходимо изъять устройство, посредством которого им совершено преступление в киберпространстве [2].

При этом расследование киберпреступлений является сложной задачей, которая требует специальных знаний и навыков. Правоохранительные органы сталкиваются с рядом проблем, которые затрудняют

расследование этих преступлений. Одной из основных проблем является сложность выявления и идентификации преступников. Киберпреступники часто используют различные методы маскировки и анонимности, такие как VPN-сервисы, TOR-браузеры и другие инструменты. Это затрудняет определение их реального местоположения и личности.

Разработанная на основании следственной практики и описанная в современной литературе криминалистическая методика в основном применяет средства по работе с уже изъятыми техническими устройствами, указывает на приемы и методы, поиска, обнаружения, изъятия, осмотра и интерпретации цифровых следов. Вместе с тем, описываемые криминалистические методы работы с компьютерной техникой реализуются не на всех этапах расследования, а как правило уже при расследовании уголовных дел либо при проверке сообщений о резонансных происшествиях [4,5].

Вместе с тем, длительность стадии возбуждения уголовного дела препятствует возможности производства обыска и изъятия средства связи, содержащего сведения составляющие охраняемую законом тайну переписки. Доследственная проверка от первоначального сообщения до возбуждения уголовного дела с принятием конкретных мер к изъятию компьютерной техники может занимать значительное время, в течение которого средства могут быть глубоко скрыты либо уничтожены, информация удалена.

В данной связи есть очевидные основания согласиться с мнением Б.Я. Гаврилова, согласно которому необходимо рассмотреть вопрос отмены как не эффективной стадии возбуждения уголовного дела [1].

Таким образом, для оптимизации противодействия киберпреступлениям необходимо принять действенные меры по повышению оперативности изъятия устройств, посредством которых преступники воздействуют на информационную среду, совершают киберпреступления.

Список цитируемой литературы:

1. Гаврилов, Б.Я. К вопросу о роли законодательства уголовно-правового комплекса в борьбе с преступностью: современное состояние и перспективы совершенствования / Б. Я. Гаврилов // Уголовно-правовые, уголовно-процессуальные и криминалистические вопросы борьбы с преступностью : Сборник статей по материалам VII Всероссийской научно-практической конференции, Краснодар, 23 ноября 2023 года. – Краснодар: Кубанский государственный аграрный университет им. И.Т. Трубилина, 2024. – С. 170-183.
2. Саркисян, А.Ж. О киберпространстве в Российской Федерации (уголовно-правовой аспект) / А. Ж. Саркисян // Проблемы противодействия

киберпреступности : Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2023. – С. 191-195.
3. Себякин, А.Г. Тактика использования знаний в области компьютерной техники / А. Г. Себякин. – Москва: Издательство «Юрлитинформ», 2023. – 200 с.
4. Петраков, С.В, Гудкова, М.А., Бащук, Д.П., Тимофеев, А.А., Пигильдин, Д.Н., Бедеров, И.С., Сорокин, Д.О., Пытайло А.В. Сбор и анализ цифровых следов преступления: практическое пособие / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло. – Санкт-Петербург: Санкт-Петербургская академия Следственного комитета, 2023. – 98 с.
5. Тактика следственного осмотра по делам о киберпреступлениях: учебно-методическое пособие / под ред. Э.Б. Хатов, А.Ю. Любавского, С.Ю. Скобелина, А.Ж. Саркисян. – Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2023. – 117 с.

Бодров Н.Ф., канд. юрид. наук, доцент кафедры
ФГБОУ ВО «Университет имени О.Е. Кутафина (МГЮА)»,
президент международной общественной организации
«Союз криминалистов и криминологов», г. Москва

Лебедева А.К., канд. юрид. наук, доцент, доцент кафедры
ФГБОУ ВО «Университет имени О.Е. Кутафина (МГЮА)»,
член международной общественной организации
«Союз криминалистов и криминологов», г. Москва

КРИМИНАЛИСТИЧЕСКОЕ ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ДИПФЕЙКОВ

Аннотация

В статье рассматриваются вопросы криминалистического противодействия распространению дипфейков. В условиях стремительного роста использования дипфейков в преступных целях возникает необходимость разработки новых методов и инструментов для их выявления, для расследования и раскрытия преступлений, в которых они фигурировали. В статье представлены основные вызовы, с которыми сталкиваются правоохранительные органы, включая сложности в установлении аутентичности цифровых продуктов и необходимость адаптации методов судебных экспертиз к условиям использования нейросетевых технологий.

Ключевые слова: дипфейк; генеративный контент; судебная экспертология; криминалистика.

Технологии искусственного интеллекта (далее – ИИ) с каждым днём всё активнее используются при совершении различных видов преступлений, разнообразный генеративный контент, созданный при помощи нейросетевых технологий, применяется при осуществлении клеветы, шантажа, различных видов мошенничества, в том числе телефонного. Данный перечь можно и далее продолжать [1]. Фальсификация цифровых продуктов с использованием нейросетевых технологий уже является источником информационных атак, а также определённым инструментом влияния на судебные процессы, что ставит под угрозы всю систему правосудия.

Однако в современных реалиях уже невозможно говорить о запрете на создание генеративного контента с помощью ИИ, как предлагают некоторые автора («Одним из вариантов решения данной проблемы может стать запрет определённых типов приложений по созданию дипфейков» [8, С. 121]), а о необходимости его правового регулирования, а также о разработке подходов к криминалистическому противодействию дипфейков.

Первоначально представим, что из себя представляет понятие «дипфейк» с нашей точки зрения, а также в чём его отличие от генеративного контента в целом.

В своих работах мы уже неоднократно представляли наше определения дипфейка, «дипфейк – это цифровой продукт в виде текста, графики, звука или их сочетания, сгенерированный полностью или частично при помощи нейросетевых технологий для цели введения в заблуждение или преодоления пользователем систем контроля и управления доступом» [2, С. 351]. Таким образом, в момент генерации цифровой продукт не становится дипфейк, свои свойства дипфейка он приобретает в момент использования и распространения с противоправной целью.

Цифровые продукты, созданные при помощи нейросетевых технологий, сейчас появляются и в арбитражных спорах о существовании исключительных прав на подобные цифровые продукты [4]. Дипфейки же все чаще фигурируют в различных делах как орудия преступного посягательства. Новостные ресурсы регулярно предупреждают своих читателей о возможностях хищения денежных средств при помощи сгенерированного контента, однако подобные превентивные меры оказывают воздействие далеко не на всех пользователей [5]. Как сообщает новостное издание «Известия»: «В 2024 году число дипфейк-атак, по подсчётам VisionLabs (структура МТС), составило десятки тысяч случаев, а в 2025 году это число может возрасти уже в десятки раз» [7].

В условиях стремительного развития технологий, с помощью которых возможно создавать цифровые продукты, сходные с аутентичным контентом до степени смешения, в связи с серьёзными трудностями в распознавании подобного контента без специальных знаний, необходимо говорить о возможностях криминалистического противодействия распространению дипфейков.

С учётом природы дипфейка возникает необходимость адаптации существующих методов раскрытия и расследования преступлений, уточнения самой процедуры доказывания для эффективного противодействия данной угрозе.

Проблема столь активного использования и распространения дипфейков затрагивает всех участников судебного процесса. В заблуждение могут быть введены как правоприменители, так и свидетели, а также эксперты. Несмотря на это, на наш взгляд, ключевое значение в доказывании по таким делам будет иметь заключение эксперта. Это обусловлено тем, что основной трудностью является установление того, был ли представленный цифровой продукт создан с использованием нейросетевых технологий или является аутентичным. Судебная практика в данной области находится на стадии формирования, сталкиваясь с рядом как правовых, так и технологических проблем. Законодатель уже осознал проблему распространения дипфейков и предложил законопроект, предусматривающем внесение в некоторые статьи Уголовного кодекса РФ дополнительного квалифицированного состава, предлагающего установить использование дипфейка в качестве квалифицирующего признака [6]. Тем не менее, ограниченный перечень статей, в которые планируется внести изменения, не решит технологические проблемы распознавания дипфейков.

Вследствие чего, целесообразно решать вопрос о необходимости назначения различных судебных экспертиз. С учётом видов дипфейка это могут быть видеотехническая, фототехническая и портретная экспертизы в случае исследования графических дипфейков, автороведческая экспертиза для исследования текстового, а также фоноскопическая в целях исследования голосового дипфейка.

При этом следует учитывать, что существующие методики большинства судебных экспертиз не были изначально разработаны для анализа объектов, являющихся результатами нейросетевой генерации. Даже категорическое заключение эксперта может оказаться неэффективным для дальнейшего доказывания в современном цифровом обществе, если в процессе экспертного исследования не был установлен факт того, что исследуемый цифровой продукт действительно является дипфейком, в таком случае выводы эксперта могут быть поставлены

под сомнение. В современных условиях, когда технологические возможности для нейросетевых генераций стремительно развиваются, отсутствие чёткого подтверждения факта фальсификации цифрового продукта или опровержения данного тезиса может серьёзно повлиять на достоверность выводов эксперта даже в случае тщательного соблюдения существующих методик. Таким образом, для обеспечения надёжности и достоверности результатов экспертного исследования, необходимо учитывать специфические особенности работы с нейросетевыми технологиями, что требует пересмотра и адаптации существующих методик судебных экспертиз [См., например, 3].

Важно понимать, что адаптация криминалистики для противодействия распространению дипфейков — это не только чисто техническая задача, но и вызов для системы правосудия в целом. Необходимо развивать не только методы судебно-экспертного распознавания дипфейков, но и повышать осведомлённость правоприменителя в условиях определённой технологической трансформации нашего общества. В этой связи криминалистика должна развиваться в соответствии с вызовами цифрового века, обеспечивая защиту от таких угроз как дипфейки, и способствуя эффективному расследованию преступлений в условиях повсеместного распространения современных технологий.

Список цитируемой литературы:

1. Бодров, Н.Ф., Лебедева, А. К. Понятие дипфейка (deepfake) в российском праве, его классификация дипфейков и проблемы правового регулирования / Н.Ф. Бодров, А.К. Лебедева// Вестник Дагестанского государственного университета (Научно-образовательный журнал). – 2023. – Т.48. – № 4 (68). – С.73-82.
2. Бодров, Н.Ф., Лебедева, А.К. Перспективы правового регулирования и алгоритм маркировки генеративного контента / Н.Ф. Бодров, А.К. Лебедева // Пенитенциарная наука. –2024. – Т. 18. – № 4 (68). – С. 348–357.
3. Бодров, Н.Ф., Лебедева, А.К. Судебно-экспертное противодействие дипфейк-дезинформации / Н.Ф. Бодров, А.К. Лебедева // Союз криминалистов и криминологов. – 2024. – № 4. – С.129-142.
4. Материалы дела № А40-200471/23-27-1448. [Электронный ресурс] – Картотека арбитражных дел. – URL: https://kad.arbitr.ru/Card/4d7f0305-69af-44fe-8841-a59e84aa7deb (дата обращения: 09.01.2024).
5. Мошенники используют нейросети в новогодние праздники, предупредили россиян. [Электронный ресурс]. – Газета.Ru. – URL: https://www.gazeta.ru/social/news/2024/12/24/24698114.shtml?updated (дата обращения: 09.01.2024).

6. Проект федерального закона № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (внесён 16.09.2024 г. депутатом Государственной Думы Я. Е. Ниловым, Сенатором Российской Федерации А. К. Пушковым) [Электронный ресурс]. – Система обеспечения законодательной деятельности. – URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 24.11.2024).
7. Сбросить вызов: россияне получают дипфейк-звонки от родственников и начальников. [Электронный ресурс]. – Известия. – URL: https://iz.ru/1810531/dmitrii-alekseev/sbrosit-vyzov-rossiane-polucaut-dipfeik-zvonki-ot-rodstvennikov-i-nacalnikov (дата обращения: 09.01.2024).
8. Свиридова, Е. А. Правила использования технологий дипфейк в праве США и КНР: адаптация зарубежного опыта правового регулирования / Е. А. Свиридова // Современное право. – 2024. – № 3. – С. 119-123.

Бородин Д.В., аспирант
ФГБОУ ВО «Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского», г. Липецк

Тестирование веб-приложений на базе CMS «1С-Битрикс: Управление сайтом» для предупреждения киберпреступлений

Аннотация

Рассмотрены методы борьбы с киберпреступлениями. Особое внимание уделено тестированию безопасности веб-приложений, созданных на платформе CMS «1С-Битрикс: Управление сайтом», как способу повышения информационной безопасности. В работе представлен алгоритм тестирования, включающий анализ используемого программного обеспечения, аудит паролей, сетевых подключений, функциональное тестирование и нагрузочное тестирование, проверке безопасности. Проведение комплексного анализа позволяет минимизировать риски успешных атак и обеспечить высокую степень защиты веб-приложений.

Ключевые слова: киберпреступления, тестирование безопасности, информационная безопасность, CMS «1С-Битрикс: Управление сайтом», веб-приложения, уязвимости, нагрузочное тестирование, автоматизированные инструменты, защита данных.

Киберпреступность продолжает развиваться, создавая угрозы для экономики, информационной безопасности и правопорядка в целом.

Современные преступные схемы включают фишинг, использование вредоносного программного обеспечения (ВПО), криптографических вирусов, хищение данных и атаки на цифровую инфраструктуру. Необходимость совершенствования методов борьбы с киберпреступлениями выражена не только сложностью их расследования, но и экономическими последствиями.

Данная проблема становится по-настоящему актуальной в настоящее время, когда компьютерные атаки, помимо преследования целей личной выгоды злоумышленников, начинают нести политический характер. Несмотря на это они касаются не только государственных организаций, но и обычных граждан страны.

Рассмотрим существующие способы повышения уровня информационной безопасности и борьбы с киберпреступлениями.

Для отслеживания возможных источников киберпреступлений предлагается осуществлять мониторинг Интернет-ресурсов для обнаружения следов возможных злоумышленников, таких как фишинговые рассылки, интернет-пирамиды [1]. В другом исследовании было предложено анализировать прогресс кибератак за последние 10 лет для предсказания возможных направлений развития кибератак в будущем [2].

Ряд иных исследований направлены на корректировки законодательной системы для повышения возможностей правоохранительной системы и отслеживания возможных действий злоумышленников на территории Российской Федерации (РФ) [3-5].

Для повышения уровня информационной защищенности граждан РФ предлагается вводить дополнительные механизмы цифровой осведомлённости, проводить обязательные разговоры о важном для школьников для воспитания в них механизмов цифровой грамотности [6-8]. Также одними из основных методов повышения уровня информационной защищенности является настройка современных механизмов защиты организаций (сетевые ограничения, установка обновлений, установка средств защиты информации) [9].

Данные способы действительно являются результативными для повышения информационной безопасности и борьбы с киберпреступлениями, но с учетом быстрорастущих темпов развития цифровизации их необходимо регулярно корректировать.

Наиболее частой причиной компрометации информационных ресурсов организаций является взлом веб-сайтов, через имеющиеся уязвимости программного обеспечения и конфигурации системы управления содержимым сайтов. Одной из самых популярных в РФ систем управления содержимых сайтов является CMS «1С-Битрикс: Управление сайтом» (CMS 1С-Битрикс). В мае 2023 года информационные ре-

сурсы на CMS 1С-Битрикс были массово взломаны с использованием уязвимости в одном из модулей (https://www.securitylab.ru/news/539321.php?ysclid=m5lc2s70g4318153660), но и после закрытия разработчиками данной уязвимости атаки на данный продукт продолжаются и в настоящее время. Причиной тому является отсутствие проверки безопасности продукта после развертывания в конструкторе сайта.

В данной работе рассмотрим наиболее популярные способы тестирования безопасности CMS 1С-Битрикс для предупреждения киберпреступлений.

Тестирование веб-приложений на базе CMS 1С-Битрикс включает следующие этапы.

Первым этапом тестирования безопасности CMS 1С-Битрикс необходимо проверить версию используемого дистрибутива, в случае использования устаревшей версии ее необходимо обновить вручную, так как старые версии могут содержать уязвимости безопасности, эксплуатируемые злоумышленниками.

Следующим этапом необходимо провести проверку используемых паролей на наличие их в утечках и списках словарных паролей, можно осуществить на сайте Kaspersky (https://password.kaspersky.com/ru/). Надежный пароль, а также его периодическая смена позволят избежать компрометации со стороны злоумышленников.

На третьем этапе проводится анализ исходных данных системы, таких как IP-адреса, открытые порты, версии используемого программного обеспечения и стандартные пути к основным компонентам. Этот процесс включает использование утилит, таких как nmap (https://nmap.org/), для сканирования портов и выявления потенциальных точек входа. CMS 1С-Битрикс поставляется вместе с дистрибутивом на базе операционной системы CentOS и при стандартной установке имеет следующий набор открытых портов:

- порт 22/TCP используется для удалённого администрирования и подключения пользователей по протоколу SSH.
- порт 80/TCP используется веб-сервером для передачи данных по протоколу HTTP в системах типа «клиент — сеть».
- порт 443/TCP используется веб-сервером для передачи данных по протоколу HTTPS в системах типа «клиент — сеть».
- порт 3306/TCP применяется для подключения к серверу баз данных MySQL.

Неограниченный доступ к портам SSH и MySQL является уязвимостью безопасности, которая при использовании стандартного или словарного пароля может привести к компрометации веб-сайта.

На четвертом этапе выполняется функциональное тестирование, направленное на проверку корректности работы всех модулей и функций приложения. Для этого создаются тест-кейсы, охватывающие стандартные и граничные сценарии использования. Важным моментом является тестирование административной панели, доступ к которой может стать целью злоумышленников.

Список некоторые из таких уязвимых точек приведен ниже:

1. /bitrix/admin;
2. /bitrix/tools/autosave.php;
3. /bitrix/tools/get_catalog_menu.php;
4. /bitrix/tools/upload.php;
5. /bitrix/tools/seo_page_parser.php;
6. /bitrix/tools/seo_google.php;
7. /bitrix/tools/seo_yandex_direct.php;
8. /bitrix/tools/seo_yandex.php;
9. /bitrix/tools/clock_selector.php;
10. /bitrix/components/bitrix/desktop/admin_settings.php;
11. /bitrix/components/bitrix/player/player_playlist_edit.php;
12. /bitrix/components/bitrix/map.yandex.view/settings/settings.php;
13. /bitrix/components/bitrix/map.google.view/settings/settings.php;
14. /bitrix/components/bitrix/map.google.search/settings/settings.ph.

Также необходимо проверить доступ к панели входа, используемой для аутентификации в мобильном приложении, которая позволяет осуществить подбор аутентификационных данных пользователей, конечная точка сайта: /bitrix/services/mobileapp/jn.php.

Пятым этапом проводится тестирование безопасности. Оно включает проверку устойчивости к SQL-инъекциям, XSS-атакам, Open Redirect-уязвимости и анализ конфигураций сервера. Также необходимо проверить доступ к потенциально уязвимым модулям CMS 1С-Битрикс: vote.php, html_editor_action.php, landing.

Для проверки используются автоматизированные инструменты, такие как Nuclei (https://github.com/projectdiscovery/nuclei?ysclid=m5np07m5gk346932198), OpenVAS (https://openvas.org/), Nikto (https://github.com/NashTech-Labs/Nikto?ysclid=m5np10l11f730988919).

Следующий этап включает нагрузочное тестирование, направленное на оценку стабильности приложения под высокими нагрузками. Этот шаг предполагает моделирование большого количества пользователей, одновременно взаимодействующих с системой, что позволяет определить её пределы производительности и выявить узкие места в коде и инфраструктуре.

Таким образом, алгоритм тестирования веб приложений на базе CMS 1С-Битрикс выглядит следующим образом:

1. Проверка обновлений используемого программного обеспечения.
2. Аудит используемых паролей.
3. Проверка сетевого доступа к ресурсам сайта.
4. Проверка работоспособности модулей системы управления содержимым сайта.
5. Тестирование безопасности с помощью сканеров безопасности.

Комплексный подход, включающий функциональное, нагрузочное тестирование, аудит безопасности и моделирование атак, позволяет обеспечить максимальный уровень защиты веб-приложений.

Реализация многоуровневого подхода к тестированию веб-приложений на базе CMS 1С-Битрикс позволяет оценить состояние системы и выявить её уязвимости. Проведение всех этапов тестирования, включая обновление программного обеспечения, анализ паролей, сканирование сетевых подключений, функциональные проверки, а также тесты на устойчивость к нагрузкам и безопасность, даёт возможность минимизировать риски успешных атак.

Подход, дополненный применением современных автоматизированных инструментов, таких как Nuclei, OpenVAS, Nikto, обеспечивает надежную степень защиты системы. Организация безопасности веб-приложений остаётся приоритетной задачей в условиях нарастающей активности киберпреступников. Только систематический анализ позволяет разработчикам и администраторам создавать защищённые цифровые продукты, которые будут соответствовать требованиям и повышать доверие пользователей.

Список цитируемой литературы:

1. Агаркова, А.А., Синицына, В.А. Киберпреступность в современной России / А.А. Агаркова, В.А. Синицина //Международный журнал гуманитарных и естественных наук. – 2021. – №. 5-3. – С. 13-16.
2. Кириленко, В.П., Алексеев, Г.В. Киберпреступность и цифровая трансформация/ В.П. Кириленко, Г.В. Алексеев //Теоретическая и прикладная юриспруденция. – 2021. – №. 1. – С. 39-53.
3. Шикула, И.Р., Куркин, Е.Н. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия / И.Р. Шикула, Е.Н. Куркин // Международный журнал экспериментального образования. – 2023. – №. 1. – С. 37 - 41.
4. Короткова, И.С., Мельникова, Н.С. Киберпреступность в банковской сфере / И.С. Короткова, Н.С. Мельникова // Вектор экономики. – 2023. – №. 4 (82).

5. Карцхия, А.А., Макаренко, Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности/ А.А. Кархия, Г.И. Макаринко // Вопросы кибербезопасности. – 2023. – Т. 1. – №. 53. – С. 58-74.
6. Кобец, П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения / П.Н. Кобец //Вестник Самарского юридического института. – 2022. – №. 1 (47). – С. 52-58.
7. Гусев, В.А. Цифровая гигиена vs. Киберпреступность / В.А. Гусев //Психопедагогика в правоохранительных органах. – 2022. – Т. 27. – №. 1 (88). – С. 102-108.
8. Шогенов, З.А. Киберпреступность как одна из основных проблем современного общества/ З.А. Шогенов //Право и управление. – 2023. – №. 2. – С. 222-226.
9. Мамцов, К.Г., Ачилов Н.Р. Киберпреступность как угроза национальной безопасности / Е.Г. Мамцов, Н.Р. Ачилов //Молодой исследователь Дона. – 2022. – №. 1 (34). – С. 42-45.
10. Уязвимости и атаки на CMS Bitrix. [Электронный ресурс]. – Github. – URL: https://github.com/cr1f/writeups/blob/main/attacking_bitrix.pdf?ysclid=m5nmsfooy320196034 (дата обращения: 08.01.2025).

Брусенцева В.А., канд. юрид. наук, доцент, доцент кафедры ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Липецкий филиал, г. Липецк

Современные угрозы безопасности несовершеннолетних в сети Интернет

Аннотация

В статье анализируются современные угрозы и риски, с которыми сталкиваются дети в сети Интернет. Анализируется алгоритм вовлечения несовершеннолетних в противоправную деятельность. Даётся характеристика основных видов преступлений, в совершении которых они задействованы. Отмечается необходимость разработки механизма нейтрализации угроз и рисков в цифровой среде и повышения уровня информационной грамотности среди несовершеннолетних.

Ключевые слова: информационная безопасность, несовершеннолетние, противоправная деятельность, сеть Интернет, вовлечение в деструктивную деятельность.

Бурное развитие информационных технологий способствовало появлению новой среды обитания человека. Всемирная паутина открыла широкие возможности и позволила объединить различные социальные группы людей, независимо от их местоположения, возраста или пола.

Тем не менее, онлайн – пространство сегодня нередко используется для достижения криминальных целей, в качестве площадки для популяризации антиобщественного поведения и совершения преступных действий. Такого рода рискам и угрозам, в наибольшей степени подвержены несовершеннолетние. Именно они являются активными пользователями сети Интернет, социальных сетей и мессенджеров.

Согласно данным, приведенным в отчете Digital 2025 Global Overview [1], в мире насчитывается около 5,56 миллиардов интернет-пользователей, среди которых возрастная группа от 0 до 19 лет составляет 32,4%. Ежедневно несовершеннолетние (в возрасте 16 – 24 лет) проводят значительное время в сети Интернет, что в среднем составляет 7 часов 22 минуты онлайн - активности. В качестве основных цифровых потребностей молодежи выделяются: социальное взаимодействие с друзьями и близкими; поиск развлечений, видео и музыки; подборка информации, связанной с обучением и новыми знаниями.

Оценка времяпровождения в сети Интернет российских детей и подростков несколько отличается. Исследование, проведенное компанией «Ростелеком» свидетельствует о том, что они (97%) ежедневно проводят в сети приблизительно 6,5 часов в сутки [2]. При этом осваивать интернет – пространство и мессенджеры дети начинают уже с четырехлетнего возраста, а заводить блоги, личные страницы и активно общаться в социальных сетях – с девяти. Предпочтения несовершеннолетних в контенте меняются в зависимости от принадлежности от определенной возрастной группе. Дети младшей возрастной группы (от 4 до 8 лет) выбирают просмотр видеоконтента (видео, мультиков, роликов, кино), игры в компьютерные игры, прослушивание музыки. Напротив, молодые люди в возрасте от 12 до 17 лет в большей степени интересуются межличностным общением, которое осуществляется через социальные сети и мессенджеры.

Следует также отметить, что по мере взросления дети активнее используют Интернет для установления новых контактов и последующего взаимодействия. При этом основными площадками для знакомств выступают: онлайн игры и игровые сервисы; лента друзей; группы в ВК; комментарии под постами; чат-рулетки и боты для знакомств.

Онлайн - активность несовершеннолетних в интернет - пространстве привлекает преступников и открывает для них достаточно широкие возможности, среди которых анонимность и отсутствие террито-

риальной привязки. Кроме того, в целях знакомства и последующего общения, злоумышленники могут создавать фейковые аккаунты, которые не позволяют объективно оценить реальные данные собеседника.

Они учитывают особенности их психики, интересы и стиль общения. Меняют подходы в зависимости от возрастной категории и типа потенциальной жертвы. Дети в силу ограниченности кругозора, неразвитости критического мышления и желания казаться самостоятельным, не могут объективно оценить сложившуюся ситуацию. В связи с чем достаточно легко попадают под влияние и зависимость злоумышленников. Они манипулируют, шантажируют и убеждают их совершить преступные действия.

Однако получить реальное представление о том, какое количество несовершеннолетних были вовлечены в совершение противоправной деятельности с помощью сети Интернет не представляется возможным. Специальная выборка не делается.

Обратимся к статистике Роскомнадзора, которая указывает на то, что в 2024 году было заблокировано около 800 тыс. интернет-страниц с запрещенной информацией. По сравнению с прошлым годом рост составил 19%. При этом, значительную долю (около 40%) противоправных материалов, подвергшихся блокировке, составляли следующие категории контента: детская порнография (19,12%); пронаркотический контент (36,51%); фейки о Вооруженных силах Российской Федерации (7,73%); суицидальный контент (9,71%); контент экстремистского и террористического характера (13,88%); материалы с пропагандой ЛГБТ (признано экстремистским и запрещено в РФ), педофилии и смены пола (13,03%) [3].

Непосредственному взаимодействию злоумышленника с несовершеннолетним, предшествует изучение его профиля, оценка коммуникационной активности, анализ личных страниц социальных сетей и аккаунтов мессенджеров, информации о месте жительства, учебе, личных данных и данных родственников и т.п. Такого рода оценка личности, позволяет выявить ее слабые и сильные стороны, круг интересов, ценности, психоэмоциональное состояние. Зачастую выбор падает на тех, кто не имеет твердых убеждений, испытывает разочарование или находится в конфликтной ситуации с окружающими (сверстниками, родителями и иными лицами), ведет асоциальный образ жизни, имеет финансовые трудности, либо находится в иных кризисных обстоятельствах.

Техника установления первоначального контакта и алгоритм последующей работы с несовершеннолетним помимо возраста, пола, интересов также зависит от специфики деятельности в которой он будет задействован. Здесь могут использоваться психологические и марке-

тинговые методы воздействия, которые необходимо рассматривать как подготовку к совершенному в последующем преступному действию. Их применение в симбиозе с информационно-коммуникационными технологиями повышает результативность преступной деятельности, а потерпевших делает своими помощниками.

Одной из активно применяемых технологий психологической манипуляции действиями детей является социальная инженерия, которая основана на использовании психологических особенностей личности в целях получения конфиденциальных сведений, обеспечивающих несанкционированный доступ к конфиденциальной компьютерной информации [4, С. 187]. Главным образом в отношении детей применяются претекстинг и обратная социальная инженерия.

Другим приемом вовлечения в преступную деятельность, получившим распространение в последнее время, стала маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами.

После этого происходит отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообществ.

Следует также отметить избирательность подходов, применяемых в процессе знакомства с детьми различных возрастных групп. Для детей младшего возраста преимущественно используются игровые формы (онлайн - игры, квесты). Напротив, для подростков представляют интерес тематические сайты и форумы, связанные с трудоустройством, молодежной тематикой и т.п.

Первый контакт может происходить случайно, а затем перерастать в общение, которое порой становится назойливым, вызывающим психологический дискомфорт. Нередко дистанционными собеседниками используются методы манипуляции, шантажа и убеждения, которые позволяют мотивировать подростков на совершение противоправных действий. В силу ограниченности кругозора, неразвитости критического мышления и желания казаться самостоятельным, они не могут адекватно оценить возможные последствия совершенных ими в последующем противоправных действий.

Анализ материалов уголовных дел [5] позволяет сделать вывод о том, что наиболее активно подростков вербуют для распространения наркотических и психотропных средств, совершения экстремистских и террористических преступлений, выполнения курьерских функций по

транспортировке денег или предметов, полученных мошенническим путём, распространение порнографических материалов с их участием. При этом они могут не осознавать реальную общественную опасность и последствия своих действий.

В этой связи выстраивание эффективного механизма нейтрализации угроз и рисков в цифровой среде, противодействия вовлечению несовершеннолетних в деструктивную деятельность предполагает создание комплексной системы мониторинга и контроля за контентом, распространяемым в сети Интернет, включая своевременное выявление и пресечение противоправной информации, пропагандирующей экстремизм, терроризм, суицидальное поведение, наркотики и другие опасные явления [6]. Немаловажное значение также будет играть повышение уровня информационной грамотности среди детей и подростков, внедрение специальных образовательных программ, направленных на формирование критического мышления и умения распознавать угрозы в виртуальном пространстве.

Список цитируемой литературы:

1. Digital 2025 Global Overview Report. [Электронный ресурс]. – URL: https://indd.adobe.com/view/9d9a68f6-38a9-4278-b61c-4506b24240b0?allowFullscreen=true&wmode=opaque (дата обращения: 15.12.2024)/
2. Виртуальный мир глазами детей: особенности поведения детей и подростков в сети интернет. Часть 1. Общение, творчество, развлечение, обучение. [Электронный ресурс]. – URL: https://www.company.rt.ru/projects/digital_economy_rf/ncit/files/RT-KIDS-2024_light.pdf (дата обращения: 12.12.2024).
3. РКН в 2024 году заблокировал почти 800 тыс. материалов с запрещенной информацией [Электронный ресурс]. – URL: https://tass.ru/obschestvo/22903351 (дата обращения: 12.12.2024).
4. Поляков, В. В. Применение технологий социальной инженерии при совершении высокотехнологичных преступлений / В. В. Поляков // Криминалистика: вчера, сегодня, завтра. – 2023. – № 3(27). – С. 175-188.
5. Судебные и нормативные акты РФ [сайт]. – URL: https:// sudact.ru (дата обращения: 04.01.2025).
6. Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу: распоряжения Правительства Рос. Федерации от 02 декабря 2015 г. № 2471-р // Собрание законодательства Российской Федерации. – 2023. – № 19. – Ст. 3481.

Галкин Д.В., канд. юрид. наук, доцент, зав. кафедрой
ФГКОУ ВО «Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева»,
Хабаровский филиал, г. Хабаровск
полковник юстиции

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С АВТОМОБИЛЬНЫМ ТРАНСПОРТОМ

Аннотация

В статье рассматриваются возможности получения криминалистической, в том числе доказательственной информации в ходе расследования преступлений, с помощью современных информационно-транспортных системам, на примере системы взимания платы за проезд большегрузных автомобилей «Платон». Подчеркивается возрастающее криминалистическое значение данных источников информации в системе других источников, основанных на цифровых технологиях. Анализируются возникающие при этом проблемы в следственной деятельности, обусловленные как особенностями действующего законодательства, так и недостатками правоприменительной практики.

Ключевые слова: источники криминалистической информации; цифровая криминалистика; информационно-транспортные системы; автомобильная телематика; система взимания платы «ПЛАТОН»; использование средств измерений в криминалистической работе.

Динамичное развитие цифровых технологий и их внедрение во все сферы жизни затронуло многие направления юридической работы по всем отраслям права. Особенно сильно технологический скачок отразился на криминалистике – прикладной области юридических знаний, самым тесным образом связанной с достижениями науки и техники [6]. Отражением данных тенденций стало научное осмысление цифровой криминалистики.

Современные фундаментальные исследования в области цифровой криминалистики сосредоточились, в основном, на теоретических вопросах, разработке понятийного аппарата, систематизации новых областей знаний [5]. Вместе с тем, для поступательного развития криминалистической науки и сохранения ее практической значимости представляется важным развивать и сугубо прикладные исследования в области цифровой криминалистики. Теоретическое осмысление является фундаментом и необходимым условием таких исследований. Необходимы анализ и обобщение современной следственной практи-

ки, выявление в ней наиболее важных элементов цифровой криминалистики, уже сейчас используемых в практической работе [1].

В современных технологических условиях профессионализм каждого следователя в отдельности и эффективности организации расследования преступлений в целом зависит от навыков поиска и использования цифровых следов. Цифровые следы пронизывают практически все сферы жизнедеятельности личности, общества и государства. Среди прочего, современные цифровые технологии активно внедряются в системы государственного и негосударственного (корпоративного) транспортного контроля, которые собирают и хранят информацию о различных параметрах самих транспортных средствах и режиме их эксплуатации. Для этого используются современные технические средства, позволяющие фиксировать такие параметры, как вес автомобиля, включая нагрузку на каждую из осей грузового тягача и прицепа, вес и размер перевозимого груза, текущее местоположение в заданный период времени и путевой маршрут, время и скорость передвижения. Возможности определения указанных параметров приобретают качественно новое значение при использовании фото и видео фиксации, технологий спутниковой навигации и дистанционной передачи цифровых данных по сетям сотовой связи.

В результате системы транспортного контроля формируют огромный массив различной информации, используемой органами власти и хозяйствующими субъектами в целях экономического регулирования, управления грузовыми и пассажирскими перевозками, обеспечения безопасности дорожного движения, сбора обязательных платежей, а также для решения других прикладных задач.

Данные информационные массивы имеют важное криминалистическое значение, которое не замыкается на преступлениях, связанных исключительно с нарушениями при эксплуатации транспорта. Глобальный характер информационно-транспортных систем, широкий спектр собираемой информации и значительное число задействованных участников определяют значимость сведений из указанных источников для установления самых разнообразных обстоятельств в рамках расследований по уголовным делам и материалам проверок. Уже сейчас следственная практика демонстрирует примеры их использования в доказывании криминальных событий и виновности их участников по делам о преступлениях против личности, в сфере экономики и налогообложения, против общественной безопасности и общественного порядка [2]. Потенциальное криминалистическое значение информационно-транспортных систем представляется еще более важным с учетом перспектив их развития, технологического оснащения и дальнейшего внедрения в сферу управления и контроля.

Действующие системы контроля за эксплуатацией транспорта имеют сложную структуру, значительное число субъектов контроля, имеющих различную подведомственность, смежные компетенции, сложную нормативную регламентацию. Нормативные и правоприменительные акты в данной сфере, техническая документация, содержат множество специальных терминов, требующих пояснения. Указанные обстоятельства обуславливают необходимость систематизации криминалистически значимой информации в данной сфере по видам, определения ее содержания, ведомственной и иной субъектной принадлежности, непосредственных источников получения.

Рассмотрим криминалистическое значение сведений, формируемых одной из современных информационно-транспортных систем – государственной системы взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 тонн, она же система «Платон». С криминалистической точки зрения представляют интерес основные технические и организационные особенности ее функционирования, структура и состав аккумулируемых сведений, правовой порядок их получения и возможности использования в качестве доказательственной информации в следственной работе.

В настоящее время уже имеются примеры следственной и судебной практики, демонстрирующие возможности криминалистического использования сведений, формируемых системой «Платон». Они используются для выяснения обстоятельств, подлежащих установлению по уголовным делам о преступлениях различных видов и категорий.

Целевое назначение системы «Платон» обуславливает использование аккумулируемой информации при расследовании налоговых преступлений, при этом связанных не только с уклонением от уплаты транспортного налога. Так, полученные с помощью системы «Платон» сведения использовались в качестве одного из доказательств обвинения при расследовании уголовного дела по факту хищения предпринимателем денежных средств из федерального бюджета путем незаконного возмещения налога на добавленную стоимость. Способ совершения данного преступления был связан с искусственным завышением расходов организации; для этого предприниматель предоставил в налоговые органы подложные документы о якобы оплаченной и реализованной перевозке груза автомобильным транспортом. Соответственно, одной из ключевых задач следствия явилось доказывание фиктивности этой грузоперевозки. От оператора системы «Платон» были получены сведения о том, что грузовой автомобиль, заявленный в путевом листе и товарно-

транспортных накладных, не осуществлял движение по маршруту и в период, указанные в подложных документах. Таким образом, данные системы «Платон» в совокупности с другими доказательствами позволили опровергнуть ложную версию обвиняемого [4].

В 2024 году в рамках проводимой в Московской академии Следственного комитета имени А.Я. Сухарева плановой научно-исследовательской работы по теме «Электронные системы транспортных средств как источник криминалистически значимой информации» в следственных органах были истребованы сведения об имеющейся у них практике использования данных, полученных с помощью встроенных и телематических автомобильных электронных устройств, включая данные системы «Платон».

Обобщение и анализ полученных материалов следственной практики подтверждают вывод о том, что криминалистическая информация из рассматриваемых источников используется при расследовании различных видов преступлений, а не только дорожно-транспортных происшествий. Например, технические данные и аудиозапись переговоров водителя автомобиля и диспетчера системы «ЭРА-ГЛОНАСС» позволили уточнить обстоятельства совершенного в отношении этого водителя грабежа. В другом случае, сведения о составе и маршруте перемещения коммерческого груза автомобильным транспортом легли в основу версии следствия о фиктивности сделки между контрагентами по уголовному делу о нарушениях в сфере государственных закупок.

Поступившие из следственных органов примеры также позволили обобщить и систематизировать наиболее типичные проблемы, возникающие в ходе использования в расследовании информации, полученной с помощью системы «Платон» и других информационных систем контроля за автомобильным транспортом. Значительная их часть связана с недостатком опыта работы с криминалистической информацией из рассматриваемых источников. Например, по уголовному делу о преступлении, предусмотренном статьей 264 Уголовного кодекса, от автотранспортного предприятия поступили сведения о скорости движения грузового автомобиля во время дорожного происшествия, полученные с помощью корпоративной телематической системы контроля за автопарком предприятия. Поступившая информация была оформлена письменной справкой. При этом в обвинительном заключении следователем указано, что «сведения о скорости движения автомобиля предоставлены системой «ГЛОНАСС». Представляется, что в данном случае неверное указание источника полученной информации о скорости движения автотранспортного средства может повлечь ее исключение судом из состава доказательственной базы по уголовному делу.

Кроме того, правовые проблемы возникают при использовании в уголовном процессе в качестве доказательств сведений о местоположении объектов, полученных с помощью технологии спутниковой навигации. К данной проблеме мы уже обращались в прошлых работах [3], и она связана с требованиями метрологического законодательства об обязательной сертификации и периодической поверке средств измерений, к которым, среди прочего, относятся и приборы спутниковой навигации. Данная проблема выходит за рамки криминалистики как науки и сферы профессиональной деятельности, затрагивая вопросы технического регулирования, государственного управления и других отраслей знаний.

Список цитируемой литературы:

1. Бессонов, А.А. Некоторые перспективные направления дальнейшего развития российской криминалистики / А.А. Бессонов // Академическая мысль. – 2019. – № 3(8). – С. 22–27.
2. Галкин, Д.В. Криминалистическое значение сведений, формируемых автоматизированными информационно-транспортными системами / Д.В. Галкин // Расследование преступлений: проблемы и пути их решения. – 2022. – № 2. – С. 108–113.
3. Галкин, Д.В. Измерительная информация в уголовном процессе: значение и правовой режим использования / Д.В. Галкин // Актуальные проблемы науки и практики: электрон. сб. науч. тр. по итогам науч. представит. мероприятий. – Хабаровск: РИО ДВЮИ МВД России, 2023. – Вып.12. – С. 375-378. [Электронный ресурс]. – URL: https://двюи.мвд.рф/Institut/Struktura/OTDELI/Redakcionno_izdatelskij_otdel/электронные-издания. (дата обращения: 24.12.2024)
4. Приговор Октябрьского районного суда г. Тамбова от 24 сентября 2018 г. по уголовному делу о преступлениях, предусмотренных ч. 4 ст. 159, ч. 3 ст. 30, ч. 4 ст. 159 УК РФ.
5. Скобелин, С.Ю. Цифровая криминалистика: объект и направления развития / С.Ю Скобелин // Российский следователь. – 2020. – № 4. – С. 42–44.
6. Смирнов, А.А. Технологические революции как фактор развития криминалистики / А.А. Смирнов // Вестник Московской академии Следственного комитета Российской Федерации. – 2022. – № 4. – С. 149–155.

Говорухин Д.С., ст. преподаватель
Россия, ФГКОУ ВО «Нижегородская академия МВД России»,
подполковник полиции, г. Нижний Новгород

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СФЕРЕ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШЕННЫМИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация

В статье анализируются обстоятельства, существенно осложняющих борьбу с преступлениями в сфере ИКТ, приводятся актуальные статистические сведения в сфере ИКТ-преступности, предлагаются меры повышения эффективности оперативно-служебной деятельности по противодействию данному виду преступности.

Ключевые слова: органы внутренних дел, преступления в сфере использования информационно-коммуникационных технологий, IT-преступность.

Глобальное развитие и совершенствование компьютерных технологий, доступные и адаптированные способы использования IP-адресов, серверов и ресурсов, в том числе находящихся вне юрисдикции Российской Федерации, детерминировали появление и неуклонный рост числа преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ). Стремительно развивающаяся архитектура виртуального пространства генерирует новые риски. Противоправная деятельность в этой области сопряжена с постоянным возникновением новых способов совершения преступлений, обеспечения анонимности преступников, а также расширением возможностей обширного охвата лиц, в отношении которых могут совершаться противоправные деяния.

Особую активность проявляют организованные преступные группы, которыми в указанных целях используются вредоносное программное обеспечение (включая вирусы-шифровальщики); фишинговые сайты; специальная техника; электронные платформы и колл-центры, осуществляющие звонки с подменных номеров; мессенджеры; виртуальные АТС; социальные сети; «SIM-боксы» и другие криминальные схемы. Международные преступные группы и сообщества ввиду трансграничности информационного пространства и отсутствия должного уровня межгосударственного взаимодействия успешно используют имеющийся в настоящее время фактор «уязвимости» в нормативно-правовом и организационно-техническом обеспечении дея-

тельности по противодействию ИКТ-преступности, нанося существенный материальный и репутационный вред гражданам и организациям Российской Федерации.

Существенное негативное влияние на криминогенную обстановку в сфере использования ИКТ оказывает сложная международная ситуация, в том числе связанная с деятельностью украинских спецслужб и неонацистских формирований, курируемых иностранным разведсообществом. Основная масса преступлений совершается транснациональными организованными преступными группировками, специализирующимися на мошенничествах, связанных с продолжающимися утечками персональных данных и расширением колл-центров, действующих с территории Украины.

Активно ведется деятельность по созданию и функционированию «финансовых пирамид», организация деятельности которых также сместилась в виртуальное пространство. Для продвижения псевдоинвестиционных и иных нелегальных проектов используются медийные личности, которыми рекламируется противоправная деятельность, обеспечивающая приток новых потенциальных потерпевших. Нередко цифровые площадки становятся местом реализации сомнительных информационных продуктов. Во многом на формирование такой ситуации влияет широкое развитие социальных сетей и иных форм интернет-коммуникации.

К числу обстоятельств, существенно осложняющих борьбу с преступлениями в сфере ИКТ, относятся возможность их совершения из любой точки мира с максимальным охватом широких слоев населения; использование средств анонимизации, криптовалют, цифровых ресурсов, зарегистрированных в недружественных странах; сложности процессуального закрепления цифровых следов преступлений.

Стратегией национальной безопасности Российской Федерации [1] борьба с ИКТ-преступлениями определена как одна из основных задач обеспечения национальной безопасности и условие устойчивого развития государства.

Согласно Доктрине информационной безопасности Российской Федерации [2] обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации и неприкосновенности частной жизни при использовании информационных технологий, признаны одним из пяти национальных интересов в информационной сфере.

В настоящее время Президентом Российской Федерации В.В. Путиным поручено создать систему эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий [3].

В нормативных правовых актах МВД России криминализация рассматриваемой сферы также определена как угроза государству, а активизация борьбы с преступлениями, совершаемыми с использованием ИКТ, – в качестве одного из приоритетных направлений деятельности МВД России в 2025 году.

Подразделения органов внутренних дел (далее – ОВД) обладают значительными силами и средствами для организации эффективного противодействия такого рода преступлениям, однако в настоящее время имеются различные проблемы, не позволяющие полноценно и своевременно решать задачи оперативно-розыскной деятельности в данном направлении. Для этого требуются применение новых тактических подходов; модернизация механизмов межведомственного взаимодействия; обобщение и распространение положительного опыта, а также совершенствование практики документирования преступлений рассматриваемой категории.

Для иллюстрации состояния преступности в рассматриваемой сфере приведем некоторые статистические данные ФКУ «ГИАЦ МВД России» за 2023 год.

Так, в 2023 году зарегистрировано 670 114 преступлений, совершенных с использованием ИКТ (по сравнению с 2022 годом рост составил 29,9%). При этом удельный вес преступлений, совершенных в сфере IT, составляет 34,8% от общего количества зарегистрированных преступлений.

За последние годы наблюдается устойчивая тенденция к увеличению количества преступлений в сфере IT. Использование сети «Интернет» в качестве средства коммуникации и коммерции, а также привлекательность информационно-телекоммуникационной среды повлияли на повышение уровня данного вида преступности. Лица, совершающие преступления, продолжают получать из даркнета готовый инструментарий для противоправной деятельности, в частности, программно-аппаратные решения, а также психологические методики воздействия («социальная инженерия»). Развитие современных технологий способствует появлению и стремительному развитию новых форм преступности.

Анализ совершенных противоправных деяний показывает, что все более широкое распространение получают хищения кредитных денежных средств, полученных как самими потерпевшими под непосредственным влиянием преступников, так и в результате их доступа к системам дистанционного банковского обслуживания или регистрации на сайтах микрофинансовых организаций под учетными данными граждан.

В целях повышения эффективности оперативно-служебной деятельности по противодействию данному виду преступности предпринят ряд мер организационного и практического характера:

1. При участии МВД России разработан Федеральный закон от 24 июля 2023 года № 369-ФЗ [4], предусматривающий предоставление оператору по переводу денежных средств права приостанавливать использование клиентом электронного средства платежа в случае нахождения информации о клиенте-получателе или его электронном средстве платежа в базе данных о попытках осуществления переводов денежных средств без добровольного согласия клиента. Также введена обязанность возмещения клиенту денежных средств, похищенных с его счета.

2. Федеральным законом от 13 июня 2023 года № 214-ФЗ [5] установлена возможность конфискации имущества, полученного в результате совершения преступлений, предусмотренных ч. 2–4 ст. 272, ст. 273, ч. 2 ст. 274, ст. 274.1 УК РФ.

3. В целях противодействия использования сервисов аренды абонентских номеров постановлением Правительства Российской Федерации от 15 сентября 2023 года № 1505 [6] к угрозам безопасности функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования отнесено предоставление доступа к информации или информационным ресурсам, позволяющим получать услуги связи и (или) их заказа, а также передачи организатором сервиса обмена мгновенными электронными сообщениями без идентификации пользователей.

4. Роскомнадзором во взаимодействии с МВД России осуществляется развитие информационной системы «Антифрод» [7], функционал которой позволяет при установлении соединений информировать оператора связи о необходимости блокировки соединений в зависимости от наличия или отсутствия информации об их инициировании. Информация о всех голосовых вызовах поступает в единую систему обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования, а оператор связи в автоматическом режиме запрашивает и получает данные об активности номера. Если система подтверждает, что вызов реальный и номер не подменный, то устанавливается безопасное соединение. Если такого подтверждения нет, решение о его отклонении принимает оператор связи.

5. Приняты меры по блокировке соединений с использованием подменных номеров, осуществляемых от лица правоохранительных и других органов государственной власти. В рамках указанной работы в Минцифры России предоставлена информация обо всех абонентских

номерах, используемых МВД России и его территориальными подразделениями, которые опубликованы в официальных источниках.

Проведенный анализ оперативно-служебной деятельности подразделений ОВД по данной линии работы, а также результаты интервьюирования сотрудников, проходивших обучение по дополнительным профессиональным программам повышения квалификации на базе Нижегородской академии МВД России в 2023–2024 годах, позволили выявить ряд проблем, с которыми сталкиваются сотрудники в своей профессиональной деятельности.

Одна из них – длительные сроки получения информации, необходимой при планировании и проведении оперативно-розыскных мероприятий (далее – ОРМ). Так, затруднен оперативный доступ к информации о движении денежных средств по лицевым счетам абонентских номеров (банковских карт); сведениям о реальных владельцах абонентских номеров (банковских карт), об аккаунтах пользователей в социальных сетях, получаемых от операторов сотовой связи, интернет-провайдеров, администраторов интернет-ресурсов, электронных бирж, кредитных организаций.

Необходимо отметить позитивные тенденции в данном направлении, связанные с внесением в 2022 году изменений в действующее законодательство [8], определивших сроки предоставления справок по операциям и счетам юридических лиц и индивидуальных предпринимателей; операциям, счетам и вкладам физических лиц из кредитных организаций. Однако данные новеллы даже после установления 10-дневного срока предоставления таких сведений органу, уполномоченному на осуществление оперативно-розыскной деятельности, решают возникающие сложности лишь частично.

В случаях отслеживания длительной цепочки сомнительных операций истребование подобных данных сопряжено с необходимостью неоднократного получения решения суда, в связи с чем срок получения таких сведений может увеличиваться до нескольких месяцев.

В качестве решения указанной проблемы может быть предложено внесение изменений в действующие нормативные правовые акты в части разрешения на получение интересующих сведений от кредитных организаций, интернет-провайдеров, администраторов интернет-ресурсов, сотовых операторов и иных уполномоченных субъектов на основании постановления руководителя органа, уполномоченного на осуществление оперативно-розыскной деятельности.

В качестве альтернативных решений могут выступать организация передачи соответствующих документов, разрешающих проведение ОРМ, в суд и получение судебного решения посредством электронного

документооборота с использованием электронной подписи и квалифицированного сертификата ключа его проверки с соблюдением необходимых требований по защите сведений, составляющих государственную тайну [9].

Необходимо отметить, что в настоящее время упрощен порядок информационного взаимодействия между Центральным банком Российской Федерации и МВД России [10]. С октября 2023 года Банком России [11] на основании полученных от МВД России сведений о совершенных противоправных действиях оперативным подразделениям предоставляется информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента – автоматизированной системе обработки инцидентов «ФинЦЕРТ» (далее – АСОИ «ФинЦЕРТ»).

Порядок информационного обмена, форма и перечень предоставляемых сведений закреплены в соглашении между указанными сторонами взаимодействия, что позволяет сократить время получения необходимой информации о денежных переводах и их происхождении. Представляется целесообразным последующая интеграция оперативно значимой информации, полученной из АСОИ «ФинЦЕРТ», в подсистему интегрированного банка данных «Дистанционное мошенничество».

Следует отметить, что в настоящее время посредством сервиса межведомственного взаимодействия ИСОД МВД России между некоторыми кредитными учреждениями (ПАО «Сбербанк», АО «Альфабанк», ПАО «ВТБ» и др.) и ОВД действует упрощенный порядок получения запрашиваемых сведений посредством электронного документооборота в рамках заключенных соглашений.

В последнее время все больше финансовых операций осуществляются через криптовалютные биржи и различные платформы-миксеры. Однако, получить необходимые сведения от них затруднительно по причине отсутствия обязательной верификации пользователей. Возникают сложности и при получении информации о транзакциях, совершенных с использованием децентрализованных криптовалютных бирж. Данные факты связаны с особенностями их функционирования, которые заключаются в отсутствии конкретного руководящего состава (к которому можно было бы применить санкции или предъявить требования), а также главного контролирующего узла или сервера, хранящего данные.

В качестве решения может быть предложена обязательная идентификация личности пользователя при входе на соответствующие интернет-платформы и приложения, администрируемые с территории Российской Федерации, с использованием аккаунта портала федераль-

ной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» («Госуслуги»).

Ключевыми проблемами в противодействии преступлениям рассматриваемой категории выступают идентификация и обнаружение владельцев и пользователей интернет-ресурсов, мобильных устройств, счетов в электронных платежных системах, в том числе критовалютных кошельков.

К числу наиболее распространенных средств по обеспечению анонимности в сети «Интернет» и сетях связи при совершении преступлений с использованием IT-технологий относятся:

– приобретение мобильных телефонов с измененным программным обеспечением, не позволяющим установить предыдущие номера IMEI, или без соответствующего идентификатора;

– использование сим-карт, не имеющих регистрационных данных или зарегистрированных на вымышленных или третьих лиц;

– использование дистанционных финансовых технологий, позволяющих избежать фактической идентификации лиц, осуществляющих управление счетом, и личного присутствия при проведении платежа (мобильный банкинг, электронные кошельки);

– возможность использования в неправомерных целях P2P-сервисов, в том числе посредством оформления банковских карт, электронных кошельков на подставных лиц;

– использование преступниками механизмов, позволяющих обеспечить анонимность совершаемых операций, таких как «миксеры», разделяющие платеж на несколько транзакций в целях дальнейшей отправки каждой из них с нового адреса на выборку не связанных друг с другом криптокошельков, а также криптовалют с повышенной анонимностью (Dash, Zcash, Monero и т. п.), технология которых не позволяет отслеживать номера кошельков и размеры переводов;

– приобретение различными способами банковских карт у лиц, не имеющих прямой связи с преступниками, в том числе с помощью посредников или сети «Интернет».

У лиц, занимающихся преступной деятельностью, сохраняется возможность избегать идентификации путем использования программных технологий VPN, TOR, позволяющих менять IP-адрес пользователя в сети «Интернет», создавать нераспознаваемые IP-адреса, а также применять технологии «подменных» абонентских номеров посредством SIP и Voip-телефонии.

Применяемые способы шифрования данных на распространенных интернет-сервисах не позволяют определять IP-адреса пользователей, отслеживать их активность, устанавливать данные пользователей. Су-

ществующий порядок оформления идентификационных модулей операторами сетей подвижной радиотелефонной связи порождает комплекс проблем, связанных с установлением абонента в процессе раскрытия преступлений.

В связи с изложенным обстоятельством предлагается расширение внедрения в практику оперативных подразделений установления биометрических данных, а также контроля иной информации через систему фиксации ее ввода и вывода при проведении ОРМ в отношении лиц, обоснованно подозреваемых в совершении преступлений с использованием IT-технологий.

Объективные сложности, возникающие при отслеживании операций с криптовалютой, могут быть решены посредством повышения уровня эффективности взаимодействия с Федеральной службой по финансовому мониторингу (Росфинмониторингом), использующей в своей деятельности сервис мониторинга криптовалютных транзакций «Прозрачный блокченйн». Данный сервис позволяет отследить криптовалютные операции с применением технологий искусственного интеллекта, а также выявить конечных бенефициаров активов.

Среди нерешенных проблем остаются недостаточное правовое урегулирование вопросов, связанных с порядком выпуска, обращения и введения ограничительных процедур в отношении виртуальных активов; отсутствие механизма оперативной блокировки счетов и приостановления (заморозки) переводов денежных средств, используемых для расчетов в криптовалюте (цифровой валюте); трудности в выявлении и возврате активов, выведенных на криптобиржи, не являющиеся субъектами российского правового регулирования.

Предложенные решения могут способствовать совершенствованию оперативно-служебной деятельности как подразделений ОВД, так и правоохранительных органов в целом.

Список цитируемой литературы:

1. О Стратегии национальной безопасности Российской Федерации: указ Президента Рос Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27. – Ч. 2. – Ст. 5351.
2. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Рос. Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.
3. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: указ Президента Рос. Фе-

дерации от 7 мая 2024 г. № 309 // Собрание законодательства Российской Федерации. – 2024. – № 20. – Ст. 2584.
4. О внесении изменении в Федеральный закон «О национальной платежной системе»: федер. закон Рос. Федерации от 24 июля 2023 г. № 369-ФЗ // Собрание законодательства Российской Федерации. – 2023. – № 31. – Ч. 3. – Ст. 5795.
5. О внесении изменения в статью 104.1 Уголовного кодекса Российской Федерации: федер. закон Рос. Федерации от 13 июня 2023 г. № 214-ФЗ // Собрание законодательства Российской Федерации. – 2023. – № 25. – Ст. 4403.
6. О внесении изменения в Правила централизованного управления сетью связи общего пользования: постановление Правительства Рос. Федерации от 15 сентября 2023 г. № 1505 // Собрание законодательства Российской Федерации. – 2023. – № 39. – Ст. 7023.
7. О внесении изменений в Федеральный закон «О связи»: федер. закон Рос. Федерации от 2 июля 2021 г. № 319-ФЗ // Собрание законодательства Российской Федерации. – 2021. – № 27. – Ч. I. – Ст. 5147.
8. О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 9 Федерального закона «Об оперативно-розыскной деятельности»: федер. закон Рос. Федерации от 1 апреля 2022 г. № 77-ФЗ // Собрание законодательства Российской Федерации. – 2022. – № 14. – Ст. 2190.
9. Говорухин, Д. С., Рогов, А.В. Проблемные вопросы противодействия экономическим преступлениям, совершаемым с использованием IT-технологий, и возможные пути их решения / Д.С. Говорухин, А.В. Рогов // Вестник МВД России. – 2023. – № 5. – (182). – С. 85–94.
10. О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе»: федер. закон Рос. Федерации от 20 октября 2022 г. № 408-ФЗ // Собрание законодательства Рос. Федерации. – 2022. – № 43. – Ст. 7271.
11. О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 г. № 161-ФЗ (в ред. от 28 декабря 2024 г.) // Собрание законодательства Рос. Федерации. – 2011. – № 27. – Ст. 3872.

Голубовский В.Ю., д-р. юрид. наук, профессор, гл. науч. сотр.
ФКГУ «Всероссийский научно-исследовательский институт
МВД России»,
генерал-майор полиции в отставке,
действительный государственный советник Российской Федерации
3 класса,
почетный сотрудник МВД России,
почетный работник высшего профессионального образования,
член-корреспондент РАЕН
г. Москва

Противодействие современным киберугрозам

Аннотация

В статье раскрывается, что реальность нашего времени подтверждает глобальный рост уровня информатизации мирового сообщества, что обусловлено масштабами внедрения в повседневную жизнь человека различных технологий, которые стремительно совершенствуются, эволюционируя в ранее неизвестную информационную индустрию. Особую общественную опасность представляют киберугрозы, инструментом совершения, которых выступает искусственный интеллект. Работающие на его основе программы и системы обладают высоким уровнем самодетерминации, что делает менее прогнозируемым результат их деятельности для пользователя или разработчика. В этой связи, необходимо выявить тенденции в сфере кибербезопасности, для своевременного реагирования на появление новых киберугроз.

Ключевые слова: искусственный интеллект, киберугрозы, кибербезопасность, тенденции, противодействие

Международное сообщество в настоящее время все активнее говорит о проблемах безопасности, которая включает Интернет или более широко киберпространство [2, С. 339]. Несмотря на стремительные темпы информатизации, действующее отечественное законодательство не содержит адекватные средства воздействия на отклоняющееся поведение в информационной сфере, что не способствует формированию и развитию благонадежного информационного общества. В этой связи, в соответствии с подп. «д» п. 20 Указа Президента Российской Федерации от 01.12.2016 № 642 (в ред. от 15.03.2021) «О Стратегии научно-технологического развития Российской Федерации» [5] приоритетами научно-технологического развития Российской Федерации следует считать те направления, которые позволят получить научные результаты, обеспечивающие противодействие техногенным, биогенным, со-

циокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства.

Многочисленные кибератаки и кражи личных данных свидетельствуют, что изощренность и интенсивность атак на средства поддержания кибербезопасности нарастают, что может иметь более широкие политические и экономические последствия. Киберпреступления становятся все привлекательнее, интереснее, а киберпреступники все изобретательнее, следовательно, и кибербезопасность тоже становится более интеллектуальной и обеспечивает оперативную реакцию на самые современные атаки. Поскольку выявить взлом компьютеров становится все сложнее, требования к защите организаций от киберугроз активно повышаются.

Лицо, реализуя свой преступный умысел, физически может находиться на территории одного государства, а объекты уголовно-правовой охраны, в отношении которых осуществляются преступные намерения, могут иметь иную национальную локацию. В этой ситуации возникает проблема распределения юрисдикционных полномочий данных государств в отношении всемирной компьютерной сети Интернет.

Новые технологии и приложения преобразуют организации, учреждения, повышая тем самым возможности реагировать на стремительно меняющиеся экономические условия и настроения клиентов, что предполагает приоритет эффективных решений для гибридной облачной безопасности. И бизнес, и киберпреступники будут использовать искусственный интеллект.

Искусственный интеллект начинает занимать центральное место в сфере кибербезопасности; он включает в себя машинное обучение, потенциально способен распознавать угрозы по мере их возникновении и реагировать на них [3].

Автоматизация позволит эффективно анализировать атаки и реагировать на них. Автоматизация и, в частности, робототехническая автоматизация технологических процессов в области кибербезопасности расширяются, в том числе в выявлении и анализе происшествий и реагировании на них. Группы технической поддержки и реагирования на инциденты нуждаются во все большей автоматизации, чтобы справляться с частотностью непрекращающихся кибератак.

Автомобили без водителя, умные города, умные дома, умные часы и виртуальные помощники, все они являются составляющими Интернета вещей и обретают все большую популярность. По мере все более широкого использования Интернет вещей они также становятся основными объектами кибератак. С учетом возникающих угроз зако-

нодательные рамки или руководства, касающиеся проблем безопасности, оказываются насущной необходимостью.

Если вести речь о перспективе, то планируется рост числа атак против малого бизнеса и физических лиц. Цифровизация предполагает, что эффективная безопасность перестает быть желательной, а становится обязательной. Число атак будет множиться, и в ближайшем будущем внимание киберпреступников будет привлекать все большее число мелкого бизнеса и даже отдельных граждан.

По итогам 11 месяцев 2024 года россияне потеряли 168 млрд. рублей в результате дистанционных мошенничеств**.** Зарегистрировано более 702 тыс. IT-преступлений, что на 14,3% больше, чем за аналогичный период 2023 года. К числу наиболее распространенных схем дистанционного мошенничества следует отнести: «Звонок от нотариуса», «На связи „начальник“», «Перерасчёт пенсии» [1].

Особое значение имеют законы о защите личных данных. Динамичная природа кибербезопасности приводит к отставанию регулирования киберпространства. В свете громких инцидентов с похищением данных клиенты выражают беспокойство и требуют более надежных мер защиты. Так, с 11 декабря 2024 года вступила в силу ст. 272.1 Уголовного кодекса Российской Федерации**,** которая устанавливает уголовную ответственность за сбор, передачу и хранение данных, полученных незаконным путём, включая создание ресурсов для их распространения [4].

Крупные организации уже проделали серьезную работу, чтобы защититься от нападений. Становится проще проводить атаки на мелкие и средние компании, у которых может не быть в наличии адекватных ресурсов и средств защиты, чтобы обезопасить себя. Мелким компаниям следует еще раз оценить свою защищенность и обеспечить внедрение адекватных мер и средств контроля, способных предохранить от современных кибератак.

Список цитируемой литературы:

1. Исторический рекорд! Посчитали, как для мошенников прошёл 2024-й. Исчезнут ли кибераферисты в 2025 году? [Электронный ресурс]. – Дзен: блог – платформа. – URL: https://dzen.ru/a/Z3qy16JA-1YogTIC (дата обращения: 14.01.2025).

2. Кунц, Е. В. Современные киберугрозы и специфика личности, их совершающей / Е. В. Кунц // Техника и безопасность объектов уголовно-исполнительной системы : сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 года. – Воронеж: Строки, 2024. – С. 339–342.

3. Симуляция жизни: каким будет мир через несколько лет при развитии цифровых двойников. [Электронный ресурс]. – Форбс. – URL: https://www.forbes.ru/tekhnologii/521909-simulacia-zizni-kakim-budet-mir-cerez-neskol-ko-let-pri-razvitii-cifrovyh-dvojnikov?ysclid=m5wbco0baf453068524 (дата обращения: 14.01.2025).
4. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 28 декабря 2024 г.) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
5. О Стратегии научно-технологического развития Российской Федерации: указ Президента Рос. Федерации от 1 декабря 2016 г. № 642 (в ред. от 15 марта 2021 г.) // Собрание законодательства Российской Федерации. – 2016. – № 49. – Ст. 6887.

Дук Ю.И., канд. юрид. наук, доцент, доцент кафедры
ФГБОУ ВО «Липецкий государственный технический университет»,
г. Елец

Киберпреступность в России: пути противодействия

Аннотация

В статье рассматриваются вопросы киберпреступности в Российской Федерации, ее уровень и динамика за последние двадцать лет, влияние на общий уровень криминализации населения, ущерб, наносимый государству и населению страны. Автор рассматривает причины и условия, способствующие совершению киберпреступлений, и пути противодействия.

Ключевые слова: киберпреступность, причины, условия, социальные сети.

Киберпространство – какое емкое и многообразное понятие для современного человека. Появившееся в результате разработки и внедрения в жизнь общества цифровых технологий, позволивших создать самые разнообразные платформы, прочно вошедших не только в экономику, финансы и производство, но и повседневную жизнь каждого отдельно взятого человек. Появление информационно-телекоммуникационных сетей, в том числе и сети «Интернет», позволило решить огромное количество проблем от космоса и медицины до быта человека. Киберпространство, сформированное цифровой составляющей, позволило вывести различные стороны жизни общества на более высокий уровень, и это касается не только промышленности,

финансов, но и экономики в целом. Эта тенденция затронула практически все страны мирового сообщества. Киберпространство не только способствует повышению производительности труда, улучшает условия жизни человека, но и влияет на формирование мировоззрения, влияет на морально этические стороны его жизни, ориентацию на те или иные ценности, создает свою специфическую киберкультуру.

Еще каких-то тридцать лет назад население нашей планеты в основной своей массе даже не могло себе представить, что такое киберпространство и насколько глубоко оно проникнет в жизнь каждого человека, отдельных групп людей и всего мирового сообщества. И несмотря на то, что некоторые представители старшего поколения так и не смогли влиться в круг пользователей интернет пространства по ряду объективных и субъективных причин, количество пользователей на сегодняшний день по некоторым данным составляет более пяти миллиардов человек.

Такое огромное количество пользователей как нельзя лучше демонстрирует привлекательность цифровых технологий и их востребованность, а в некоторых случаях и необходимость, как для представителей государственных органов и бизнеса, так и для отдельных граждан.

Современное российское общество не является исключением, и стратегия развития страны, сформулированная президентом Российской Федерации В.В. Путиным, включает в себя, в том числе и использование искусственного интеллекта. В частности, Президент поручил кабмину еще в конце декабря 2020 года подготовить стратегии цифровой трансформации для десяти ключевых отраслей российской экономики и социальной сферы. «Уже в ближайшее время правительству необходимо утвердить стратегии цифровой трансформации десяти ключевых отраслей отечественной экономики и социальной сферы, практические меры по внедрению в их работу алгоритмов искусственного интеллекта, чтобы они стали надежными помощниками врачей, преображали наши города, широко применялись в коммунальном хозяйстве, на транспорте, в промышленности», - сказал он. Путин заявил, что все это должно самым позитивным образом отразиться на качестве жизни людей [8].

Однако наряду с позитивными последствиями использования цифровых технологий и искусственного интеллекта мировое сообщество и наше государство в частности столкнулись и с серьезным негативом в виде киберпреступности, то есть преступности в сфере высоких технологий с использованием злоумышленниками компьютеров, компьютерных сетей и иные электронных устройств, являющихся объектом, способом или средством достижения преступного результата.

Профессор В.А. Номоконов дает следующее определение киберпреступности – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [10].

Возможность проникновения в любую сферу жизнедеятельности человека с помощью компьютера и телекоммуникационных систем, особенно сети Интернет, позволило киберпреступникам расширить свою преступную деятельность не только в границах государства проживания, но и далеко за его пределами.

Низкий уровень киберпреступности, регистрируемой в нашей стране в начале двухтысячных годов, находился в пределах общественной терпимости и не вызывал у государства особой тревоги на фоне общей регистрируемой преступности в Российской Федерации. Так в 2003 году МВД РФ зарегистрировало 7540 преступлений в сфере компьютерной информации, предварительное следствие по которым обязательно, что составило от общего количества зарегистрированных преступлений (2756398) всего 0,27%, и даже это процентное соотношение имело тенденцию к снижению. В 2011 году было зарегистрировано 2698 преступлений, что составило от общего количества зарегистрированных преступлений (2407807) 0,11% [9].

Однако преступный элемент не ограничивался совершением только преступлений в сфере компьютерной информации, а использовал цифровые технологии при совершении самых разнообразных преступлений. Для систематизации и отражения уровня и динамики киберпреступлений в соответствии с Указанием Генеральной прокуратуры РФ и МВД России от 27 декабря 2017 г. № 870/11/1 «О введении в действие перечней статей Уголовного кодека Российской Федерации, используемых при формировании статистической отчетности» [5], данная категория преступлений была выделена в отдельную позицию, озаглавленную как преступления совершенные с использованием компьютерных и телекоммуникационных технологий. Это объединение позволило увидеть полную картину регистрируемой киберпреступности, для определения стратегии противодействия. Таким образом, в 2017 году МВД РФ было зарегистрировано 90587 преступлений, в 2023 их количество составило уже 676951 [9], а это семикратное увеличение регистрируемой киберпреступности в РФ за последний семилетний период. Данное положение дел вызвало серьезную обеспокоенность руководителей правоохранительных органов и Центробанка РФ, в результате чего в конце 2024 года было проведено координационное совещание под председательством

Генерального прокурора РФ Игоря Краснова по вопросу противодействия киберпреступности. Генпрокурор РФ сообщил, что киберпреступность получила широкое распространение, появились новые способы преступных посягательств, совершаемые в отношении социально уязвимых категорий граждан РФ. Активизировалась организованная преступность, использующая фишинговые сайты, колл-центры, различные электронные платформы и финансовые пирамиды. Так же отметил, что наряду с положительными результатами противодействия киберпреступности имеется ряд недостатков, тормозящих позитивный процесс противодействия. Среди этих недостатков низкая раскрываемость данного вида преступлений, которая в 2024 году составила 25,0%, что характеризуется шаблонностью и безынициативностью проводимой оперативной работы, отсутствием наступательности, и слабой эффективностью предварительного расследования [3].

Обеспокоенность общества справедлива и вызвана огромным валом преступных проявлений, практически каждый житель нашей страны ощутил на себе влияние киберпреступности. Преступники, используя компьютерные и телекоммуникационные технологии, проявляют свою наибольшую активность при совершении хищений денежных средств посредством мошенничества, похищения конфиденциальной информации, шпионажа, распространении наркотических средств, детской порнографии, прибегают к дезорганизации работы информационных систем, тем самым расшатывая систему безопасности сраны, возбуждая сепаратизм, экстремизм, вызывая недовольство проводимой политикой государства и ее руководством.

Не один десяток раз каждому гражданину нашей страны, пользующемуся услугами сотовой связи, поступали звонки от мошенников, пытающихся обманным путем под любыми предлогами похитить денежные средства. Так, в 2023 году мошенникам удалось успешно совершить больше одного миллиона хищений денежных средств на общую сумму 15,8 млрд. рублей, осуществить вербовку россиян для совершения террористических актов на территории Российской Федерации, таких как поджоги военкоматов и релейных шкафов на железной дороге, убийство журналистов, руководителей администраций различных уровней, военнослужащих, и этот перечень, к сожалению, не полный.

Сложность противодействия киберпреступности в глобальных компьютерных сетях с использованием персонального компьютера и сотового телефона, позволяющего осуществлять доступ в сеть Интернета, состоит в ее особенностях. Так, по мнению А.Л. Осипенко к ним относятся:

1) высокая латентность совершаемых преступлений со сложной инфраструктурой и анонимностью пользователей.

2) трансграничный характер сетевых преступлений, при котором жертва и злоумышленник могут находиться на территории разных государств;

3) высокоинтеллектуальная и специфическая подготовка преступной деятельности;

4) сложность, нестандартность, многообразие, возможность частого обновления способов и средств;

5) автоматизация процесса преступного деяния и его групповой характер, как сообщников, так и жертв;

6) дистанционный характер преступных действий, отсутствие непосредственного контакта с жертвой и как следствие ее неосведомленность [6, С. 109–110].

Российские ученые среди причин, создающих дополнительные сложности в расследовании и активном противодействии киберпреступности, отмечают недостаточное владение субъектами расследования киберпреступлений специальными познаниями и опытом работы в области цифровых технологий. Второй причиной признают открытость интернет среды, позволяющей совершать преступные действия беспрепятственно, выбирая такую правовую среду, которая соответствует их целям. При этом выбирают не только среду, но и государство, в котором совершаемые ими деяния не подпадают под уголовную ответственность, позволяя злоумышленникам действовать, безнаказанно совершая преступления с территории своей страны, особенно если руководство страны или ее спецслужбы поддерживают или инициируют данные действия. Примером является Украина, на территории которой работают сотни коллцентров, направленных на хищение денежных средств у россиян.

Российское государство, по мнению некоторых отечественных ученых и политиков, столкнулась с высокоинтеллектуальным противником, имеющим на своем вооружении современную технику и разрабатывающим свои методы совершения преступлений настолько быстро, что сложная и медлительная система государственного принятия решения по противодействию тому или иному способу совершения киберпреступления просто не успевает реагировать. Государство постоянно идет с опозданием в силу того, что принятие законов и разработка методик противодействия – процесс достаточно длительный, нежели разработка очередной преступной киберсхемы. Для эффективной борьбы с киберпреступностью необходимы совершенно новые иногда нестандартные подходы, иная стратегия, которая отличалась бы от принятых, традиционных методик противодействия преступности.

Одним из таких подходов может являться перераспределение вектора борьбы с киберпреступностью в гражданско-правовую плоскость

ответственности. Совершенно справедливым является включение в обязанность всех производителей и распространителей объектов, продуктов, систем, программ и т.д. обеспечение безопасности, как для отдельного пользователя, так и для страны в целом. Одним из примеров такого подхода на наш взгляд является поручение Президента Владимира Путина правительству и ЦБ РФ рассмотреть возможность создания механизма выплаты банками и кредитными организациями компенсаций гражданам, у которых мошенники украли деньги со счетов [2]. С выработкой такого механизма будет поставлен надежный заслон мошенникам и данная система хищения денежных средств прекратит свое существование без использования уголовно-правовых механизмов.

Так же для противодействия преступлениям с использованием телекоммуникационных технологий, на наш взгляд, необходима разработка и скорейшее внедрение отечественных продуктов в области цифровых технологий с целью отказа от различных иностранных платформ, не принимающих российских общегосударственных условий защиты граждан от преступных посягательств. Это относится и к социальным сетям, вошедшим прочно в жизнь нашего общества. По данным ВЦИОМ 86% россиян пользуются хотя бы одной социальной сетью или мессенджером с коммуникационным функционалом (ВКонтакте, WhatsApp, Telegram, TikTok, Одноклассники и т.д.). Новостные сообщества возглавляют рейтинг самых популярных подписок российских пользователей социальных сетей (77%). Далее с ощутимым отрывом идут образовательные (41%), юмористические (35%), развлекательные (33%) и научные (30%) сообщества [4].

Действительно, социальные сети являются неотъемлемой частью современного российского общества, однако кроме положительных сторон несут и криминальное давление, позволяя злоумышленникам совершать большое количество преступных деяний от мошенничества с хищением денежных средств до торговли наркотиками, детской порнографии, экстремизма и терроризма. Примером противоправной деятельности с использованием социальных сетей TikTok и ВКонтакте является призыв к несовершеннолетним россиянам выходить на протесты в поддержку Навального, беспорядки в Махачкалинском аэропорту, а также серия антисемитских атак в Нальчике, Хасавьюрте, Черкесске. Все эти беспорядки, в том числе и протесты «навальнят» были спровоцированы агентами иностранных спецслужб, которые использовали социальные сети для распространения слухов о размещении в Дагестане еврейских беженцев, эвакуировавшихся из Израиля после вторжения ХАМАС. И данные факты не являются единичными.

Одним из эффективных методов противодействия киберпреступности на бытовом уровне, который мы поддерживаем, является ограничение контента для несовершеннолетних. Будут ли такие ограничения работать и возможно ли их применение повсеместно - достаточно спорный вопрос. При этом наиболее популярные платформы принадлежат иностранным разработчикам, и воздействие со стороны государства на распространяемую информацию на данных платформах серьезно ограничено.

Так, WhatsApp, Telegram, TikTok, Facebook разработаны и принадлежат гражданам иностранных государств, проводящих враждебную политику против Российской Федерации, за исключением TikTok, которая принадлежит китайской компании ByteDance. Даже основатель Telegram и ВКонтакте Павел Дуров, имеющий гражданство четырех стран, уехал из России после того как ФСБ предприняло попытки получить доступы к ключам шифрования Telegram, хотя спецслужбам США после ареста во Франции выдал данные тысяч пользователей [1].

Средства массовой информации, коими являются и социальные сети, в обязательном порядке должны находиться под строгим контролем государства и его спецслужб, именно контролем, не подвергаться цензуре, а отвечать требованиям моральных и этических норм, декларируемых в нашем государстве, принадлежать государству, российским общественным организациям и объединениям. В настоящее время большинство средств массовой информации принадлежат частному капиталу. Вот что в свое время говорил В.И. Ленин о средствах массовой информации:

1) «Свобода печати во всём мире, где есть капиталисты, есть свобода покупать газеты, покупать писателей, подкупать и покупать, и фабриковать «общественное мнение» в пользу буржуазии».

2) «Буржуазная свобода печати — это есть свобода богатых людей покупать газеты и создавать нужное общественное мнение».

3) «Капитализм делал из газет капиталистические предприятия, орудия наживы для богачей, информации и забавы для них, орудия обмана и одурачения для массы трудящихся» [7].

Необходимы срочная разработка и внедрение своих российских социальных сетей и мессенджеров, защищенных от иностранного вмешательства. Существует же Государственная граница России, проходящая по суше, воде и воздушному пространству, которая охраняется специальными войсками от несанкционированного, враждебного проникновения, так почему отсутствует таковая и в цифровом пространстве, почему по территории нашей страны вольно через интернет и социальные сети гуляют все кому не лень, в том числе и наши откровенные враги и различного рода преступники, совершая в отношении

наших граждан, критически важных объектов и государственного порядка управления различные преступления, разжигают сепаратистские настроения, совершают террористические акты? На наш взгляд, для снижения киберпреступности необходимо добиться полного импортозамещения и в сфере цифровых технологий.

Список цитируемой литературы:

1. ВЦИОМ. Новости: Социальные сети и мессенджеры: вовлеченность и предпочтения [Электронный ресурс] – Режим доступа: URL // https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennost-i-predpochtenija. (Дата обращения: 13.01.2025).
2. Дуров сломался? Основатель Telegram начал сотрудничать с американскими спецслужбами после ареста во Франции [Электронный ресурс] – Режим доступа: URL // https://dzen.ru/a/Z3-jIibj0llJP_CX (Дата обращения: 13.01.2025).
3. Ленин о средствах массовой информации. [Электронный ресурс] – Режим доступа: URL // https://yandex.ru/search/?text=ленин+о+средствах+масовой+информации&clid=2270456&search_source=dzen_desktop_safe&src=suggest_W&lr=10713 (Дата обращения: 13.01.2025).
4. Новости - Генеральная прокуратура Российской Федерации. [Электронный ресурс] – Режим доступа: URL // https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092 (дата обращения 05.01.2025).
5. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропинина // Криминология вчера сегодня завтра – 2012.- №1 (24). – С.48.
6. Осипенко, А.Л. Сетевая компьютерная преступность: теория и практика борьбы [Текст] : монография / А. Л. Осипенко ; М-во внутренних дел Российской Федерации, Омская акад.. — Омск : Омская акад. МВД России, 2009. — 479 с. : 21 см.; ISBN 978-5-88651-445-2 (в пер.).
7. Официальный сайт МВД РФ. [Электронный ресурс] – Режим доступа: URL // https://mvd.ru/folder/101762. (дата обращения 05.01.2025).
8. Перечень N 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации \ КонсультантПлюс. [Электронный ресурс] – Режим доступа: URL // https://www.consultant.ru/document/cons_doc_LAW_451498/4b19951cd8806522f08eedf31686410dca97465/. (дата обращения 05.01.2025).
9. Путин заявил о необходимости цифровой трансформации России – ТАСС. [Электронный ресурс]. – Режим доступа: URL

https://tass.ru/ekonomika/10172635?ysclid=m5w6u77d9y68075182 (Дата обращения: 13.01.2025).
10. Путин поручил подготовить для банков правила выплат клиентам, обманутым мошенниками [Электронный ресурс] – Режим доступа: URL // https://www.interfax.ru/business/880655 (Дата обращения: 13.01.2025).

Дягилев А.А., канд. юрид. наук, доцент, нач. кафедры
ФГКОУ ВО «Нижегородская академия МВД России»,
полковник полиции, г. Нижний Новгород

Раскатов Р.А., заместитель начальника ОБК,
ГУ МВД России по Нижегородской области,
майор полиции, г. Нижний Новгород

Противодействие вовлечению несовершеннолетних в противоправную деятельность с использованием сети Интернет

Аннотация

В статье рассматриваются способы вовлечения несовершеннолетних в противоправную деятельность с использованием сети Интернет. Дается характеристика основных информационных ресурсов, при помощи которых осуществляется деструктивное воздействие на подрастающее поколение. Авторами предлагается механизм информационного противодействия вовлечению детей в совершение преступлений.

Ключевые слова: несовершеннолетние, противоправная деятельность, сеть Интернет, информационные технологии.

Информационные технологии сейчас являются неотъемлемой частью жизни современного человека. Особенно актуально это утверждение для представителей молодого поколения, детей и подростков, которые большую часть своей коммуникации перенесли в цифровую среду. Вместе с тем, особенности подобного рода он-лайн общения порождают не только удобства, но и создают угрозообразующие факторы, связанные с активным использованием преступниками открывшихся технических возможностей для достижения своих противоправных целей.

Стоит согласиться с мнением профессора В.И. Шарова, в части того, что в развитие информационных технологий, как породило ранее не существовавшие виды уголовных деликтов, так и позволило традиционным преступлениям получить новый импульс развития, в результате перехода в цифровую среду [8, с. 6]. Не случайно одним из прио-

ритетов в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, обозначено обеспечение государственной защиты интересов российских граждан в информационной сфере [3].

Также стоит отметить, что современная геополитическая ситуация, накладывает отпечаток на формирование новых криминальных угроз. Так, Президент Российской Федерации В. В. Путин, выступая на расширенной коллегии МВД России в апреле 2024 года, обратил внимание, что почти на треть увеличилось число доказанных фактов противоправной деятельности в сети Интернет, совершаемых в организованных формах. При этом значительная угроза исходит из-за рубежа, прежде всего с территории Украины [5]. Внешние деструктивные силы и связанные с ними представители российского общества, в попытках дестабилизации обстановки в нашей стране все активнее используют различные приемы вовлечения молодежи в противоправную деятельность. «В условиях глобализации информационных потоков и развития способов информационного воздействия на человека несовершеннолетние являются наиболее восприимчивой возрастной группой в контексте склонения к девиантному поведению» [4].

В настоящее время в сети Интернет функционирует целый ряд информационных ресурсов, при помощи которых осуществляется деструктивное воздействие на подрастающее поколение и вовлечение отдельных его представителей в совершение преступлений. К числу которых можно отнести группы в социальных сетях и мессенджерах, а также другие Интернет ресурсы:

– пропагандирующие экстремистскую и террористическую идеологию (в том числе движения «А.У.Е», «Колумбайн», «М.К.У» и др.), а также вовлекающие представителей молодого поколения в совершение преступлений экстремисткой и террористической направленности, связанные как с распространением запрещенного контента в сети Интернет, так и совершением противоправных действий вне цифрового пространства. К числу последних можно отнести поджоги и повреждение инфраструктурных объектов, покушения на жизнь представителей государственных органов и общественных деятелей.

– непосредственно осуществляющие рекрутинг молодежи в преступные организации, специализирующиеся на незаконном обороте наркотиков, совершении мошеннических действий и др. Как правило, представители организованных преступных формирований, используют несовершеннолетних в качестве исполнителей. Наример, дропов, на чьи платежные инструменты поступают похищенные денежные средства, ку-

рьеров, организующих тайники с наркотиками либо забирающих деньги у жертв мошенников и т. п. Как отмечается в специальной литературе «опасность состоит в том, что на практике для несовершеннолетних реально существует определенный «социальный лифт» — в случае качественного исполнения своих обязанностей подростки переходят на другие ступени структуры незаконного наркооборота, занимая «вышестоящие» и более оплачиваемые должности. Таким образом, стимулируется интерес подростка к более активным действиям, как результат, динамично расширяются круг участников и масштабы сетевой наркоторговли» [2].

– распространяющие депрессивно-суицидальный контент и склоняющие к самоубийству, а также пропагандирующие различные сексуальные девиации и смену пола, вовлекающие детей и подростков в преступления, связанные с проституцией, производством и распространением порнографических материалов. В этом случае имеет место своего рода двойственность, когда вовлеченное в противоправную деятельность лицо, само фактических становится жертвой данного вида преступлений. Например, в случаях изготовления и распространения информационного контента порнографического содержания с участием ребенка.

Таким образом, мы видим, что спектр угроз вовлечения несовершеннолетних в преступную деятельность по средствам информационных ресурсов весьма широк. Противодействие этому должно носить комплексный характер.

Учитывая возросшую роль информационных технологий в вовлечении несовершеннолетних в совершение преступлений, вполне обоснованным является тезис, согласно которому противодействие этому также должно осуществляется с использованием цифровых ресурсов.

Информационное противодействие должно включать в себя две основные группы действий.

Во-первых, деятельность по развенчанию информационных мифов, касающихся привлекательности образа представителей мира криминалитета, повышению уровня юридической и цифровой грамотности, а также развитию критического мышления подростков, в части оценки поступающих им предложений о «легком» заработке и формирования трезвой оценки возможных негативных для них последствий в случае принятия подобного рода предложений.

Во-вторых, установление каналов распространения такого рода информационного контента, а также их связи со специальными службами иностранных государств, экстремистскими и террористическими организациями, преступными формированиями, а также блокирование их деятельности на территории нашей страны.

Вместе с тем, стоит отметить, что исключительно информационных мер противодействия для эффективного противодействия вовлечению несовершеннолетних в преступную деятельность недостаточно. Это обусловлено рядом причин. Как психологическими, личностными особенностями представителей молодого поколения, имеющего при недостаточном жизненном опыте склонность к демонстративному поведению (определённый социальный протест, «бунтарство»), противопоставлению себя окружающему миру, так и техническими особенностями функционирования цифровой среды, осложняющими обеспечение полного запрета и удаления того или иного контента. Уровень развития программно-аппаратных решений в сфере информационно-коммуникационных технологий, позволяет с той или иной степенью эффективности получать доступ к запрещенной информации и заблокированным интернет ресурсам. Например, для этого могут быть использованы ресурсы сети DarkNet, VPN протоколы и т. п.

Соответственно наряду с информационными мероприятиями необходимо осуществление комплекса мер, как технического, так и разведывательно-поискового характера. Требуется развитие новых и адаптация традиционных, доказавших свою результативность методов оперативно-розыскной деятельности, для своевременного получения информации в цифровой среде и принятия соответствующих мер реагирования [1].

Кроме того, необходимо также продолжать проводимую в настоящее время работу по совершенствованию нормативной правовой базы, регламентирующей вопросы противодействия вовлечения несовершеннолетних в преступную деятельность. В данном случае с положительной стороны необходимо отметить внесенные в 2024 году изменения в положения статьи 150 УК РФ, усиливающие ответственность за вовлечение несовершеннолетнего лица в совершение преступлений [6, 7].

Список цитируемой литературы:

1. Дягилев, А. А. Проблемы правового регулирования оперативно-розыскной деятельности в сфере борьбы с преступлениями против основ конституционного строя и безопасности государства / А. А. Дягилев, Я. Д. Абдуллаев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2023. – № 2(62). – С. 92–95.
2. Кузина, Л.С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в незаконный оборот наркотиков / Л.С. Кузина // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 285–290.
3. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Рос. Федерации от 9 мая

2017 г. № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901.
4. Пояснительная записка к проекту федерального закона «О внесении изменения в статью 150 Уголовного кодекса Российской Федерации» [Электронный ресурс]. – URL: https://sozd.duma.gov.ru/bill/512731-8?ysclid=m5o33t59c7124029531 (дата обращения: 09.01.2025)
5. Расширенное заседание коллегии МВД России [Электронный ресурс]. – Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/events/president/news/73770 (дата обращения: 09.01.2025).
6. О внесении изменения в статью 150 Уголовного кодекса Российской Федерации: федер. закон Рос. Федерации от 29 мая 2024 г. № 111-ФЗ // Собрание законодательства Российской Федерации. – 2024. – № 23, ч. 1. – Ст. 3049.
7. О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 28 декабря 2024 г. № 514-ФЗ // Собрание законодательства Российской Федерации. – 2024. – № 53, ч. 1. – Ст. 8524.
8. Шаров В. И. Оперативно-розыскная деятельность в Интернет: монография / В.И. Шаров. – Н.Новгород: Нижегородская академия МВД России 2019. – 108 с.

Егоров В.А., канд. пед. наук, доцент, доцент кафедры ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Липецкий филиал, г. Липецк

КОМПЕТЕНЦИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНЫХ ИНСПЕКЦИЙ ПРИ ПРОВЕДЕНИИ ЭЛЕКТРОННОГО МОНИТОРИНГА В ОТНОШЕНИИ ПОДНАДЗОРНЫХ ЛИЦ

Аннотация

Статья раскрывает особенности применения системы электронного мониторинга подконтрольных лиц (далее – СЭМПЛ) сотрудниками УИИ ФСИН России. Важную задачу, которую необходимо реализовать – это снижение рецидивной преступности и предупреждение повторных преступлений, а также получение необходимой информации о противоправном поведении данного контингента.

Ключевые слова: система электронного мониторинга подконтрольных лиц, осужденный, всесторонний контроль за деятельностью УИИ, задачи и цели контроля.

Уголовно-исполнительные инспекции (УИИ) – это специализированные территориальные органы Федеральной службы исполнения наказаний Российской Федерации (ФСИН), наделенные полномочиями по исполнению уголовных наказаний, не связанных с лишением свободы. Их правовой статус и функции закреплены в ст. 16 Уголовно-исполнительного кодекса РФ, а также в Положении об уголовно-исполнительных инспекциях, утвержденном приказом Минюста России № 142. Основной задачей УИИ является реализация уголовной политики государства в части исполнения наказаний, таких как: обязательные и исправительные работы; ограничение свободы; условное осуждение с возложением обязанностей; меры уголовно-правового характера, назначаемые несовершеннолетним; административный надзор за определенными категориями лиц [2, С. 122]. «Инспекциями осуществляется надзор за отбыванием осужденными наказания в виде ограничения свободы, который заключается в наблюдении за поведением осужденных, соблюдением ими установленных судом ограничений и принятии в случае необходимости установленных законом мер воздействия» [5, С. 74].

В частности, УИИ вправе «в установленном порядке использовать аудиовизуальные, электронные и иные технические средства надзора и контроля для обеспечения надзора за осужденными к наказанию в виде ограничения свободы и контроля за нахождением подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением ими наложенных судом запретов и (или) ограничений».

Кроме того, УИИ осуществляют контроль за поведением осужденных, профилактическую работу с ними, обеспечивают взаимодействие с судами, органами внутренних дел, органами опеки и попечительства, а также с иными субъектами профилактики правонарушений. Характерной чертой деятельности УИИ является сочетание надзорных функций с социальной направленностью работы. Инспекции призваны не только контролировать соблюдение установленных судом обязанностей, но и способствовать ресоциализации осужденных, включая консультирование, помощь в трудоустройстве, восстановлении социальных связей и пр. Иными словами, УИИ представляют собой важнейший институт пенитенциарной системы России, ключевое звено в системе исполнения наказаний, не связанных с лишением свободы обеспечивающий их исполнение с применением как традиционных, так и современных технических средств контроля.

В соответствии со ст. 60 УИК РФ «для обеспечения надзора, предупреждения преступлений и в целях получения необходимой информации о поведении осужденных уголовно-исполнительные инспекции

вправе использовать аудиовизуальные, электронные и иные технические средства надзора и контроля» [9, С. 327]. Одной из современных форм надзора, находящейся в их ведении, выступает применение средств электронного мониторинга в отношении лиц, осужденных к ограничению свободы или иным мерам контроля.

В контексте СЭМПЛ, к полномочиям УИИ относятся: осуществление контроля за исполнением установленных судом обязанностей поднадзорных лиц; взаимодействие с техническими подразделениями, обслуживающими оборудование электронного мониторинга; принятие мер к предупреждению нарушений режима; составление материалов в случае фиксации нарушений условий отбывания наказания с применением СЭМПЛ [7, С. 31].

«Административный надзор устанавливается судом на основании заявления исправительного учреждения или органа внутренних дел». Назначение средств СЭМПЛ осуществляется в рамках исполнения уголовных наказаний, административного надзора или мер пресечения, не связанных с изоляцией от общества.

Основанием для применения СЭМПЛ является судебное решение или постановление органа, осуществляющего предварительное расследование, в зависимости от категории лиц (осужденные, подозреваемые, обвиняемые, лица, находящиеся под административным надзором).

Как правило, электронный мониторинг применяется при назначении наказания в виде ограничения свободы (ст. 53 УК РФ), условного осуждения с возложением определенных обязанностей (ст. 73 УК РФ), а также при административном надзоре за лицами, освобожденными из мест лишения свободы. Так, к примеру, на основании ст. 53 УК РФ, наказание в виде ограничения свободы предполагает контроль за осужденным. Суд может определить необходимость технического контроля, в том числе с применением электронного браслета, стационарных и мобильных устройств.

Итак, сущность порядка назначения электронного мониторинга начинается с вынесения соответствующего решения. УИИ направляет поднадзорному лицу предписание, организует установку оборудования и проводит инструктаж.

Представляется целесообразным более детальное рассмотрение порядка. Первоочередно, судом или уполномоченным органом принимается решения с указанием на необходимость контроля с применением технических средств. В решении указывается срок, границы передвижения и обязанности поднадзорного лица. После происходит передача материалов в уголовно-исполнительную инспекцию, осуществляющую исполнение наказания.

Далее следует назначение даты и времени установки оборудования, разъяснение прав и обязанностей осужденного, а также предупреждения об ответственности за несанкционированное вмешательство в работу устройств. Получение письменного уведомления под роспись является обязательным элементом. При этом применение СЭМПЛ предполагает обязательное согласие поднадзорного на соблюдение режима, а также на ношение технических средств контроля.

После того, как лицу была разъяснена «инструкция по эксплуатации», происходит непосредственный монтаж технических средств контроля, включая установку электронного браслета, мобильного или стационарного контрольного устройства и настройка соответствующего программного обеспечения. Оборудование привязывается к конкретному адресу и координатам нахождения, а также фиксируется в базе данных.

Затем наступает стадия непосредственного текущего контроля и фиксация нарушений, проводимые УИИ при поддержке Центра инженерно-технического обеспечения и вооружения ФСИН России. В случае нарушений составляется акт, а материалы направляются в суд, что, в свою очередь, может повлечь за собой ужесточение меры наказания или направление материалов в суд для замены наказания на более строгое.

По своей сути процедура назначения СЭМПЛ представляет собой комплекс юридических и технических мероприятий, обеспечивающих правомерное и эффективное применение дистанционного контроля в целях предупреждения новых правонарушений и соблюдения режима исполнения наказания.

Применение СЭМПЛ в отношении поднадзорных лиц представляет собой установленную законом процедуру, направленную на обеспечение эффективного контроля за поведением лиц, отбывающих наказания, не связанных с лишением свободы, либо находящихся под административным надзором.

Процесс применения СЭМПЛ первоочередно включает в себя постановку на учет и анализ оснований. После поступления соответствующего решения суда либо иного уполномоченного органа УИИ проводит проверку возможности применения технических средств контроля, оценивая социально-бытовые условия, текущее местонахождение, доступность сигналов навигационных систем и иные технические аспекты.

После установки происходит оперативное отслеживание соблюдения установленных ограничений. В процессе исполнения наказания производится непрерывный мониторинг: фиксируется местоположение поднадзорного лица, его перемещения, попытки нарушения режима либо снятия устройства. Контроль осуществляется с использовани-

ем спутниковой навигации (ГЛОНАСС/GPS), радиоканалов и специальных серверов.

Важно отметить реагирование на правонарушения и нарушения режима. При выявлении отклонений (несанкционированный выход за пределы зоны, повреждение оборудования, отказ от ношения устройств) УИИ обязана зафиксировать факт и инициировать соответствующие, ранее описанные меры. «Процесс контроля за выполнением осужденными установленных ограничений осуществляется СЭМПЛ в автоматическом режиме с выводом тревожных сообщений на пульт мониторинга в УИИ. Отчет с координатами о местонахождении подконтрольного лица формируется автоматически через заданный промежуток времени с последующей архивацией отчетных сведений в файл, который хранится в течение заданного промежутка времени на сервере территориального органа ФСИН России и может быть использован сотрудником УИИ в любое время» [11, С. 98].

В основном на практике используется четыре вида устройств. Самое тривиальное из них применяется, как правило, к подросткам – несовершеннолетним, для которых наказание в виде лишения свободы Суд счел неподходящим. В данном случае речь идет о небольшой технике, которую следует носить с собой. «При выходе из определенной зоны молодой человек обязан позвонить на определенный номер телефона и сообщить о месте своего нахождения. Звонок фиксирует компьютер. Если пройдет 5 минут, и он не позвонит, аппаратура подаст сигнал надзирающему инспектору, который может обратиться в суд с требованием принять меры к нарушителю».

Другие применяемые средства СЭМПЛ характеризуются большей, в сравнении, сложностью конструкции, наличием большего числа функций и «назначений».

К одной из указанных категорий относят устройства контроля по телефонной линии связи. «Эта модель состоит из базовой станции и легкого электронного браслета, благодаря чему человек свободно может передвигаться в небольшом радиусе от станции. Приемное устройство устанавливается по месту проживания осужденного и требует периодической подзарядки. Задача устройства – фиксировать время входа и выхода человека из помещений и регистрация совершенных им правонарушений, связанных с несоблюдением расписания или попытками повреждения устройства. Принцип работы электронного устройства по слежению за заключенным прост. Находясь в радиусе действия поля «базы», заключенный не может покинуть эти пределы. Как только он пересечет границу, устройство сразу посылает сигнал на телефон и на компьютер курирующему инспектору».

Следующий вид техники представляет собой аналогичное предыдущему устройство контроля по сотовой связи. В большинстве своем она имеет право на существование в городах, в то время как территории, не охваченные вовсе или надлежищам образом сотовой связью, не представляется целесообразным.

Наконец, самым распространенным типом выступают устройства постоянного слежения (непрерывного наблюдения). Их конструкция включает в себя несколько компонентов: персональный браслет-передатчик, мобильное устройство с GPS-навигацией и стационарный ретранслятор, устанавливаемый в месте проживания осужденного, чаще всего в его квартире.

По своему внешнему виду браслет напоминает наручные часы. Внутри корпуса располагаются чувствительный тепловой датчик и радиомодуль. Устройство фиксируется на запястье или лодыжке и активируется при помощи специального электронного ключа. Принцип действия датчика тепла исключает возможность обмана системы: браслет должен находиться в постоянном контакте с телом, а попытка снять или переместить его, например, в карман, моментально фиксируется системой как нарушение.

Технические характеристики устройства позволяют его использование в широком температурном диапазоне, вплоть до +100°C. Конструкция герметична, благодаря чему браслет можно кратковременно погружать в воду (до 5 метров глубиной и до 15 минут времени), что дает возможность осужденным посещать баню или принимать душ без снятия устройства.

Контроль за осужденным осуществляется в одном из трех режимов: посредством радиоканала, спутниковой навигации (GPS/ГЛОНАСС) или в комбинированной форме. В домашней обстановке активируется стационарное радиоустройство, напоминающее стационарный телефон без клавиш. Через него диспетчер может в любой момент установить голосовую связь с поднадзорным. При выходе за пределы квартиры радиоканал отключается, и наблюдение переходит на носимое GPS-устройство, закрепленное на поясе или плече. Некоторые модели браслетов оснащены встроенными навигационными модулями, работающими без необходимости в отдельном трекере.

Особое внимание уделяется соблюдению не только территориальных, но и временных ограничений. Осужденный обязан строго придерживаться установленного графика: вовремя выходить на работу и возвращаться домой. При возникновении уважительных причин, таких как визит к врачу, допускается внесение временных изменений в маршрут.

Передача координат на сервер производится автоматически через мобильную связь, как правило, с интервалом в четыре часа. Однако при возникновении нестандартной ситуации (например, выход за разрешенный периметр) данные отправляются немедленно. Система незамедлительно уведомляет нарушителя сообщением, после чего поднадзорный должен подтвердить получение сигнала и устранить нарушение. В противном случае инспекция получает тревожный сигнал, и к месту направляется наряд.

Таким образом, применение СЭМПЛ носит не только надзорный, но и превентивный характер, позволяя минимизировать риски рецидива, обеспечивать общественную безопасность и осуществлять контроль за соблюдением установленных судом ограничений без изоляции лица от общества.

Уголовно-исполнительные инспекции, в свою очередь, выполняют важнейшую роль в обеспечении исполнения наказаний с использованием современных технологий, что позволяет не только уменьшить нагрузку на пенитенциарную систему, но и обеспечить баланс между контролем за поведением правонарушителя и его правом на свободное передвижение в рамках закона.

Список цитируемой литературы:

1. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г.(в ред. от 5 октября 2022 г.) // Собрание законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.
2. Голубцова, К.И. Особенности применения системы электронного мониторинга подконтрольных лиц сотрудниками уголовно-исполнительных инспекций ФСИН России / К.И. Голубцова, Д.В. Брызгалов // Вестник Самарского юридического института. – 2022. – № 4 (50). – С. 122–126.
3. Голубцова, К.И. Проблемные вопросы эксплуатации систем электронного мониторинга подучетных лиц в Федеральной службе исполнения наказаний и перспективные направления их решения / К.И. Голубцова, К.И. Давлетшина // Вестник Самарского юридического института. – 2021. – № 5 (46). – С. 122–127. – Текст: непосредственный.
4. Гилева, В.Ю. Положительный опыт применения электронного мониторинга зарубежом и заимствование его в России / В.Ю. Гилева // Назначение и исполнение наказаний, не связанных с лишением свободы, и иных мер уголовно-правового характера : материалы III Всероссийской научно-практической конференции, Самара, 27 марта 2015 года / под общ. ред. А. А. Вотинова. – Самара: Самарский юридический институт ФСИН России. – 2015. – С. 42–46.

5. Дегтярева, О.Л. Система электронного мониторинга подконтрольных лиц (СЭМПЛ), как одна из форм контроля осужденных к ограничению свободы / О.Л. Дегтярева // NovaInfo. – 2015. – № 33. – С. 74–78.
6. Зараменских, Е.П. Принципы построения системы электронного мониторинга подконтрольных лиц в России: монография / Е.П. Зараменских, Д.В. Смирнов, И.Е. Артемьев. – Новосибирск: Издательство «СИБ-ПРИНТ», 2011 – 74 с.
7. Исыкуев, У. РЭА особого назначения: системы электронного мониторинга подконтрольных лиц (СЭМПЛ) / У. Исыкуев // Современная электроника и технологии автоматизации. – 2025. – № 2. – С. 30–36.
8. Крюкова, Д.Ю. СЭМПЛ: история, международное законодательство и современные проблемы развития в России / Д.Ю. Крюкова // Уголовно-исполнительная система на современном этапе: взаимодействие науки и практики : материалы Международной научно-практической межведомственной конференции, Самара, 16-17 июня 2016 года / под общ. ред. А.А. Вотинова. – Самара: Самарский юридический институт Федеральной службы исполнения наказаний. – 2016. – С. 338–340.
9. Медведева, И.Н. О некоторых особенностях применения электронного мониторинга поднадзорных лиц в странах Европейского Союза / И.Н. Медведева // Право и управление. – 2024. – № 9. – С. 327–332.
10. Мясникова, И.С. Особенности применения электронных средств контроля и надзора при исполнении наказаний / И.С. Мясникова, Е.Д. Шатохина // Молодой ученый. – 2016. – № 14 (118). – С. 453–456.
11. Назарова, А.Б. Проблемные вопросы применения системы электронного мониторинга подконтрольных лиц в отношении осужденных к наказанию в виде ограничения свободы / А.Б. Назарова // Информатизация и техническое обеспечение уголовно-исполнительной системы Российской Федерации: проблемы, решения и перспективы развития : сборник материалов межведомственной научно-практической конференции, Тверь, 04 октября 2021 года. – Тверь: Федеральное казенное учреждение «Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний». – 2021. – С. 98–101.

Захарова А.Д., адъюнкт
ФГКОУ ВО «Московский университет МВД России
имени В.Я. Кикотя», г. Москва

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРАВОВОГО СТАТУСА РЕБЕНКА, В УСЛОВИЯХ СОВРЕМЕННЫХ ВЫЗОВОВ И УГРОЗ

Аннотация

Деятельность международного механизма по защите прав ребёнка весьма обширен. В работе рассматриваются основные направления деятельности международного сообщества, целью которого является защита жизни и здоровья ребёнка, а также недопущения или минимизации действий, связанных с вовлечением ребёнка в деятельность, связанную с угрозой его жизни и здоровья.

Ключевые слова: вовлечению ребёнка в преступную деятельность; сексуальная эксплуатация несовершеннолетних, посредством информационных сервисов; склонение детей и подростков к суицидальным действиям через Интернет-пространство.

В настоящее время, под эгидой ООН существует огромный массив правовой базы международных соглашений по противодействию преступлениям, направленных на личные права ребёнка. Основными видами преступлений, направленных на личные права ребёнка, а также способствующих вовлечению ребёнка в преступную деятельность, является: торговля детьми; работорговля; распространение порнографического материала; пытки; жестокое обращение ребёнком, направленное на физическое и моральное страдание; деятельность связанная с распространение наркотических веществ, а также их прекурсоров; сексуальная эксплуатация детей; вовлечение детей в деятельность террористического характера и другое.

В большинстве случаев преступления, направленные против несовершеннолетних лиц, являются тяжкими или особо тяжкими преступными деяниями. К ним относятся действия, связанные с торговлей детьми на страницах «тёмного и глубинного интернета»; сексуальная эксплуатация несовершеннолетних, посредством информационных сервисов; склонение детей и подростков к суицидальным действиям через Интернет-пространство и др [3].

Преступные действия, совершенные в информационно-телекоммуникационных системах, характеризуются рядом отличительных черт от традиционных преступлений международного характера, направленных против детей. К этим отличительным чертам относятся высокая степень скрытности преступного лица; преступные дей-

ствия чаще совершаются хорошо организованной преступной группой, очень часто имеющих своих представителей в различных государствах; действия преступников носят транснациональный характер.

Скрытность лица, ощущение безнаказанности приводит к особой жестокости преступных лиц. Одними из примеров данной жестокости и чувства полной свободы преступных действий могут выступать действия по организации преступниками киберсекс-притонов, которые транслируют действия сексуального насилия над несовершеннолетними и малолетними лицами в прямой трансляции. А также создание организованных групп, которые под предлогом игры, квеста, заставляют несовершеннолетних лиц заканчивать жить самоубийством. Примером данных «групп смерти» могут служить такие преступные группировки как «Синий кит», она же «Blue whale challenge», «Красная сова». Данные группы осуществляют свою деятельность на территории стран СНГ, стран Европейского союза, отметим, что подобные организации существуют во всем мире [1].

Для достижения своих целей преступники знакомятся с подростками и детьми, а в последующем посредством уговоров требуют отправку компрометирующей информации, после чего под угрозами пересылки данных материалов родителям или опубликования материалов на веб-сайтах, вынуждают ребёнка на личные встречи или совершение каких-либо действий. Нередки случаи шантажа по причинению вреда близким родственникам ребёнка.

Существенными причинами развития преступности в Интернет-пространстве, является несоблюдение общих правил пользования информационно-телекоммуникационной сетью, в частности социальными сообществами. Значительное количество преступлений совершается по причине открытого доступа к личной информации о детях на сайтах, в том числе это относится к информации, предоставляемой школьными и медицинскими учреждениями. В частности, недопустимо, чтобы образовательные и медицинские учреждения имели в открытом доступе сведения о расписании ребёнка, о его личных данных, и других сведениях, способствующих созданию благоприятной среды для совершения преступления.

Несовершеннолетние лица, ставшие объектом преступного посягательства, подвергаются риску стать жертвами нескольких особо тяжких преступлений. Так, в случае с преступлениями, связанными с половой неприкосновенностью несовершеннолетних и малолетних лиц, то помимо сексуальных домогательств, преступники часто снимают и продают порнографические материалы в Интернет-пространстве, нередки случаи, продажи несовершеннолетних лиц с це-

лью эксплуатации [1], которая включает в себя как принуждение к занятию проституцией, так и любые другие формы сексуальной эксплуатации, а также использование детского труда или услуг [2].

Рассматривая виды преступного посягательства на личные права детей, необходимо выделить, преступления международного характера, направленные на торговлю детьми. Проблема торговли детьми, не раз понималась международным сообществом, на различных исторических этапах. Торговля детьми через информационное пространство, в частности через сервисы “тёмного и глубинного Интернета”, значительно облегчают этапы подготовки к совершению преступного посягательства, а также делают данный процесс наиболее доступным. Преступные посягательства, направленные на личные права детей, в информационном пространстве, являются высоко латентными, транснациональными преступными деяниями, совершающиеся организованными группами. Вследствие чего, данный вид преступности, достаточно остро ставится перед международным сообществом, а также перед государственными органами различных государств.

Преступные посягательства характеризуется следующими факторами, преступные действия совершаются на просторах тёмного или глубинного Интернета, с переводом денежных средств на электронные счета, не попадающие под контроль государственных органов, в частности криптосчета. Наиболее часто такие преступные действия осуществляются в среде мигрантов, а также лиц находящихся, в пределах крайней нищеты. Отметим, что по данным, предоставленным Российской Федерации, в связи с запросом Специального докладчика Совета ООН, по правам человека, было выявлено, что наиболее уязвимой возрастной категорией для торговли, являются дети в возрасте от рождения до одного г. [4]. В данном докладе также отмечается, что действия по продаже детей, чаще всего осуществляются родителями, или близким кругом взаимодействия с ребёнком, однако нередки случаи похищения и контрабанды ребёнка. Вместе с тем следует отметить, что деятельность преступников, направленная на торговлю детьми, чаще всего имеет своей целью, создание самостоятельного состава преступления, такого как сексуальная эксплуатация несовершеннолетнего.

Правоохранительные органы отмечают, что, попав под преступное посягательство, несовершеннолетние достаточно редко сообщают о данных обстоятельствах старшим лицам, опасаясь, что их техническая неграмотность не сможет изменить последствий уже случившихся преступных действий, а также боясь, что помимо этого наступят ограничивающие действия по пользованию телефоном, компьютером или иными техническими средствами. Данный факт достаточно серьёзно

сказывается на осуществлении международного и уголовного преследования лиц, совершающих преступные действия, посягающих на личные права ребёнка.

Преступные деяния, направленные на вовлечение несовершеннолетних лиц через информационно-телекоммуникационные в преступления, представляет серьёзную угрозу, как для международной, так и национальной безопасности государства. Связано это в первую очередь с тем, что данные преступные действия, способствуют омоложению преступника, так как они направлены на изменение моральных установок ребёнка, в том числе на сексуальную распущенность, пропаганду асоциального образа жизни, идеализации преступного мира.

Преступные действия международного характера, направленные на вовлечение детей через информационно-телекоммуникационные сети в преступления, обладают следующими характеристиками: преступные действия являются высоко латентными; сохраняется высокая анонимность лиц, совершающих преступные посягательства; преступления являются транснациональными; субъектами преступления чаще всего являются хорошо организованные преступные группы. Отметим, что преступные деяния, направленны на вовлечение несовершеннолетних лиц в информационном пространстве, имеет ряд особенностей, во-первых, деятельность представляет собой, привлечение большой группы несовершеннолетних лиц, которая подвергается определённому психологическому воздействию, в том числе вербовки детей, посредством информационно-телекоммуникационных технологий. Механизмы преступного воздействия на детей направляются в основном на разжигание этнической и религиозной ненависти, социальной и межнациональной напряжённости, пропаганды экстремисткой идеологии, в том числе привлечение к террористической деятельности. Во-вторых, деятельность преступников направлена на формирование у несовершеннолетних определённых информационных зависимостей. Отметим, что формирование информационных зависимости условно можно подразделить на две категории: компьютерные игры, направленные на формирование агрессивного, преступного поведения; а также прохождение квестов, игр в непосредственно «реальном мире». Компьютерные игры, направленные на формирование преступного поведения, способствуют смешиванию реального и виртуального мира, вследствие чего несовершеннолетние теряют связь с «реальной действительностью» и под воздействием игрового сценария компьютерной игры, совершают преступные действия. Преступные действия по прохождению квестов, игр в «реальном мире», функционируют по аналогии с квестами, направленными на лишение жизни несовершен-

нолетних. Преступники, заинтересовывают детей, получают от них информацию, на основании которой путём угроз, обмана, обещаний, вовлекают несовершеннолетних в преступления.

Преступные деяния, направленные на вовлечение несовершеннолетних лиц через информационно-телекоммуникационные системы, осуществляется по следующим основным направлениям: распространение наркотических веществ и их аналогов и вербовка несовершеннолетних лиц к преступной деятельности террористического характера, привлечение к преступлениям в сфере экономики.

Распространение наркотических веществ, в информационном пространстве, представляет собой, сложно организованное преступное деяние, которое направлено на распространение наркотических веществ и получения большего количества зависимых лиц от наркотических препаратов. Для реализации международного сотрудничества по транснациональной преступности по распространению наркотических веществ, существуют как универсальные, так и региональные механизмы взаимодействия. Говоря, о привлечении несовершеннолетних в преступную деятельность по распространению наркотических веществ, через информационные технологии, в первую очередь имеется ввиду, распространение наркотических веществ в подростковом обществе или выполнение задач связанных с закладкой наркотических веществ. Преступники, обладают высокой степенью анонимности, так как все действия по информированию несовершеннолетних, а также созданию влияния на них, осуществляется через информационные каналы «тёмного интернета». Под преступные действия, связанные с распространением наркотических веществ, чаще всего попадают подростки, не имеющие средств к существованию, из неблагополучных семей, которые ищут быстрый способ подработки денежных средств в Интернет-пространстве. Злоумышленники под предлогом перевозки и передачи определённых веществ обещают данным лицам постоянный заработок посредством выполнения несложных задач.

Вербовка несовершеннолетних лиц, а также привлечение детей к действиям террористического характера, чрез информационно-телекоммуникационные сети, представляют собой сложно спланированные преступления, направленные на развитие высокого интереса детей к террористическим действиям, развитие различных форм дискриминации, склонение к агрессии и насилию. Отметим, что под данные преступные действия чаще всего попадают несовершеннолетние, имеющие пристрастие и фанатизм к виртуальным играм, направленным на военные действия, состоящие в социальных группах данных игр и отличающихся социальной активностью в данных группах. Про-

граммы по склонению детей к террористическим действиям мало чем отличаются от преступлений международного характера, посягающих на личные права детей, а доведения несовершеннолетних до самоубийства. Террористические организации, создают в информационном пространстве, определённые условия для завлечения ребёнка, после чего несовершеннолетнему предлагаются сделать какие-либо действия. Рассматривая данную деятельность, на примере компьютерных игр: игра составлена таким образом, что каждое последующее задание является более жестоким, по отношению с предыдущим, более того данная игра в определённый момент выходит за границы виртуального пространства. В силу своей психологической несформированности, несовершеннолетние не всегда способны адекватно оценить данные обстоятельства и очень часто становятся исполнителями тяжких и особо тяжких преступлений. Помимо этого, нередки случаи открытого опубликования информации в подростковых сообществах, направленных на создание дискриминации по полу, религии, расе и т.д.

Для реализации защиты детей от вовлечения в преступления, необходимо постоянное сотрудничество государств в данных сферах. В настоящее время информационная безопасность несовершеннолетних пользователей одна из приоритетных задач в сфере национальной безопасности, а также международного сотрудничества государств. Отметим, что международное сотрудничество должно складываться: во-первых из постоянно действующих международных организаций, осуществляющих постоянный контроль за Интернет-пространством, вовлеченности детей в виртуальные игры, социальные сети, а также их безопасности; во-вторых в разработке и принятии международных договоров о стандартах взаимодействия, позволяющих проводить расследование преступлений, совершенных в киберпространстве, предоставлении электронных доказательств с учётом трансграничности преступных действий; в-третьих в отлаженном сотрудничестве правоохранительных органов по розыску преступных лиц, жертв преступлений, по выдаче преступных лиц или непосредственному осуществлению правосудия; в-четвертых, в постоянном информировании населения о преступных деяниях, совершаемых в сети Интернет, и безопасном использовании технических устройств, а также применении необходимых мер по сообщению о преступных деяниях, в случае совершения преступного посягательства. Таким образом, международное сотрудничество является одним из необходимых условий борьбы с преступлениями в информационно-коммуникационных сетях, а также обеспечения безопасного использования несовершеннолетними информационно-телекоммуникационными сетями.

Из выше рассмотренного можно прийти к следующему выводу, разработанный механизм международной защиты прав ребенка, условно можно подразделить по следующим направлениям угроз, направленных на права детей: угрозы, связанные с военным положением государства, а также насильственные действия или действия, связанные с жестоким обращением с ребенком, в мирное время. Особое значение международным сообществом уделяется вниманию насильственным действиям, связных с преступной деятельностью международного характера. В настоящее время наибольшую озабоченность международное сообщество выражает в развитии преступной деятельности в информационном пространстве.

Список цитируемой литературы:

1. Бычкова, А.М., Раднаева, Э.Л. Доведение до самоубийства посредством использования интернет-технологий: социально- психологические, криминологические и уголовно- правовые аспекты / А.М. Бычкова, Э.Л. Раднаева // Криминологический журнал. – 2018. – № 1. – С. 101–115.
2. Лебединец, И.Н. Международно-правовые основы сотрудничества государств в борьбе с торговлей женщинами и детьми / И.Н. Лебединец // Актуальные проблемы российского права. – 2016. – № 11. – С. 186–195.
3. COVID19 - Child Sexual Exploitation and Abuse threats and trends. Report. [Электронный ресурс]. – INTERPOL. – URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse (дата обращения: 15.01.2021).
4. Управлению Верховного комиссара ООН по правам человека: Информация Российской Федерации в ответ на запрос специального докладчика Совета ООН по правам человека по вопросу о торговле детьми, детской проституции и детской порнографии по теме «Торговля детьми и их сексуальная эксплуатация, включая проституцию, порнографию и другие виды насилия». г. Женева 17 октября 2019 г. № 4155.

Зиганшин Т.Р., аспирант
ФГКОУ ВО «Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева»,
старший инспектор отдела организации образовательной деятельности
Следственного комитета Российской Федерации
г. Москва

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ ПРОИЗВОДСТВЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ИЛИ С ПРИМЕНЕНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Аннотация

В статье рассматриваются и подвергаются разбору ключевые организационно-тактические проблемы и особенности применения специальных знаний, которые необходимы для применения должностными лицами при проведении следственных действий в ходе расследования преступлений в сфере компьютерной информации. Рассматриваются некоторые аспекты в качестве особенностей криминалистической деятельности при обнаружении, изъятии и фиксации материальных и цифровых следов преступления. Автором обозначен ряд проблем связанных с деятельностью специалистов при работе с компьютерной техники и электронными следами. Предлагаются мероприятия по улучшению качества и результативности производства следственных действий.

Ключевые слова: предварительное расследование; следственные действия; экспертиза; специальные знания; специалист; компьютерные экспертизы.

XXI век стал эрой технологического прогресса связанного в том числе и с развитием информационных технологий, уверенно внедряющимися во все сферы деятельности человека и общества в целом. Кроме того, одним из приоритетных направлений внутренней политики Российской Федерации является создание инфраструктуры для развития автономного информационного пространства и телекоммуникационных технологий. Данные обстоятельства связаны с повсеместной возможностью мгновенной передачи массива данных на неограниченные расстояния, а также создания и функционирования различных государственных услуг представляемых органами законодательной, исполнительной и судебной власти в электронном виде.

Государственные институты, различные сектора экономической деятельности также стремительно внедряются в систему цифровой трансформации. В процессе оптимизации кадров и в целях ускорения

процесса оказания услуг повсеместно используется цифоровизация общественных отношений. Представление документов, финансовые операции производятся в виртуальном пространстве по различным каналам связи, защищенность которых прямо пропорционально зависит от степени развития противодействия преступным элементам, посягающим на предмет цифровых отношений. И как показывает практика, зачастую степень развития технологий и возможностей злоумышленников превосходит возможности защиты передачи данных, что является фактором роста преступлений, совершаемых с использованием информационно-коммуникационных технологий. При этом последними оказывается высокое противодействия направленное на их пресечение, выявление и раскрытие и как следствие привлечение к предусмотренной законом ответственности. В ходе реализации преступного умысла ими используются сложные информационные технологии, а также технические средства, используемые как для получения информации так и ее сокрытия.

По мнению многих криминалистов, в настоящее время фиксируется виртуализация преступности, т.е. переход общественно опасных деяний в информационную среду, исключающую физический контакт преступника и жерты, обеспечивающую «традиционную, классическую преступность современными информационными технологиями в виде систем конспирации и скрытой связи. «Классические» преступления будут оставлять значительно больше цифровых следов и требовать от преступника технической компетентности, что несомненно, повлияет на механизм следообразования [1. С. 207-211].

Данное обстоятельство подтверждается статистическими данными, и практический опыт следственных органов показал, что к основным видам преступлений в сфере компьютерной информации и преступлений, совершенных с использованием информационно-коммуникационных технологий, относятся:

1) преступления против конституционных прав и свобод человека и гражданина (ст.ст. 137 и 138.1 УК РФ);

2) преступления против половой свободы и половой неприкосновенности, совершенные посредством социальных сетей и мессенджеров в отношении малолетних (ст. 132 УК РФ с учетом примечания к ст. 131 УК РФ);

3) преступления в сфере экономической деятельности (ст. 171.2 УК РФ);

4) преступления против здоровья населения и общественной нравственности (ст.ст. 228, 228.1, 242, 242.1 и 242.2 УК РФ);

5) преступления против государственной власти (ст.ст. 290 и 291 УК РФ).

Между тем, юридическое понятие «цифровой след» в настоящее время не закреплено. Мещеряков В.А. под этим термином понимает «различное изменение автоматизированной системы, сопряженное с преступлением и зафиксированное как компьютерная информация» [2, С. 423]. В свою очередь, Бессонов А.А. определяет в качестве цифрового следа «информацию, зафиксированную в цифровом формате, содержащуюся в электронно-вычислительных машинах и иных цифровых устройствах» [3, С. 47].

В наше время все чаще появляется необходимость при расследовании сложных, резонансных преступлений изымать и выявлять нетрадиционные для криминалистики цифровые следы, искать вещественные доказательства, которые представлены в виде информации телекоммуникационной или вычислительной системы, либо на магнитных носителях [4, С. 165-167].

В ходе проведения следственных действий, таких как осмотр места происшествия, обыск возможно изъятие предметов имеющих доказательственное значение по уголовному делу и относящихся к цифровым устройствам: компьютеры, ноутбуки, нетбуков, мобильных устройства, флэш-накопители и иные носители цифровой информации. Данные объекты изымаются в целях установления на них цифровых следов или получения информации, содержащей сведения, которые могут использоваться в качестве доказательств. Однако, осмотр и изъятие подобных элементов сопряжены с определенными рисками, которые обусловлены отсутствием специальных навыков у должностных лиц, осуществляющих предварительное расследования. В целях минимизации таковых требуется привлечение для участия в процессе специалистов. Более того, указанный вид деятельности обеспечивает действие специалиста с субъектами раскрытия и расследования преступлений в режиме реального времени. Примером может является обнаружение специалистом в ходе осмотра компьютера, изъятого при проведении обыска у лица, причастного к совершению преступления, следов подключения устройства, предназначенного для негласного получения информации и планируемого к сбыту на территории Российской Федерации, что в последствии подтвердило факт наличия устройства в жилище обвиняемого, использования его и последующей продажи.

В качестве компетентных лиц, принимающих участие в следственных и процессуальных действиях направленных на добычу доказательств могут выступать специалисты СЭЦ СК России, ЭКЦ МВД России, сотрудники различных организаций, обладающие профессиональными знаниями работы с компьютерной техникой и информационными технологиями, в случае наличия у них соответствующего образования, которое подтверждено дипломом [5, С. 224].

Важно отметить и нахождение на устройстве специализированных вредоносных программ, используемых в качестве препятствий для получения скрытой информации [6, С. 221]. В связи с этим любые действия с техническими средствами без консультации со специалистом в области информационных технологий преждевременны. Кроме того, профессиональные преступники используют средства и методы защиты информации в области шифрования, парольной защиты, криптографии. Без специальных знаний невозможно не только дешифровать информацию, но и даже установить ее местонахождение на компьютере [7, С. 126-128].

В ходе проведения следственных и процессуальных действий при расследовании преступлений в сфере ИКТ не стоит забывать и о наличии традиционных криминалистических следов, веществ и объектов, для фиксации и изъятия которых также требуется привлечение специалиста или следователя-криминалиста. При реализации процесса доказывания таких преступлений также могут применяться криминалистические и иные виды учетов. Например возможности федеральной базы данных геномной информации и централизованной интегрированной автоматизированной дактилоскопической информационной системы МВД России (ЦИАДИС-МВД), которые содержат данные криминалистически значимых объектов – ДНК и следов пальцев рук [8, С. 16-21]. Обобщая изложенное можно прийти к выводу об использовании возможности взаимодействия специалистов разного профиля: в сфере компьютерной техники с экономистами по уголовным делам в сфере экономики, с лингвистами в сфере противодействия экстремизму, химиками и биологами в сфере незаконного оборота наркотических средств и др.

После проведения мероприятий по добыче необходимых доказательств возникает необходимость назначения судебной экспертизы. При решении данного вопроса следует согласиться с мнением Гаврилина Ю.В. о том, что «в процессе производства компьютерной экспертизы используются специальные знания в области информатики и вычислительной техники, информационных систем и технологий, программной инженерии, информационной безопасности, электроники, радиотехники и систем связи, инфокоммуникационных технологий» [9, С. 133]. При производстве таковой возможно разрешить ряд задач, выводами которых послужит заключение эксперта, впоследствии используемое для обвинения, например:

- поиск информации на машинном носителе, созданной с помощью прикладных программ;

- поиск информации на машинном носителе о действиях пользователя (процессах обработки файлов, ведения баз данных, работе в сетях передачи данных);

- определение свойств программ и программных продуктов;

- определение возможности совершения каких-либо действий с помощью средств вычислительной техники;

- установление материальных объектов по компьютерной информации;

- установление фактических обстоятельств совершения преступления.

Важным аспектом является достаточность объектов представляемых для исследования, а также постановка вопросов вносимых на экспертизу, которые должны удовлетворять определенным требованиям, которые в общем смысле можно разбить на две группы: общие требования и частные. Общие требования должны формулироваться четко и однозначно с использованием устоявшегося понятийного аппарата, исключающего полупрофессиональные термины. Частные требования должны соответствовать представляемым на экспертизу объектам, вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того подразделения в котором назначается экспертиза.

Резюмируя изложенное, полагается необходимом проводить консультацию с экспертом, на предмет достаточности представленных объектов для исследования, а также технических и иных возможностей необходимых для производства экспертизы, более того, следует заранее обговорить перечень и формулировку вопросов выносимых на разрешение. Думается, что консультацию разумнее провести перед назначением экспертизы во избежание необходимости разрешения возникающих в процессе ее проведения ходатайств и увеличения сроков проведения.

Делая акцент на значительно возросшем количестве преступлений совершаемых исследуемым образом, а также развитие возможностей экспертных учреждений по разработке методики и внедрения инновационных средств противодействия их совершению и изобличению лиц причастных к их совершению, путем проведения новых видов судебных экспертиз, следует использовать возможности специальных знаний в полном объеме на всех этапах предварительного расследования.

По мнению органов предварительного расследования, обстоятельствами, способствовавшими совершению подобных преступлений по прежнему являются

1) низкая компьютерная грамотность населения;

2) недооценка общественной опасности компьютерной преступности;

3) недостаточные действия по администрированию публичных страниц в телекоммуникационной сети Интернет и социальных сетей, в том числе, со стороны владельцев публичных страниц и данных сетей;

4) недостаточные действия лиц, ответственных за хранение сведений, по обеспечению сохранности личных данных, в том числе, несвоевременное принятие мер по защите компьютерной системы от вмешательства извне;

5) быстрая распространяемость публикаций, не позволяющая своевременно блокировать размещенную противоправную информацию.

В целях создания условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием ИКТ полагается:

1) проводить профилактическую работу с населением и предупреждать об угрозе преступлений, совершенных при помощи ИКТ;

2) обеспечить надлежащее администрирование своих сайтов их владельцами в телекоммуникационной сети Интернет;

3) регулярно повышать квалификацию должностных лиц, ответственных за выявление и пресечение анализируемых преступлений.

Как известно, «внутреннее убеждение представляет собой уверенность лиц, принимающих уголовно-процессуальные решения относительно допустимости, относимости, достоверности и достаточности доказательств, а также выводов, которые следуют из совокупности этих доказательств» [10, С. 39]. Без использования специальных знаний и системного взаимодействия с экспертами и специалистами изучение и проведение тщательного анализа документов и иных материалов уголовного дела, подтверждающих совершение лицом преступных деяний не всегда возможно сделать правильные выводы о виновности лица.

Следует согласиться со словами ведущего эксперта на рынке информационной безопасности, президента ГК InfoWatch Натальи Касперской «Если мы не хотим превратить нашу страну в цифровой концлагерь, нам необходима будет система табу, которые позволят человеку оставаться человеком. А для того, чтобы к ней прийти, необходима широкая дискуссия общества и государства, результатом которой станут правильные критерии регулирования цифровой сферы с учетом тех рисков, с которыми мы сталкиваемся в сети».

Проводя итоги вышесказанного, можно смело заявить, что применение специальных знаний органами осуществляющими предварительное расследование по раскрытию и расследованию преступлений совершенных в киберпространстве и с использованием ИКТ является безапелляционной необходимостью. Расследование подобных преступлений исключительно на основе идеальных доказательств не может рассматриваться как исчерпывающий процесс дающий основания считать лицо виновным. Необходимость в привлечении специалистов вызвана не столько необходимостью выявления обстоятельств подле-

жащих доказыванию и обстоятельств, способствовавших совершению преступления, но и влиянию цифровой трансформации общественных отношений и в целом человеческой деятельности.

Список цитируемой литературы:

1. Грибунов, О.П. Криминалистическая теория причинности в контексте установления механизма следообразования: философские и теоретические аспекты /О.П. Грибунов // Вестник Томского государственного университета. – 2019. – № 446. – С. 207–211.
2. Мещеряков, В.А. Следы цифрового века / В.А. Мещеряков // Вопросы экспертной практики. – 2019. – № 1. – С. 423–426.
3. Бессонов, А.А. О некоторых возможностях современной криминалистики в работе с электронными следами / А.А. Бессонов // Вестник Университета имени О.Е. Кутафина. – 2019. – № 3 (55). – С. 46–52.
4. Ткачев, А.В. Возможности исследования компьютерных средств / А.В. Ткачев // Вещественные доказательства: собирание и возможности исследования / отв. ред. Н.Н. Егоров. – Москва: Юлитинформ, 2017. – С. 165–187.
5. Баев О.Я. Тактика следственных действий / О.Я. Баев. – Москва: Юлитинформ, 2013. – 224 с.
6. Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений / Л.Н. Соловьев. – Москва: Собр., 2004. – 221 с.
6. Лантух, Э. В. Выявление сокрытия преступлений с использованием криминалистических средст / Э. В. Лантух // Криминалистика - наука без границ: традиции и новации : Материалы ежегодной всероссийской научно-практической конференции, Санкт-Петербург, 02 ноября 2018 года / Составитель О.С. Лейнова. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2019. – С. 126–128.
7. Бессонов, А.А. Перспективы использования технологии искусственного интеллекта в экспертно-криминалистической деятельности / А.А. Бессонов // Судебная экспертиза и исследования. – 2022. – № 1. – С. 16–21.
8. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : Учебное пособие. В 2-х частях / Ю. В. Гаврилин, А. В. Аносов, В. В. Баранов [и др.]. Том Часть 1. – Москва : Академия управления Министерства внутренних дел Российской Федерации, 2019. – 208 с.
9. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / под общ. Ред. А.И. Бастрыкина. – Москва: Волтерс Клувер, 2008. – 907 с.

Зуев С.В., д-р. юрид. наук, профессор, профессор кафедры ФГБОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск

АДМИНИСТРИРОВАНИЕ В ЦИФРОВОМ УГОЛОВНОМ ПРОЦЕССЕ КАК ВЫСШАЯ ФОРМА ОРГАНИЗАЦИИ РАБОТЫ ОРГАНОВ РАССЛЕДОВАНИЯ И СУДА

Аннотация

В статье определяется значение администрирования в цифровом уголовном процессе. Утверждается, что в современном уголовном судопроизводстве особая роль отводится качеству интернет-соединений, что обеспечивает надежный доступ граждан к электронному правосудию. Цифровые платформы должны обслуживаться специалистами, обеспечивая защиту персональных данных от незаконного распространения.

Ключевые слова: цифровизация; уголовный процесс; администрирование; цифровые платформы; персональные данные.

Технологическое развитие как явление в обществе и государстве вряд ли у кого-то вызывает сомнения. В уголовном судопроизводстве оно также наблюдается через внедрение цифровых технологий. Представляется возможным выделить некоторые векторы развития цифрового уголовного судопроизводства.

Несмотря на то, что уголовный процесс в цифровой среде в полном виде можно представить только в перспективе, определенные начинания, тенденции можно заметить уже сейчас. Для того, чтобы анализировать, просматривать направления развития, необходимо видеть цель и представлять задачи, которые предстоит решать.

Векторы технологического развития цифрового уголовного судопроизводства – это относительно самостоятельные направления модернизации уголовного процесса как науки, теории и практики под влиянием, совершенствованием и внедрением в правовые механизмы современные технологии и информационные системы.

Представляется, что к таким векторам можно отнести: «электронные доказательства», «цифровые платформы», «искусственный интеллект», «электронное взаимодействие», «дистанционные формы коммуникаций», «видеомоделирование» и т.п. Возможно после выхода на достаточно высокий уровень развития понадобится организация работы органов расследования и суда, для чего будет востребовано компьютерное администрирование. Последнее требует должного внимания в плане научного обоснования, поскольку это не должно сводиться к чисто техническому обслуживанию. Ненадлежащее осуществление дан-

ной деятельности может привести к нарушениям прав человека и незаконному распространению персональных данных.

Администрирование принято понимать как управление, руководство чем-либо, распоряжение. Возможно администрирование данных, системное администрирование, что вполне может быть применимо к цифровому уголовному процессу. Последнее представляется в виде обслуживания интернет-платформы, а значит потребуется настройка и поддержка соответствующего оборудования, обеспечивающее производство по уголовным делам в электронном формате, а также постоянное развитие и модернизация всего уголовного судопроизводства.

П. С. Пастухов считает, что с использованием цифровых платформ формируется новая форма и содержание информационного взаимодействия в автоматизированном режиме, минимизируя действие человеческого фактора. За счет цифровых платформ происходит выстраивание взаимодействия способом, который признается максимально удобным для сторон [3, с. 522].

Для этих целей понадобится системное администрирование для создания, обслуживания и осуществления высокотехнологичных следственных и судебных действий, проведения оперативно-розыскных мероприятий в сети «Интернет», для поддержки информационных систем при обработке и передачи больших данных, разграничения доступа к материалам электронных уголовных дел.

Многообразие компьютерной техники, ее сложность позволяет предположить, что для работы с ней потребуются специалисты-юристы, обладающие набором компетенций, необходимых для осуществления уголовного судопроизводства в цифровой среде. Именно такие специалисты должны готовиться в ВУЗах страны.

Кроме того, потребуется участие администратора, а значит ему должен будет открыт доступ ко всем данным предварительного расследования и суда. Данная проблема соприкасается с сохранением тайны предварительного расследования и защитой персональных данных всех участников уголовного процесса. Системный администратор становится лицом, от которого будет зависеть качество интернет-соединений, а значит и обеспечения доступа граждан к электронному правосудию. Если такая связь связана с участием защитника, то это напрямую относится к правам обвиняемого (подозреваемого, подсудимого). Проблемы могут возникать по ходу функционирования системы, многое будет зависеть от общих условий и конкретных случаев.

Администрирование тесно связано с решением технологических и правовых вопросов.

В технологическом плане активно применяются и развиваются «цифровые платформы (шеринговые платформы, поисковые системы, социальные сети, правительственные платформы и др.), и формируемые ими платформенные экосистемы трансформируют мир, меняя различные виды социально экономической активности» [1, с. 100]. Данный вопрос также актуален для цифрового уголовного судопроизводства, поскольку экосистема – лучшая форма отправления электронного правосудия [2, с. 186].

Уголовное судопроизводство в цифровой среде невозможно представить без использования облачных провайдеров, настройки серверов и сервиса для отказоустойчивой работы. Заслуживает внимание архитектура виртуальной машины, на которой будут установлены все необходимые средства обмена и интеграции данных, а также установлена защита от угроз, которые могут нарушить функционирование всей системы [4; 5].

С правовой стороны интерес представляет решение вопроса относительно доступа специалистов по администрированию цифрового уголовного процесса. Кроме общей задачи по сохранению персональных данных, существует необходимость в обеспечении тайны предварительного расследования (ст. 161 УПК РФ). Представляется, что кибербезопасностью должны заниматься профессионалы этого дела. Сегодня на российском рынке успешно работают такие организации, как: «Лаборатория Касперского», Positive Technologies, «ИнфоТеКС», «Код Безопасности», и UserGate и др.

Данные фирмы успешно обеспечивают безопасность как коммерческим организациям, так и государственным органам. Так, например, компания Positive Technologies – является лидером рынка результативной кибербезопасности, и, для примера, занимается защитой IT-инфраструктуры Минсельхоза России, внедрив автопилот MaxPatrol O2, позволяющий с минимальным участием человека предотвращать реализацию недопустимых событий, способных нанести организациям неприемлемый ущерб [6].

Важным остается вопрос о допуске к осуществлению цифрового уголовного процесса специалистов в IT-сфере, решение которого возможно по аналогии с участием переводчика (ст. 59 УПК РФ).

Процессуальность всегда занимала законодательную «нишу». Администрированию как организационной стороне, как правило, отводится уровень подзаконных правовых актов. Технологические вопросы могут находить отражение на всех уровнях правового регулирования. Это означает, что сбои технологического характера, нарушение подзаконных актов может привести к процессуально значимым по-

следствиям. Вместе с тем на сегодня порядок уголовного судопроизводства на территории Российской Федерации устанавливается только Уголовно-процессуальным кодексом (ч. 1 ст. 1 УПК РФ). Поэтому все указанные вопросы имеют существенное значение и требуют грамотного разрешения.

Список цитируемой литературы:

1. Александров, М. А. Цифровые правительственные платформы: этапы институционализации и технологии оценивания (на примере платформы «Госуслуги») / М. А. Александров, Г. А. Меньшиков, Н. А. Пруель // Умная цифровая экономика. – 2022. – Т. 2, № 4. – С. 100–110.
2. Зуев, С. В. Уголовное судопроизводство как цифровая социальная экосистема / С. В. Зуев // Университетские правовые диалоги «Право и экология»: материалы Международной научно-практической конференции, Челябинск, 25–26 марта 2021 года. – Челябинск: Южно-Уральский государственный университет (национальный исследовательский университет), 2021. – С. 186–189.
3. Пастухов, П. С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве / П. С. Пастухов // Пермский юридический альманах. – 2023. – № 6. – С. 521–540.
4. Радченко М. В. Принципы создания архитектуры сервера для стабильной работы iTOP CMDB и обеспечения защиты сервера от хакерских атак / М. В. Радченко, А. М. Кумратова, К. А. Тарасенко, А. И. Василенко // Инженерный вестник Дона. – 2023. – № 10(106). – С. 95–106.
5. Тюменцев, Д. В. Оценка потенциала использования serverless-технологий в контексте системного администрирования / Д. В. Тюменцев // Инновационная наука. – 2024. – № 7-1. – С. 49–54.
6. IT-системы Минсельхоза России под защитой MaxPatrol O2. [Электронный ресурс]. – Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/about/news/it-sistemy-minselhoza-rossii-pod-zashchitoj-maxpatrol-o2/ (дата доступа: 10.01.2025).

Изотова В.Ф., канд. физ.- мат. наук, доцент, доцент кафедры ФГБОУ ВО «Саратовская государственная юридическая академия», г. Саратов

Проблемы противодействия несанкционированному распространению персональных данных в киберпространстве

Аннотация

Проблемы противодействия несанкционированному распространению персональных данных (ПД) в киберпространстве являются важным направлением обеспечения национальной безопасности. В статье проанализирована степень защищенности информационных систем (ИС), в которых обрабатываются ПД. Выявлены основные факторы, способствующие несанкционированному распространению ПД. Сформулированы предложения по совершенствованию правового регулирования в этой сфере.

Ключевые слова: информационные системы, персональные данные, несанкционированное распространение данных, киберпространство.

Электронное государство представляет собой модель государственного управления, базирующуюся на предоставлении физическим и юридическим лицам определенных информационных ресурсов и информационных услуг, а также на построении взаимодействия всех органов публичной власти и населения с учетом современного уровня развития информационно-телекоммуникационных технологий [1,2].

Электронные технологии государственного управления базируются на повсеместном применении систем электронного документооборота (ЭДО) и Информационных систем (ИС), что обеспечивает интеграцию документационного контента организаций в единое информационное пространство Российской Федерации. Тенденции развития правового регулирования цифровых трансформаций информационного общества активно обсуждаются научным сообществом [3,4].

Целью защиты персональных данных в информационных системах является снижение рисков и ущерба, возникающего в результате потенциальных угроз безопасности этих данных. Правовая основа защиты персональных данных в первую очередь определяется следующими нормативными актами: Федеральным законом «О персональных данных, Трудовым кодексом (глава 14), Гражданским кодексом.

Федеральный закон определяет основные понятия. «Персональные данные (сокр. ПД) или личностные данные – сведения, относящиеся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных), которые могут быть

предоставлены другим лицам». «Персональные данные – это любая информация, относящаяся к человеку, с помощью которой его можно идентифицировать». ПД можно разделить на четыре категории: общие данные, биометрические данные, специальные данные, общедоступные данные (или обезличенные) [5].

«Информационная система – это взаимосвязанная совокупность средств и методов, используемых для хранения, обработки и выдачи информации в целях её дальнейшего использования». ИС может быть охарактеризована как организованное и структурированное объединение документов (или массивов документов) и информационных технологий, включая применение вычислительных средств и средств связи. «ИС ПД – совокупность информационных и программных, а также технических средств» [6].

Основные компоненты информационных систем по обработке персональных данных (ИСПД) включают в себя: ПД, хранящиеся в базах; технические средства и системы, используемые для обработки ПД; программные средства, средства защиты информации (СЗИ), вспомогательные технические устройства и системы связи, которые не участвуют в обработке ПД.

ИС можно классифицировать по различным критериям.

• По типу использования информации: информационно-справочные системы и системы обработки данных.

• По функциональному назначению: производственные системы, маркетинговые системы, финансовые системы, кадровые системы и другие.

• По объектам управления: системы управления ресурсами, управления предприятием, управления технологическими процессами, управления базами данных, автоматизированные системы управления и системы автоматизированного проектирования.

• По уровню автоматизации: информационные системы с полной автоматизацией (автоматические) и с частичной автоматизацией (автоматизированные).

• По сфере применения: государственные, территориальные и отраслевые информационные системы управления.

Группы информационных систем обработки персональных данных (ИСПД) по принадлежности делятся на: ИСПД, принадлежащие государственным и муниципальным органам и ИСПД, принадлежащие юридическим и физическим лицам, которые обрабатывают ПД и определяют цели и содержание этой обработки.

По наличию выхода в Интернет выделяют с системы многоточечного выхода в сеть, системы одноточечного выхода в интернет, без доступа в Интернет.

В различных группах ИСПД могут быть доступным различные операции с данными. В одних ИСПД разрешены только операции чтения и поиска, т.е. база данных сформирована и не подлежит дополнению или изменению. В других возможны операции записи, удаления и сортировки данных. В-третьих, доступны операции модификации и передачи данных, что характерно для большинства систем.

По разграничению доступа к персональным данным ИСПД разделяют на системы, в которых доступ к ПД имеют только субъект ПД и отдельные сотрудники оператора, и системы, где Доступ ко всем ПД имеют все сотрудники оператора.

По уровню обезличивания данных ИСПД разделяют на системы, где:

1) пользователи ИСПД получают только обезличенные данные;

2) данные обезличиваются для передачи в другие организации, но сотрудники оператора получают их в необезличенном виде;

3) данные не подвергаются обезличиванию даже для передачи.

ИСПД по объему предоставления базы данных другим компаниям делятся на те, где оператор предоставляет доступ:

1) ко всей базе ПД другой компании по запросу;

2) предоставляет доступ только к части данных, например, к информации об отдельных пользователях;

3) не предоставляет никакой информации и хранит базу исключительно для собственного использования.

Актуальные угрозы безопасности персональных данных (ПД) представляют собой совокупность условий и факторов, которые создают риск несанкционированного, в том числе случайного, доступа к ПД в процессе их обработки в информационной системе. Эти угрозы определены в постановлении Правительства РФ №1119 и разделяются на три типа.

1. Угрозы первого типа связаны с недекларированными, возможностями в системном программном обеспечении.

2. Угрозы второго типа касаются недекларированных возможностей в прикладном программном обеспечении.

3. Угрозы третьего типа включают риски, связанные с системным и программным обеспечением, которые не относятся к предыдущим двум категориям.

Система защиты ПД представляет собой совокупность мер и мероприятий, направленных на обеспечение безопасности ПД.

Организационные меры включают в себя: уведомление Роскомнадзора о начале обработки ПД; разработку локальных нормативных актов; внедрение системы контроля доступа на объекты, где хранятся массивы с ПД; заключение соглашений с третьими лицами; определение актуальной модели угроз; классификацию сотрудников по уров-

ням доступа к конфиденциальной информации и создание системы внутреннего контроля.

Технические меры включают: использование межсетевых экранов и различных систем ограничения доступа; применение криптографических средств и блокировщиков; использование генераторов шума, экранированных кабелей и высокочастотных фильтров.

Разработка системы защиты ПД должна учитывать актуальные угрозы и уровень ответственности оператора. Требования к защите ПД при их обработке в ИС регламентированы постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Контроль и надзор за соблюдением законодательства в области обработки ПД осуществляет Роскомнадзор (Федеральная служба по надзору в сфере связи и массовых коммуникаций). ФСТЭК России (Федеральная служба по техническому и экспортному контролю) разрабатывает методы и способы защиты информации в информационных системах с использованием технических средств. ФСБ России (Федеральная служба безопасности РФ) определяет методы и способы защиты информации в информационных системах в рамках своих полномочий, включая регулирование использования криптографических средств защиты информации.

Доказано, что наивысшей степени защиты персональных данных удается достичь в локальных информационных системах. Хотя выявлены неоднократные прецеденты разглашения конфиденциальных сведений недобросовестными сотрудниками даже при блокировке считывания и сохранения информации из ИС [7].

Развитие инфраструктуры электронного государства приводит к расширению обмена данными, в том числе ПД, между государственными органами, что обостряет проблемы защиты информации, особенно в условиях использования в ИС технологий искусственного интеллекта [8,9]. Что требует выработки единых подходов к формированию политик информационной безопасности под эгидой Роскомнадзора. В этой связи все более ощутима значимость саморегулирования в этой сфере путем формирования документов стандартизации, договорной базы, деятельности саморегулируемых организаций.

При электронном документообороте нарушение права на частную жизнь в значительной мере связано с противоправным распространением и использованием ПД. Установлено, что утечка ПД в большей степени это проблема частных организаций, в том числе в IT-сфере и в банковской сфере.

Считаем, необходимым расширить субъектный состав административных правонарушений. В части 7 статьи 13.11 КоАП сегодня предусмотрена ответственность только для операторов, являющихся государственными или муниципальными органами. Мы считаем, что эта ответственность должна быть расширена абсолютно на весь субъектный состав.

Для исключения внутренних причин утечки конфиденциальной информации при их хранении, обработке и передачи в ИС считаем целесообразным дополнить КоАП новым составом административного правонарушения – за невыполнение оператором или иным лицом, получившим доступ к персональным данным, обязанности по соблюдению требования конфиденциальности персональных данных.

Список цитируемой литературы:

1. Изотова, В.Ф., Чайковский, Д.С. Правовые основы формирования электронного государства / В.Ф. Изотова, Д.С. Чайковский // Историко-правовой, философский и социокультурный опыт развития российской государственности. Сборник докладов по материалам Всероссийской научно-практической конференции в рамках IV Саратовского молодежного юридического форума. – Саратов: Изд. – во Сарат. гос. юрид. акад., 2024. – С. 139–144.
2. Чаннов, С. Е. Информационное право: учебник / под ред. С. Е. Чаннова. – Москва: Норма: ИНФРА-М, 2024. – 448 с.
3. Вызовы информационного общества: тенденции развития правового регулирования цифровых трансформаций : Монография по материалам 3.0 международной научно-практической конференции / Е. Н. Абанина, М. А. Агаларова, Д. А. Агапов [и др.]. – Саратов : Саратовская государственная юридическая академия, 2022. – 432 с.
4. Вызовы информационного общества: тенденции развития правового регулирования цифровых трансформаций: монография по материалам 4.0 Международной научно-практической конференции (г. Москва, 24-25 мая 2023 г.) / А. С. Анисимова, Е. А. Артамонова, Е. В. Архангельская [и др.]. – Саратов: Саратовская государственная юридическая академия, 2023. – 501 с.
5. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ (в ред. от 6 февраля 2023 г.) // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1. – Ст. 3451.
6. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ (в ред. от 2 ноября 2023 г.) // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1. – Ст. 3448.

7. Неприкосновенность частной жизни в условиях цифровизации и ответственность за ее нарушение. Стенограмма парламентских слушаний [Электронный ресурс] – Совет Федерации Федерального Собрания Российской Федерации. – URL: http://council.gov.ru/activity/activities/parliamentary/127610/ (дата обращения: 23.11.2024)
8. Ковалева, Н.Н., Ересько, П.В., Изотова, В.Ф. Проблемы и перспективы использования искусственного интеллекта в единой государственной информационной системе здравоохранения / Н.Н. Ковалева, П.В. Ересько, В.Ф. Изотова //Вестник Саратовской государственной юридической академии. – 2024. – № 3 (158). – С. 95–102.
9. Ковалева, Н.Н., Ересько, П.В., Изотова, В.Ф. Проблемы и перспективы использования искусственного интеллекта в системах электронного документооборота / Н.Н. Ковалева, П.В. Ересько, В.Ф. Изотова // Вестник Воронежского государственного университета. Серия: Право. – 2023. – № 4 (55). – С. 87–92.

Иовлева А.С., следователь по особо важным делам
1 отдела Следственной части по расследованию организованной
преступной деятельности ГСУ ГУ МВД России
по г. Санкт-Петербургу и Ленинградской области
майор юстиции

ПРИМЕНЕНИЕ МЕРЫ ПРЕСЕЧЕНИЯ В ВИДЕ ЗАПРЕТА ОПРЕДЕЛЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация

Запрет определенных действий является единственной динамичной мерой пресечения, которая в процессе применения может меняться исключая, либо вводя новые запреты. В статье рассматриваются возможности применения современных цифровых технологий для целей уголовного судопроизводства в рамках реализации уголовного процесса. С учетом множественности видов киберпреступлений представляется возможным применение в отношении преследуемых лиц ограничений включающих запрет на использование средств связи и информационно-телекоммуникационной сети «Интернет». Автором предложены новые способы контроля за соблюдением возложенных судом запретов, предусмотренных ч.6 ст.105.1 УПК РФ.

Ключевые слова: запрет определенных действий, меры пресечения, киберпреступность, IT- преступления, информационная безопасность.

Свободное пространство сети «Интернет», содержащее минимальное количество ограничений, открывает огромную платформу для совершения противоправных деяний, которые в научной среде и правоприменительной практике именуются киберпреступлениями или IT-преступностью. Развитие сетей связи, активное использование возможностей информационно-коммуникационных технологий в бизнесе и государственном управлении, легкий и непрерывный доступ к конфиденциальной информации или данным способствует появлению новых способов криминальной активности, наносящих ущерб экономической целостности страны. Именно в кибернетическом пространстве, которое считается виртуальным и нематериальным, совершаются многочисленные преступления, нанося значительный ущерб: физические лица и отечественные корпорации несут экономические убытки, государственные учреждения приостанавливают работу, тем самым снижая процессы социального обеспечения населения. Кража личных данных и аккаунтов, кибератаки на различного рода интернет-ресурсы, прерывание связи, носят международный характер и могут повлечь угрозу национальной безопасности.

Одним из видов воздействия и обеспечения надлежащего функционирования интернет-пространств является разработанная система контроля и анализа трафика для блокировки нежелательных ресурсов в сети «Интернет», внесенных в Единый реестр запрещённых сайтов. Ограничение доступа к информации устанавливается федеральными законами и актами Президента Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства [1].

Безопасность, осуществляемая в интернет-среде, организована согласно Федеральному закону от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации». Введение действующих ограничений в сети «Интернет» создает экологичность интернет-пространств и возможность дифференцированного контроля со стороны государства. Важным практическим способом борьбы с IT-преступностью действующее законодательство определяет максимальную идентификации лица (пользователя) в существующем едином информационном поле глобальной сети, а также отнеся операторов связи к значимым объектам критической информационной инфраструктуры [2], с присвоением категорий значимости и указанием в реестре (данный признак является квалифицирующим ст.274.1 УК РФ).

Согласно части 1.3 статьи 1.1 Федерального закона от 08.08.2024 № 303-ФЗ «О внесении изменений в Федеральный закон "О связи" и отдельные законодательные акты Российской Федерации»: «в случае, если объем аудитории персональной страницы составляет более десяти тысяч пользователей социальной сети и сведения о такой персональной странице не включены в перечень персональных страниц, создавший такую персональную страницу пользователь социальной сети не вправе размещать информацию, содержащую предложения о финансировании данного пользователя, а также сведения о возможных способах осуществления этого финансирования».

Мониторинг запрещённых сайтов, аккаунтов и иных источников, служащих угрозой целостности инфопространства РФ, осуществляется беспрерывно «Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций» [3], фактически реализуется через установленное программное обеспечение с введением необходимых фильтров и расширений (пример, как программно-аппаратный комплекс «Ревизор», «СКАТ»).

А.Ю. Чурикова, анализируя позитивный опыт применения искусственного интеллекта «в качестве ключевых направлений применения программного обеспечения в целях противодействия киберпреступности выделяет:

1) «умный» анализ большого массива данных;

2) использование чат-ботов для информирования населения и широкого распространения информации;

3) предиктивный анализ, позволяющий прогнозировать преступную активность.» [4]

С учетом возможности современных цифровых технологий, неизбежно встает вопрос о применении их для целей уголовного судопроизводства в рамках реализации уголовного процесса. К сожалению, интеграция в действующую правоохранительную систему цифровых инструментов ничтожно мала, отправление правосудия ведётся в «ручном» режиме, не позволяя в полной мере обрабатывать большой массив информации и своевременно реагировать на меняющиеся требования информационной преступности.

В ходе расследования киберпреступлений встает вопрос об избрании в отношении обвиняемых адекватной меры пресечения. Отечественный законодатель придерживается политики сокращения числа лиц, содержащихся под стражей, чему находится много сторонников в научном сообществе. Соответственно, с учетом действующей иерархии системы мер пресечения, множественности видов киберперступлений, следует признать, что заключение под стражу не относится к

приоритетным мерам пресечения такого вида преступной деятельности. Представляется, что наиболее оптимальными мерами пресечения для киберперступников являются домашний арест (ст.107 УПК РФ) и запрет определенных действий (ст.105.1 УПК РФ), устанавливающие ограничения не связанные с лишением свободы, и могущие включать, помимо прочего, запрет на использование средств связи и информационно-телекоммуникационной сети «Интернет».

Запрет определенных действий как мера пресечения получила широкое распространение на территории РФ с момента введения ее в действующее законодательство, однако, правоприменителями создана неоднозначная практика. У рассматриваемой меры нет ограничений применения в части отражающей квалификации содеянного, то есть в отношении обвиняемого или подозреваемого независимо от категории совершенного преступления, характерны основания, позволяющие применить любые запреты, предусмотренные ч.6 ст.105.1 УПК РФ. (применима с изъятиями запретов в совокупности со ст.ст.106, 107 УПК РФ).

Исследуемая природа запретов дает основания полагать, что видимым инструментом в вопросе контроля могут стать наработки государства в сфере IT и современный подход к контролю и существованию уголовно-исполнительной системы в киберпространстве. Однако решение вопроса эффективного контроля за исполнением возложенных судом запретов представляется сложной задачей.

Как мы указали ранее, в Интернет-пространстве имеются контролируемые ограничения, экосистема портала «Госуслуг» успешно защищает конфиденциальные данные от хакеров с помощью внедрения двухфакторной аутентификации (2FA), частично обладает самообучающимся искусственным интеллектом, также в виртуальной сети на территории РФ работает единая централизованная система мониторинга, позволяя блокировать интернет-ресурсы, внесённые в Единый реестр запрещённых сайтов. При существующих возможностях, на сегодняшний день реализация контроля запретов, предусмотренных ч.6 ст.105.1 УПК РФ не отвечает техническим мощностям уголовно-исполнительных инспекций УФСИН России на территориальном уровне.

Таким образом, стоит обратить внимание на введение отдельных альтернативных мер по контролю осуществления запретов избранных в судебном порядке в отношении обвиняемого (подозреваемого), таких как, например, разработка технического программного обеспечения с установлением на компьютерную технику (телефонного оборудования) обвиняемого (подозреваемого), позволяющих отслеживать местоположение лица, с блокированием входящих звонков, с запретом осу-

ществления звонков участникам процесса, с отправлением о нарушении действующих ограничений сигнала сотруднику УФСИН и другое.

Безусловно, приложение по осуществлению контроля по исполнению наложенных судом запретов в настоящее время может выглядеть как индикатор риска повторного совершения или сокрытия преступления, а также могут быть затронуты права субъектов при автоматизированной обработке их персональных данных [5].

Развитие цифровых гигантских экосистем (портал «Госуслуги»), соединения в едино большого количества баз и мгновенная обработка информации позволяет существенно быстрее реагировать на контролируемых субъектов. Существуют все технические возможности с минимальной стоимостью технического оснащения в виде разработки программного обеспечения, которое может выступить реальной альтернативой применения браслетов (СЭМПЛ – система электронного мониторинга подконтрольных лиц) к лицам, находящимися под домашним арестом, либо к которым применены ограничения, предусмотренные действующим законодательством ч.6 ст.105.1 УПК РФ. Определение степени и границ допустимого вмешательства в частную жизнь, охраняемую Конституцией РФ при осуществлении контроля в рамках отправления правосудия, используя возможности Интернет-ресурса еще предстоит установить и апробировать посредством включения современных технологий не только на первоначальных этапах раскрытия киберпреступлений, но и для дальнейшего обеспечения целей уголовного процесса до вступления приговора в законную силу.

Список цитируемой литературы

1. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ (в ред. от 23 ноября 2024 г.)// Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1. – Ст. 3448.
2. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ (в ред. от 10 июля 2023 г.) // Собрание законодательства Российской Федерации. – 2017. – № 31. – Ч. 1. – Ст. 4736.
3. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»): постановление Правительства Рос. Федерации от 16 марта 2009 г. № 228 (в ред. от 18 июля 2024 г.) // Собрание законодательства Российской Федерации. – 2009. – № 12. – Ст. 1431.

4. Чурикова, А.Ю. Применение искусственного интеллекта и индикаторов риска для противодействия киберпреступности/ А.Ю. Чурикова // Российский следователь. – 2024. – № 5. – С. 47–51.
5. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ (в ред. от 8 августа 2024 г.) // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1. – Ст. 3451.

Клементьева Е.С., ст. преподаватель
ФГКОУ ВО «Московский университет МВД России
имени В.Я. Кикотя», г. Москва

Мишуков Я.О., студент
ФГБОУ ВО «Российский государственный университет правосудия»,
г. Москва

НОВЫЕ ПОДХОДЫ В УГОЛОВНО-ПРАВОВОЙ ОХРАНЕ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Аннотация

В статье рассматриваются актуальные вопросы уголовно-правовой охраны права на неприкосновенность частной жизни. Правовое регулирование в этой сфере должно соответствовать современным вызовам. Анализируются проблемы, обусловленные открытостью и доступностью персональных данных в киберпространстве.

Ключевые слова: права человека, неприкосновенность частной жизни, интернет, личная информация, персональные данные, уголовный закон.

Стремительное развитие цифровых технологий, увеличение объема обрабатываемых личных данных граждан привело к уязвимости права на неприкосновенность частной жизни. В условиях, когда персональные данные могут быть собраны, обработаны и использованы в огромных масштабах как государственными, так и частными структурами, защита этого конституционного права требует пересмотра подходов к регулированию и правоприменению. Отмечается рост преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, включая неприкосновенность частной жизни, личную и семейную тайну, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся всё более

изощрёнными. Существенная проблема состоит в том, что имеющиеся правовые механизмы не всегда успевают адаптироваться к новым вызовам цифровой среды, что требует научного анализа и разработки новых решений для баланса интересов граждан, государства и бизнеса.

Проблемы уголовно-правовой охраны частной жизни представляют научный интерес, были предметом рассмотрения в работах ученых - И.Р. Диваевой, В.П. Жеребкина, Б.Н. Кадникова, О.В. Максимовой, Т.Н. Нуркаевой, И.А. Шевченко, Е.В. Хохловой и других.

Частью 1 статьи 23 Конституции Российской Федерации каждому гарантировано право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а согласно части 1 статьи 24 Основного закона сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, подобного рода положения содержатся в статье 12 Всеобщей Декларации прав человека (1948 г.), статье 17 Международного пакта о гражданских и политических правах. Понятие «частная жизнь» находится в тесной взаимосвязи с такими явлениями, как «тайна» и «неприкосновенность». В научных трудах виды тайн, относящихся к частной жизни, трактуются неоднозначно. Однако личная и семейная тайны несомненно составляют её важнейшие составляющие.

Частная жизнь — это собственное пространство личности: то, что касается конкретного человека и не должно контролироваться обществом и государством, если нет нарушения закона.

В Указе Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [3] говорится о необходимости обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну (п. 31).

Право на неприкосновенность частной жизни считается неотъемлемой частью личных прав. При этом его содержание трактуется неоднозначно. Некоторые ученые выделяют в составе личных прав отдельные категории, такие как защита частной жизни, неприкосновенность жилища, конфиденциальность переписки и телефонных разговоров (К.Б. Толкачев, Е.И. Козлова и др.), другие полагают, что эти права органично включаются в содержание права на неприкосновенность личной жизни (И.Б. Григорьев, Малеин Н.С., Красавчикова Л.О. и др.).

Право на неприкосновенность частной жизни связано с правом на личную свободу, т. е. индивид сам определяет границы открыто-

сти своей частной жизни. В этой связи неслучайно подобные преступления относятся к категории частно-публичного обвинения, где потерпевший

Следует отметить, что развитие общественных отношений в информационной сфере приводит как к расширению содержания тайны частной жизни – к ним добавляются персональные данные лица, биометрия, геолокация и перемещение лица и пр. Особенно уязвимыми является личная информация, имеющая цифровую форму. Процесс цифровизации общественных отношений приводит к появлению цифровых прав или прав в цифровой форме, соответственно появляются новые способы противоправных нарушений этих прав. В содержание права на неприкосновенность частной жизни включаются информационные составляющие, такие как право индивида контролировать информацию о себе, а также сбор, обработку и использование персональных данных, недопустимость использования личных данных без согласия лица.

Исследователи придерживаются разных подходов к определению термина «частная жизнь». Е.В. Хохлова считает необходимым разграничить понятия «частная жизнь» и «персональные данные» и предлагает использовать термин «неприкосновенность персональных данных», подчеркивая необходимость их уголовно-правовой защиты [7, С. 14].

В свою очередь, Д.В. Санников рассматривает частную жизнь более широко, выделяя три группы данных: идентификационные (цифровые персональные данные, включая аккаунты, cookie-файлы, цифровые изображения и 3D-модели органов), тайные (банковская, нотариальная, врачебная тайны и другие, хранящиеся в информационных системах) и коммуникационные (геолокационные данные, переписка в мессенджерах или электронной почте) [6, С. 13].

Законодатель, регламентируя уголовно-правовую охрану частной жизни, сосредотачивается на уточнении предмета преступления в соответствующих статьях.

Основная статья, охраняющая неприкосновенность частной жизни, — ст. 137 УК РФ, однако перечень норм, направленных на защиту личной информации, расширяется. Так, нарушение тайны переписки, телефонных переговоров или иных сообщений регулируется ст. 138 УК РФ, если действия нарушают личную, семейную или иную тайну частного характера.

Кроме того, нарушение неприкосновенности жилища (ст. 139 УК РФ) может быть связано с вмешательством в частную жизнь, так как предоставляет доступ к информации о личной жизни. Это особенно

актуально, если вторжение сопровождается разглашением данных личного характера.

Нарушение тайны усыновления (удочерения), определяемое как незаконное распространение сведений о семейной тайне без согласия лица (ст. 155 УК РФ), также рассматривается как вмешательство в частную жизнь и выступает частной нормой относительно ст. 137 УК РФ.

Одной из наиболее значительных угроз является несанкционированный сбор данных. Современные технологические компании активно используют данные о пользователях для улучшения своих продуктов, что нередко ведет к массовому сбору персональной информации. Пользователи часто не имеют достаточной информации о том, как и в каких целях используются их данные. Законодательство стремится регулировать эти процессы, но технологии и методы сбора данных развиваются быстрее, чем могут адаптироваться законы. В России, например, законодательство в области персональных данных основывается на Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» [1], но его положения нуждаются в актуализации в свете постоянно меняющихся цифровых реалий.

Новые формы личной информации требуют новых подходов в их защите. В Указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» подчеркивается необходимость снижения до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений, установленных российским законодательством требований по защите такой информации и персональных данных (пп. 6 п. 57) [3].

Превышение полномочий служащими частных охранных или детективных служб, предусмотренное ст. 203 УК РФ, тоже может посягать на неприкосновенность частной жизни, в части совершения действий, нарушающих права граждан на неприкосновенность жилища, тайну переписки, телефонных переговоров, телеграфных и иных сообщений. И опять же в связи с развитием информационно-коммуникационных технологий, наличием легального и нелегального сбора персональной информации, деятельность частных детективов находится на грани законности.

В связи с этим отметим важный шаг в этом направлении - принятие Федерального закона от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» [2], которым введена новая статья 272.1, предусматривающая уголовную ответственность за незаконные действия с персональными данными. Примечательно, что это вызвало неоднозначную реакцию юридического сооб-

щества. К преступным относятся как действия по собиранию, распространению сведений о частной жизни лица, так и персональных данных, в этой связи необходимо четкое разграничение этих понятий в уголовном законе.

Личные данные стали общедоступными благодаря многочисленным социальным сетям, вопросы правомерности использования данных из соцсетей, а также изображений лица с персональной страницы аккаунта остаются открытыми. Как верно отмечает Волкова Г.Е., цифровые следы («интернет-следы», «интернетотпечатки», digital footprint), которые ежедневно оставляем в информационном пространстве, после анализа и обобщения, проведенного с помощью возможностей искусственного интеллекта, могут сформировать наш цифровой портрет, содержащий более точные сведения как о поведении человека, его социальном статусе, взаимоотношениях с окружающими, вкусах и привычках, чем те, которые можно было бы узнать из личного общения или психологических тестов [5, С. 175].

Различные коммерческие организации, правоохранительные органы в своей деятельности используют технологии OSINT (англ. - Open Source Intelligence) – поиск информации (разведка) по открытым источникам в интернете с помощью определенных методов и средств, таким образом, частная жизнь человека становится уязвимой для вмешательства. В связи с этим в Резолюции Генеральной Ассамблеи ООН от 18 декабря 2013 г. № 68/167 «Право на неприкосновенность личной жизни в цифровой век» подчеркивается, что необходимость обеспечения общественной безопасности может оправдывать сбор и защиту некоторой конфиденциальной информации, но государства должны гарантировать соблюдение в полном объеме своих международно-правовых обязательств в сфере прав человека.

В Указе Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [4] обозначены существующие угрозы праву на тайную жизнь в цифровой среде и ставятся цели по их предотвращению.

На наш взгляд, право на тайну частной жизни подразумевает возможность человека определять, как именно используется информация о нем, а также его право на сохранение конфиденциальности сведений о личной жизни. Обеспечение данной конфиденциальности должно быть задачей как государства через разработку правовых норм, так и сервисов, занимающихся хранением и обработкой данных.

Подводя итог проблемам уголовно-правовой охраны права на неприкосновенность частной жизни в эпоху цифровизации, следует обратить внимание на изменения содержательной стороны этого пра-

ва, особенности и механизмы реализации, защиты этого права человека, о важности выработки точно определенных законодательных формулировок.

Список цитируемой литературы:

1. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 № 152-ФЗ (в ред. от 8 августа 2024 г.) // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. 1. – Ст. 3451.
2. О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 30 ноября 2024 № 421-ФЗ // Собрание законодательства Российской Федерации. – 2024. – № 49. – Ч. IV. – Ст. 7412.
3. О Стратегии национальной безопасности Российской Федерации: указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27. – Ч. II. – Ст. 5351.
4. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Рос. Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.
5. Волкова, Г.Е. Право на неприкосновенность частной жизни в цифровую эпоху / Г.Е. Волкова // Философия права. – 2022. – № 4 (103). – С. 174-178.
6. Санников, Д.В. Гражданско-правовая охрана частной жизни в условиях цифровизации общества : автореферат дисс. ... канд. юрид. наук / Д.В. Санников. – Ульяновск, 2024. – 32 с.
7. Хохлова, Е.В. Незаконные действия с персональными данными уголовно-правовое исследование : автореф. дисс. … канд. юрид. наук / Е.В. Хохлова. – Саратов, 2023. – 26 с.

Климов А.С., канд. юрид. наук, доцент, зав. кафедрой
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Особенности совершенствования уголовного законодательства, предусматривающего ответственность за киберпреступления

Аннотация

В данной статье рассматриваются особенности совершенствования уголовного законодательства, предусматривающего ответственность за киберпреступления. Проанализированы изменения, внесенные в 2024 году в Уголовный кодекс РФ в сфере противодействия киберпреступлениям.

Ключевые слова: информационно-телекоммуникационные сети, информационно-телекоммуникационные технологии, киберпреступления, компьютерная информация, персональные данные

Стремительное развитие информационных технологий в XXI веке повлекло за собой изменение в различных видах и сферах деятельности, так особенно заметно расширился дистанционный формат различных работ, а также получило широкое распространение использование искусственного интеллекта. Все это, в свою очередь, повлекло увеличение количества преступлений, совершенных в сфере информационных технологий. По сей день в Уголовном кодексе РФ нет определения «киберпреступление». Среди ученых под «киберпреступлениями» понимают: ««преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами», «преступления в высоких компьютерных технологиях», «преступления в информационном пространстве» и т.д.» [2, с. 162].

В период с января по декабрь 2024 года в России было зафиксировано 765,4 тысячи киберпреступлений, что на 13,1% больше, чем за аналогичный период 2023 года. Согласно документам МВД, их доля среди всех зарегистрированных преступлений увеличилась с 34,8% в 2023 году до 40% в 2024 году. В 2022 году доля IT-преступлений составляла 26,5% от общего количества преступлений в стране, в 2021 году – 25,8%, а в 2020 – 25%.

По мнению В. Б. Клишкова, Е. В. Стебеневой и М. А. Яковлева к признаками киберпреступлений можно отнести следующее: «1) опера-

тивность; 2) удаленность; 3) масштабность; 4) высокая анонимность; 5) самодостаточность; 6) виртуальности» [3, с. 107].

В Уголовном кодексе Российской Федерации содержатся статьи, относящиеся к так называемым «киберпреступлениям» - это, прежде всего, деяния, которые содержатся в гл. 28 «Преступления в сфере компьютерной информации», а именно ст.ст. 272-274.2 УК РФ, кроме того широкое распространение получил квалифицирующий признак – «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», а также «совершенное с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»).

В то же время 15.12.2022 г. было принято постановление Пленума Верховного Суда РФ № 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»», посвященный вопросам, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»».

В целом киберпреступления совершаются с целью: 1) оказать влияние на конкретное лицо или группу и добиться соответствующего поведения. Цель в этом случае может быть абсолютно любая – приобретение материальных благ или освобождение от материальных затрат, продвижение экстремистских идей, удовлетворение половой страсти и т. д.; 2) получить соответствующую информация, как правило, это персональные данные.

Только в 2024 году в уголовное законодательство, предусматривающее ответственность за киберпреступления были внесены изменения целым рядом законов: 1. Федеральный закон от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»; 2. Федеральный законом от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»; 3. Федеральный закон от 28.12.2024 № 514-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

Федеральным законом от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в законодательство было внесено новое отягчающее обстоятельство – «т) совершение

умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)», кроме того, в статьи глав 16 и 17 УК внесен квалифицирующий признак – «совершенное с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»). В пояснительной записке данного проекта отмечено, что в последнее время становится популярным треш-стримы. Треш (от английского Trash - мусор, отбросы, сор; strim - поток) - это потоковое видео или аудио. Данный термин также употребляется пользователями как сленговое название прямых трансляций на видеохостингах. Ю. В. Грачева и С. В. Маликов определяют треш-стрим, как: «специфический жанр прямых трансляций в интернете, в ходе которых за вознаграждение (как правило, это деньги) участники (стримеры) выполняют различные задания, сознательно нарушая грани дозволенного и приемлемого в обществе поведения (насилие, унижение, оскорбление)» [1, с. 203].

Также, в пояснительной записке отмечено, что совершение преступлений с публичной демонстрацией повышает уровень общественной опасности деяния и имеет дополнительный объект - общественную безопасность и общественный порядок, особенно страдает психика детей и молодых людей, они начинают подражать известным трешстримерам. Характерно, что именно в указанных составах предусматривается такое дополнительное наказание, как лишение права занимать определенные должности или заниматься определенной деятельностью, именно это позволит ограничить доступ преступников в сеть «Интернет».

Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в главу 28 была внесена ст. 272.1 – «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения».

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Объективная сторона данного преступления может выражаться в следующих незаконных действиях в отношении компьютерной информации, содержащей персональные данные, полученной незаконным путем: 1) использование; 2) передача (распространение, предо-

ставление, доступ); 3) сбор; 4) хранение. В ч. 6 ст. 272.1 УК предусмотрена ответственность за создание и (или) обеспечение функционирования информационного ресурса (сайта в сети «Интернет» и (или) страницы сайта в сети «Интернет», информационной системы, программы для электронных вычислительных машин), заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем.

Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 28.12.2024 № 514-ФЗ добавил квалифицирующие признаки в ст.ст. 150 и 151 Уголовного кодекса РФ - с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). В пояснительной записке к Проекту Федерального закона N 670471-8 «О внесении изменений в статьи 150 и 151 Уголовного кодекса Российской Федерации» указано, что внесение данных квалифицирующих признаков обусловлено тем, что в современных реалиях такие деяния, совершенные с использованием информационно-телекоммуникационных технологий, получают все более широкое распространение за счет отсутствия непосредственного контакта жертвы и преступника, анонимности и возможности охвата обширной аудитории несовершеннолетних.

Таким образом, следует отметить, что в уголовном законодательстве происходит трансформация, которая обусловлена широким распространением информационно-телекоммуникационных технологий, а также распространением преступлений, которые совершаются при отсутствии непосредственного контакта потерпевшего и преступника.

Список цитируемой литературы:

1. Грачева, Ю.В., Маликов, С.В. Треш-стрим: социальная обусловленность криминализации/ Ю.В. Грачева, С.В. Маликов // Актуальные проблемы российского права. – 2021. – № 16 (6). – С. 202-210.
2. Кочкина, Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений / Э.Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3. – С. 162-169.
3. Клишков, В.Б., Стебенева, Е.В., Яковлева, М.А. Киберпреступность: понятие, признаки, основные направления противодействия/ В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева // Вестник Нижегородского университета им. Н. И. Лобачевского. – 2022. – № 4. – С. 106-113.

Кочкина М.С., адъюнкт
ФГКОУ ВО «Воронежский институт МВД России»,
старший лейтенант полиции, г. Воронеж

Предупреждение онлайн-груминга несовершеннолетних в сети Интернет

Аннотация

Статья посвящена исследованию сущности онлайн груминга несовершеннолетних и разработке эффективных мер его профилактики. Предлагает комплексный подход к профилактике рассматриваемого явления.

Ключевые слова: онлайн-груминг, сексуальная эксплуатация, несовершеннолетние, интернет-безопасность, цифровые технологии.

Груминг (англ. grooming – «ухаживание») представляет собой долговременное установление взрослым близких, доверительных отношений с несовершеннолетним с целью завоевания доверия и последующего сексуального совращения. В последние годы груминг стал особенно распространен в онлайн-среде, где грумеры используют социальные сети, мессенджеры и онлайн-игры для установления контакта с детьми. Несмотря на свою популярность данное явление остается малоизученным в России, в то время как зарубежные исследователи уже более 20-ти лет занимаются его всесторонним изучением [1,2]. Считаем, что онлайн-груминг следует рассматривать как форму сексуальной эксплуатации, которая заключается в установлении доверительных отношений с несовершеннолетним с целью совершения в отношение его преступлений в сфере половой неприкосновенности и половой свободы, как физически, так и удаленно.

Как правило, онлайн-груминг является манипуляцией, и зачастую многие его жертвы могут не осознавать опасность социальной коммуникации с грумером (взрослым человеком, который желает совершить посягательство на половую неприкосновенность или свободу несовершеннолетнего). Воспринимая такие отношения как дружеские или романтические подростки могут делиться с ним информацией откровенного характера, не осознавая, что это и есть его главная цель. В глазах несовершеннолетнего возможность такой близкой переписки предстает как степень высокой близости и доверия, в то время как грумер реализует свой преступный замысел.

К профилактическим мерам онлайн-груминга можно отнести:

– повышение осведомленности о проблеме: необходимо проводить широкомасштабные образовательные кампании для детей, роди-

телей и педагогов, фокусируясь на осознании рисков онлайн груминга и навыках безопасного поведения в интернете;

– улучшение технологических средств защиты: разработка и внедрение более эффективных инструментов родительского контроля и систем модерации контента являются необходимыми мерами;

– межведомственное взаимодействие: эффективная борьба с онлайн грумингом требует тесного сотрудничества между правоохранительными органами, специалистами по защите детей, провайдерами интернет-услуг и образовательными учреждениями;

– развитие психологической помощи: жертвы груминга нуждаются в специализированной психологической и психиатрической помощи для восстановления после травмы. Так, если подросток пережил сексуализированное насилие с целью минимизации последствий и защиты от сексуального насилия несовершеннолетних создан кризисный центр, который оказывает психологическую помощь несовершеннолетним, пережившим сексуальное насилие – «Тебе поверят» [3]. Данный сервис психологической поддержки создан независимыми психологами и функционирует с 2019 года. На сайте центра можно оставить заявку на бесплатные сеансы с психологом, ознакомиться с информационной подборкой, освещающей темы сексуального насилия над детьми.

Ряд зарубежных стран (Австралия, Великобритания, Канада, Польша) криминализировал онлайн груминг. В России же подобные действия могут быть квалифицированы по ст. 133 (понуждения к действиям сексуального характера) УК РФ и ст. 135 (развратные действия) УК РФ. Однако отсутствие юридического закрепления понятия «онлайн груминга» и его признаков, позволяют множественным фактам данного явления находиться за рамками правового поля, что является серьезной проблемой и заставляет задуматься о необходимости его криминализации в России.

Список цитируемой литературы:

1. Craven, S., Brown, S., & Gilchrist, E. Sexual grooming of children: Review of literature and theoretical considerations/ S. Craven, S. Brown, E Gilchrist // Journal of Sexual Aggression. –Volume 12. – 2006. – pp. 287– 299.
2. Finkelhor, D. Child sexual abuse new theory and research / D. Finkelhor. – New York, USA: The Free Press, 1984 – 260 p.
3. Тебе поверят. [Электронный ресурс] – Тебе поверят: интернет – платформа. – URL : https://teen.verimtebe.ru. (дата обращения: 11.01.2025).

Корнев А.С., канд. юрид. наук, доцент кафедры
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

К ВОПРОСУ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация

В современных условиях для любого государства одной из приоритетных задач становится обеспечение нормального и эффективного развития систем искусственного интеллекта (ИИ), а также пресечение преступных посягательств на данную сферу. Искусственный интеллект предоставляет собой новые возможности для человечества во всех сферах жизнедеятельности, но к сожалению, и в совершении различных преступлений. Это порождает новые вызовы для правоохранительных органов, традиционных методов расследования и правовой системы в целом. В данной статье рассматриваются ключевые аспекты выявления, раскрытия и расследования преступлений, совершенных с помощью ИИ, а также предложены рекомендации для эффективного противодействия этим угрозам.

Ключевые слова. Искусственный интеллект (ИИ), преступления.

Искусственный интеллект (ИИ) стал неотъемлемой частью повседневной жизни, оказывая влияние на различные сферы общества. К возможностям искусственного интеллекта и его внедрению в жизнь человека приковано внимание представителей всех отраслей науки, практики, а также и правоохранительных органов. И это неудивительно ведь с одной стороны отмеченное явление является малоизученным и многоаспектным, с другой же - внедрение подобных технологий возможно практически в неограниченном количестве сфер общества. Причем именно с возможностями и перспективами использования искусственного интеллекта (ИИ) все чаще ассоциируется прорывное технологическое развитие. Однако параллельно с его положительными аспектами возникают и негативные последствия.

В таких условиях для любого государства одной из приоритетных задач становится обеспечение нормального и эффективного развития систем искусственного интеллекта, а также пресечение преступных посягательств на общественные отношения в данной сфере. Кроме того, наряду со стимулированием развития указанных технологий важно выработать комплект мер, направленных на недопустимость использо-

вания систем искусственного интеллекта в преступных целях. Стоит отметить, что уже сегодня технологии искусственного интеллекта не только стимулируют трансформацию традиционной преступности, но и влияют на появление новых форм и видов противоправных деяний. Преступный элемент используют ИИ для автоматизации и оптимизации своих действий, что усложняет процесс выявления и расследования преступлений. Вместе с тем выполнение отмеченных задач невозможно без четкого понимания сущности и содержания такого явления как искусственный интеллект. Ведь бороться с тем, что неведомо или неясно невозможно, или, по меньшей мере, непродуктивно. Это в полной мере относится к выявлению. Раскрытию и расследованию преступлений, совершенных с помощью ИИ. Примеры таких преступлений включают кибератаки с использованием машинного обучения, подделку цифровых удостоверений личности, автоматизацию мошеннических схем, персонализации фишинг-атак, корпоративного шпионажа и манипуляций через фейковый контент и др.

Использования понятий, связанных с искусственным интеллектом в различных нормативно-правовых актах, свидетельствуют о терминологических неточностях, существующих в указанной области. К сожалению, в настоящее время существует обилие нормативно-правовых актов, рекомендаций в сфере искусственного интеллекта, которые не только не согласованы, но в ряде случаев содержат противоречащие друг другу положения. В этой связи в целях обеспечения устойчивого и эффективного развития указанных технологий, в том числе уголовно-правовой охраны общественных отношений в данной сфере целесообразно продолжить совершенствование правового регулирования в области искусственного интеллекта.

Применение ИИ в преступной деятельности вызывает множество вопросов, которые иногда не понятны для лиц из числа правоохранительных органов, которые выявляют, раскрывают и расследуют преступления, совершенные ИИ.

Так, рассмотрим некоторые:

- анонимность и сложность идентификации: использование ИИ позволяет преступным элементам оставаться анонимными, например, алгоритмы могут скрывать их местоположение или усложнять процесс отслеживания их действий;

- адаптивность и эволюция преступлений: киберпреступники используют ИИ для создания адаптивных стратегий, которые позволяют им обойти традиционные механизмы безопасности;

- этические и правовые вопросы: внедрение ИИ в процедуру выявления, раскрытия и расследования преступлений, может привести к

правовым и этическим дилеммам, связанным с соблюдением конфиденциальности и защиты прав граждан.

На взгляд автора, для успешного выявления, раскрытия и расследования преступлений, совершенных с помощью ИИ, правоохранительным органам необходимо адаптировать свои методы и стратегии. Разработать и подготовить специальные программы обучения для сотрудников оперативного блока и следственных подразделений, которые должны включать понятие, нормативную базу, а также изучение технологий ИИ и их применения как в повседневной жизни, так и в преступной деятельности.

Для повышения эффективности борьбы с преступностью в сфере ИИ, организовать межведомственное сотрудничество, то есть обмениваться информацией между различными подразделениями правоохранительных органов.

Применение современных аналитических платформ, способных обрабатывать большие объемы данных, что по мнению автора поможет в ускоренном порядке выявлять закономерности и аномалии в действиях преступников, которые пользуются услугами ИИ.

Данная статья подчеркивает ключевые проблемы и подходы к выявлению, раскрытию и расследованию преступлений, совершенных с использованием ИИ, и служит отправной точкой для дальнейших исследований в этой актуальной области.

Список цитируемой литературы:

1. Уголовное право. Общая часть: специализированный учебник для юридического колледжа / под ред. В. П. Бодаевского, В. М. Зимина, А. И. Чучаева. – Москва: Проспект, 2017. – 272 с.
2. Мосечкин И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник СПбГУ. Право. – 2019. – Т. 10. – Вып. 3. – С. 461–476.
3. Прозументов Л. М. Криминализация и декриминализация деяний. – Томск: Изд-во Том. ун-та, 2012. – 142 с.
4. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июля 1996 г. № 63-ФЗ (в ред. от 28 декабря 2024 г.)// Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

Кузнецов А.А., канд. юрид. наук, доцент кафедры
ФГБОУ ВО «Липецкий государственный технический университет»,
г. Липецк

Понятие цифровых доказательств

Аннотация

Использование возможностей цифровизации вывело гражданский процесс на новый уровень. Стало возможным использовать новые виды доказательств, которые представлены в электронном формате. Их цель – подтвердить юридически значимые обстоятельства. В современных условиях граждане и юридические лица всё чаще и чаще используют мессенджеры, такие как WhatsApp, Telegram для ведения повседневной и деловой переписки. Кроме того, возможно использование новых видов цифровых доказательств, которые до настоящего времени не получили надлежащей правовой оценки. Особое место занимает вопрос допустимости цифровых доказательств и их соответствие требованиям процессуального законодательства. Вопрос использования цифровых доказательств напрямую связан с законностью их получения. Цель настоящей статьи дать правовую оценку и предложить определение понятия «цифровые доказательства».

Ключевые слова: цифровые доказательства, процессуальное законодательство, допустимость доказательства, электронные документы, информационные технологии.

Развитие современных информационных технологий дало возможность для граждан и юридических лиц перейти в новый формат общения – цифровая переписка и цифровой документооборот. Он занимает важное место с точки зрения фиксирования информации и юридических фактов, имеющих значение для установления определенных обстоятельств.

Пандемия COVID-19 изменила ситуацию в целом. Широкое развитие получила дистанционная форма взаимодействия между хозяйствующими субъектами. Возможности информационно-телекоммуникационной сети «Интернет» дали новые возможности не только для получения информации, но и для электронного документооборота.

В ст. 434 Гражданского кодекса РФ закреплена возможность заключения договоров путём составления электронного документа [2]. Применительно к цифровому документу заключение договора связано с тем, что стороны путём переписки в мессенджерах определили все его существенные условия и усматривается факт соглашения.

Некоторые юристы при составлении договора отдельным пунктом указывают, что взаимодействие между сторонами сделки происходит посредством информационно-телекоммуникационной сети «Интернет».

Переход в новый цифровой формат общения путём использования электронной формы документа привел к тому, что в процессе судопроизводства стал использоваться новый вид доказательства, который вызвал много вопросов. Речь идёт о цифровых доказательствах.

Гражданский процессуальный кодекс РФ в ст. 55 даёт определение понятия доказательства [3]. Это полученные в предусмотренном законом порядке сведения о фактах, на основе которых суд устанавливает наличие или отсутствие обстоятельств, обосновывающих требования и возражения сторон, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела. Исходя из этого определения можно выделить следующие их признаки:

1) содержат сведения о фактах;

2) являются основанием для установления юридически значимых обстоятельств;

3) сведения получены на основании строго соблюдения законодательных норм.

В современных условиях Г.Г. Шинкарецкая относит к источникам получения доказательств персональные компьютеры, USB-накопители, мобильные телефоны и т.п. [7]. Содержащаяся в них информация может иметь различные формы, а именно: текстовые документы в виде файлов Word или Excel, электронные письма, сообщения в мессенджерах, цифровые изображения, данные GPS, истории интернет-браузеров, то есть, все то, что является атрибутом коммуникативной деятельности.

Важной особенностью цифровых доказательств является то, что многие из них находятся в открытом доступе и их получение не вызывает особого труда. Примером может служить официальный сайт предоставления сведений из ЕГРЮЛ/ЕГРИП в электронном виде (https://egrul.nalog.ru/index.html). Он позволяет получить выписки о зарегистрированных юридических лицах и индивидуальных предпринимателях. То есть, на официальных сайтах, которые размещены в информационно-телекоммуникационной сети «Интернет» размещена информация, которая определяет или опровергает определенные юридические факты.

Ещё одна особенность цифровых доказательств состоит в том, что все действия с документированной информацией обрабатываются, сохраняются, передаются по каналам цифровой связи или с помощью электронных носителей.

Практически во всех процессуальных кодифицированных актах есть упоминание о цифровых доказательствах.

В части 1 ст. 71 ГПК РФ определено, что к письменным доказательствам относятся документы и материалы, выполненные в форме цифровой записи с использованием сети «Интернет» [4].

В части 3 ст. 75 АПК РФ, части 1 ст. 70 КАС РФ представлено аналогичное определение цифровых доказательств, которое также дано через по-нятие письменных доказательств.

Уголовно-процессуальный кодекс РФ не даёт четкого определения понятия «цифровое доказательство». В части 2 ст. 84 УПК РФ они отнесены к иным носителям информации [3].

Таким образом, имеет место правовая неопределенность и неясность при реализации понятия цифровые доказательства. Это привело к тому, что их нельзя признать универсальными доказательствами.

Для формирования определения цифровых доказательств необходимо их юридическую допустимость, которая связана с законностью их получения. Если речь идёт о том, что они получены из официальных источников, таких как Единый портал государственных и муниципальных услуг (ЕПГУ) или Госуслуги (gosuslugi.ru), то полученные справки, выписки и иные документы имеют статус официальных. Это связано с тем, что этот портал является федеральной государственной информационной системой, которая позволяет идентифицировать правообладателя учетной записи в личном кабинете. В этой связи портал Госуслуг представляет интерес для мошенников.

Говоря о цифровых доказательствах необходимо упомянуть о том, что если они получены с нарушением действующего законодательства, то они не могут быть признаны допустимыми. Это следует из положений ст. 23 Конституции РФ, которая устанавливает гарантии неприкосновенности частной жизни [1].

Неоспоримым является тот факт, что цифровые доказательства имеют большое значение в современных условиях развития информационного общества. При этом, их исследование связано с использованием специального подхода. С одной стороны, это может быть исследование и анализ цифровых доказательств в рамках процессуальных правомочий о проведении экспертизы. Ни судья, ни участники процесса не обладают специальными познаниями в области информационных и компьютерных технологий. Основная цель проведения экспертизы в том, чтобы целостность и соответствие цифровых доказательств процессуальным требованиям. С другой стороны – суд может самостоятельно исследовать источник, где находятся эти доказательства. Например, одно из самых распространенных доказательств – это пере-

писка в мессенджерах и социальных сетях. По ходатайству одной из сторон, которая располагает цифровыми доказательства-ми в виде обмена электронными письмами, где указывается владелец телефона, кому принадлежит используемый норме, также для обзора суду предоставляется сам телефон с перепиской.

Анализ судебной практики показал, что четкое соблюдение алгоритма исследования цифровых доказательств делает их весьма эффективным инструментом для установления истины по делу. Кроме того, соблюдается такие конституционные принципы судопроизводства, как:

– законность, определенный в части 2 ст. 15 Конституции РФ [1];

– равенство участников процесса перед судом и законом, часть 1 ст. 19 Основного закона.

Также реализуются процессуальные принципы состязательности и равноправия сторон, независимости судей и гласности правосудия.

Важно понимать, что современные цифровые технологии постоянно меняются и совершенствуются, что требует от законодателя постоянного правового совершенствования регулирования и поиска новых методов проведения экспертизы.

Основными формами цифровых доказательств является электронный документ; цифровое видео; цифровая фотография. Все они выступают носителями информации, то есть, содержат сведения о юридических фактах и выполняют другие функции, например, коммуникационные. Перечисленные цифровые доказательства используются в различных публично-правовых и иных правоотношениях.

Важной особенностью цифровых доказательств является то, что они содержатся в цифровой и буквенно-графической форме.

Следует отметить, что подтверждением достоверности цифровых доказательств является исполнение электронной подписи с различной степенью защиты.

Много вопросов возникает при анализе и использовании цифровых доказательств в рамках уголовного процессуального законодательства. Положения современного УПК РФ не содержат действенного инструментария для обнаружения, фиксации и закрепления этого вида доказательств. Это связано с тем, что правовая природа цифровых доказательств не позволяет работать с ними в рамках имеющихся следственных действий. Это следует из цифрового характера исследуемых доказательств, а именно содержание цифровой информации не зависит от фиксации на конкретном материальном носителе, поскольку электронные носители информации не уникальны и легко заменимы.

Важность и значение цифровых доказательств для выявления, предупреждения и пресечения преступной деятельности заключается в

том, что они содержат метаданные, которые включают в себя тип файла, дата создания, название, автор, устройство на котором был создан, кем изменялся и т.д. Они входят в предмет доказывания и могут являться доказательством обстоятельств совершения преступления.

Все эти свойства не позволяют осматривать цифровые доказательства в рамках видов осмотров, которые закреплены в УПК РФ, поскольку их невозможно отнести ник предметам, ни к документам.

Решение этой проблемы возможно путём закрепления в ст. 176 УПК РФ нового следственного действия – осмотр цифровых доказательств. Реализация этого предложения повлечет за собой закрепление в ст. 177.1 УПК РФ конкретного механизма сбора цифровых доказательств. Важно закрепить привлечение специалиста к осмотру цифровой информации. Для этого ему надо разъяснить права и обязанности, а также ответственность. Специалист должен обеспечить доступ к цифровой информации с помощью специальных технических устройств. Кроме того, в обязанность специалиста должна входить обеспечение целостности этого вида информации.

Согласно ч.5 ст. 166 УПК РФ в протоколе должны быть указаны также технические средства, примененные при производстве следственного действия, условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты.

Можно сказать, что в рамках настоящего научного исследования предложен универсальный механизм сбора цифровых доказательств.

Таким образом, бесспорным является то, что цифровые доказательства занимают важное место в процессуальной деятельности судов, при этом, необходимо соблюдение нескольких, на наш взгляд, важнейших условий. Прежде всего, соблюдение законности получения цифровых доказательств, что обеспечит их допустимость в рамках процессуального законодательства. Достоверность доказательств обеспечивается с помощью нотариального заверения и проведения технической экспертизы. Ещё одно обстоятельство, без которого нельзя говорить о юридической значимости цифровых доказательств – это особенности их хранения и передача содержащихся в них данных.

Список цитируемой литературы:

1. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г.(в ред. от 5 октября 2022 г.) // Собрание законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.
2. Гражданский кодекс Российской Федерации. Часть 1 : федер. закон Рос. Федерации от 30 ноября 1994 г. № 52-ФЗ (в ред. от 08 августа

2024 г.) // Собрание законодательства Российской Федерации. – 1994. – № 52, ч. 1. – Ст. 5496.
3. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 года № 95-ФЗ (в ред. от 28 декабря 2024 г.)// Собрание законодательства Российской Федерации. – 2001. – № 52, ч. I. – Ст. 4921.
4. Гражданский процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 14 ноября 2002 г. № 138-ФЗ (в ред. от 31 июля 2025 г.) // Собрание законодательства Российской Федерации. – 2002. – № 46. – Ст. 4532.
5. Арбитражный процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 24 июля 2002 г. № 95-ФЗ (в ред. от 01 апреля 2025 г.): федер. закон Рос. Федерации от 24 июля 2002 года № 95-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 30. – Ст. 3012.
6. Кодекс административного судопроизводства Российской Федерации: федер. закон Рос. Федерации от 8 марта 2015 г. № 21-ФЗ (в ред. от 07 июня 2025 г.)// Собрание законодательства Российской Федерации. – 2015. – № 10. – Ст. 1391.
7. Жукова, А. И. К вопросу о применении электронных доказательства в гражданском судопроизводстве / А. И. Жукова // Цивилистика : право и процесс. – 2024. – № 1. – С. 50–57.
8. Михайленко, Н. В. Перспективы и проблемы отправления цифрового правосудия в Российской Федерации / Н. В. Михайленко // Закон и право. – 2020. – № 4. – С. 120–127.
9. Основы теории электронных доказательств: монография / под ред. д-ра юрид. наук С.В. Зуева. – Москва: Юрлитинформ, 2019. – 400 с.
10. Шинкарецкая, Г.Г. Цифровые доказательства в процессе Международного Суда / Г. Г. Шинкарецкая // Международное право и международные организации / International Law and International Organizations. – 2023. – № 1. – С. 55–65.

Кунц Е.В., д-р. юрид. наук, профессор, гл. науч. сотрудник
ФКУ «Научно-исследовательский институт
Федеральной службы исполнения наказаний», г. Москва

СТРАТЕГИЯ ПО ПРЕДОТВРАЩЕНИЮ ПРЕСТУПЛЕНИЙ В КИБЕПРОСТРАНСТВЕ

Аннотация

В статье отмечается, что преступления, совершаемые в кибепространстве в настоящее время, превратились в серьезную проблему. Точные масштабы распространения этих преступлений неизвестны. Рост масштабов преступлений, совершаемых в сети Интернет, привел к тому, что представители правоохранительных органов вынуждены активно противостоять постоянно развивающимся угрозам со стороны киберпреступности, которые усугубляются быстрым развитием технических средств, используемых правонарушителями. Установлено, что преступники могут применять эти средства для противоправной деятельности в различных юрисдикциях, что позволяет им мгновенно нарушать не только административные границы, но и государственные границы, несколькими простыми ударами по клавиатуре компьютера или несложными манипуляциями с «умными» устройствами.

Ключевые слова: жертва, интернет, киберпространство, правоохранительные органы, подозреваемый, преступления, расследование.

В сложившейся ситуации правоохранительные органы должны тесно взаимодействовать друг с другом. Ни один государственный орган, независимо от своих размеров и ресурсов, не может позволить себе действовать самостоятельно. Более чем когда-либо прежде, высшей ценностью становится объединение усилий на всех уровнях – федеральном, региональном и местном. Реагирование на преступления в киберпространстве и их профилактика являются высшими приоритетами для обеспечения суверенитета государства.

Киберпреступность порождает многочисленные проблемы, и особо важными из них являются те, что совершаются через компьютерные устройства и сеть Интернет либо становятся возможными благодаря им.

Преступления, представляющие собой прямую угрозу правам и свободам человека, исторически всегда находились в центре внимания отечественной правоохранительной системы. В течение многих лет указанные органы осуществляли защиту прав и интересов детей от тех, кто пытался сделать их своей добычей и лишить невинности. По мере того, как расширялось использование Интернета, для представителей правоохранительных органов становилось все более очевидным, что постоянно суще-

ствующая проблема защиты детей от сексуального насилия и онлайн-хищников, занимающихся распространением детской порнографии, становилась все более сложной и многообразной. Подозреваемых стало сложнее обнаружить и идентифицировать, поскольку они используют все более совершенные методы анонимизации в сети и другие способы маскировки, затрудняющие их выявление и поимку. Чтобы защитить тех, кто подвергается риску стать жертвой преступников, органы правопорядка должны установить между собой прочные и успешные взаимоотношения.

Наряду с вложениями в инфраструктуру и совершенствование ресурсов и возможностей сотрудники правоохранительных органов культивируют тесные партнерские отношения. Правоохранительные органы активно используют возможность сотрудникам проходить профессиональную переподготовку для овладения передовыми методами расследований, а также пользоваться компьютерным криминалистическим оборудованием.

Сложность в четком определении способа и обстоятельств совершения компьютерных преступлений в их расследовании связана с используемой в данной сфере терминологий, поскольку она имеет технический характер [1, С. 123].

Практика, которая применяется в ходе расследования преступлений против детей или любой другой противоправной деятельности в киберпространстве, заключается в том, чтобы «вести» подозреваемых или их жертвы в многочисленных юрисдикциях и в разных странах по всему миру. Способность при проведении расследования использовать для достижения поставленных целей устоявшиеся отношения с правоохранительными органами за пределами Российской Федерации неоднократно приводила к успеху расследований внутри страны. В то же время правоохранительные органы извлекают неоценимую пользу из опыта и знаний, которыми располагают подразделения на местах. Эта взаимовыгодная модель совместных расследований была и остается частью стратегии, реализуемой отечественными правоохранительными органами. Совместные расследования помогают следователям принимать адекватные решения о том, выдвигать ли обвинения на федеральном уровне или на региональном уровне. Это обеспечивает правосудию максимальную гибкость и означает, что изобличенным в совершении преступлений будет назначено максимальное наказание за свои действия. Имеющиеся статистические данные отрезвляющим образом демонстрирует грандиозность проблем, стоящих перед всей правоохранительной системой.

По данным МВД России, в январе — августе 2024 года зарегистрировано 500,4 тысячи преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере

компьютерной информации. Это на 16,4% больше, чем за тот же период 2023 года [3].

Стратегия при проведении расследований должна объединяет основные усилия на идентификацию и определение местоположения жертв. Такой подход, при котором в центре внимания находится жертва, неизбежно приводит к одновременной идентификации преступника к его задержанию. В результате удается выявить и спасти детей и подростков, подвергавшихся сексуальной эксплуатации.

По данным Генеральной прокуратуры Российской Федерации, за период 2023 и 2024 годов зафиксировано более тысячи преступлений**,** совершённых с применением цифровых технологий против детей, а также выявлено почти четыре тысячи случаев производства детской порнографии [2]. По мере развития технологий хранения информации объемы данных будут расти, последовательно развиваются новые и инновационные способы решения стоящих перед правоохранительными органами. В частности, речь идет об автоматизации и внедрении новых технологий для ускорения процесса просеивания и анализа информации с целью выявления жертв, а, следовательно, и преступников. Активно внедряются в практику средства оценки биометрической информации и другие самые современные технические новинки.

Правоохранительные органы должны наращивать свои усилия, чтобы свести к минимуму ущерб, наносимый жертвам. Нелегальная торговля наркотиками, услуги на сайтах, многие из которых находятся в офшорах, осуществляется в открытом виртуальном пространстве, что создает огромные сложности. Поиск лиц, осуществляющих перемещение лиц, совершающих сексуальное насилие над детьми, распространение материалов, связанных с эксплуатацией детей, дистанционное мошенничество в Интернете, остается главной задачей лиц, осуществляющих расследование.

Список цитируемой литературы

1. Голубовский, В. Ю. Правовые и процессуальные аспекты противодействия преступлениям в сфере информационной безопасности / В. Ю. Голубовский // Пенитенциарная система и общество: опыт взаимодействия : Сборник материалов XI Международной научно-практической конференции, посвященной 145-летию уголовно-исполнительной системы Российской Федерации, Пермь, 03–05 апреля 2024 года. – Пермь: Пермский институт Федеральной службы исполнения наказаний, 2024. – С. 121-125.

2. Генпрокуратура: выявила рост IT-преступлений против детей в 2023-2024 годах [Электронный ресурс]. – Ридус: интернет – издание. –

URL: https://www.ridus.ru/genprokuratura--vyyavila-rost-it-prestuplenij-protiv-detej-v-2023-2024-godah-479276.html (дата обращения: 13.01.2025).
3. За пять лет число киберпреступлений увеличилось более чем вдвое [Электронный ресурс]. – Российская газета. – URL: https://rg.ru/2024/09/25/policiia-v-seti.html?ysclid=m5w2frxa2452100789 (дата обращения: 14.01.2025).

Левашова О.В., канд. юрид. наук, доцент, доцент кафедры
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Проблемы и перспективы совершенствования норм уголовного законодательства о кибербезопасности

Аннотация

Посредством интеграционных процессов, происходящих в обществе, внедряется всё больше новых технологий, зачастую не урегулированных в правовом смысле. Законы Российской Федерации, которые регулируют данную сферу, недостаточно разработаны, вследствие чего усложняется возможность предупреждения киберпреступлений. В статье рассматриваются проблемы применения норм уголовного законодательства в сфере кибербезопасности и выработка обоснованных предложений по совершенствованию и повышению эффективности уголовного законодательства об ответственности за отдельные виды таких деяний и практики их применения.

Ключевые слова: уголовное право. Уголовный кодекс РФ, кибербезопасность, ответственность, профилактика.

Достижения научно-технического прогресса позволило современному обществу удовлетворить массу потребностей благодаря технологиям, открывающим возможности расширения собственных возможностей. Техническое развитие открыло доступ к устройству возможностей эффективного построения критических инфраструктурных систем, направленных на более качественную реализацию социальных институтов. Однако такое повсеместное распространение информационных систем, открывает возможности помимо извлечения пользы, осуществлять незаконные действия злоумышленников более разрушительно. В связи с чем, развитие современных технологий требует эффективных моделей уголовно-правовой охраны. Принятые законодателем уголовно-правовые «устарели», поскольку отечественное уго-

ловное законодательство не успевает за расширением информационного поля и динамичным развитием информационных технологий.

Следует заметить, что современное российское законодательство не в полной мере успевает за стремительным развитием информационного пространства, в связи с чем нормативное регулирование кибербезопасности является недостаточно разработанным. Специфика современной киберпреступности состоит в том, что отдельно взятое государство не может противостоять данному феномену в силу транснационального и трансграничного характера рассматриваемого явления.

«Существенным недостатком действующего российского уголовного закона является несоответствие терминологии ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ современному состоянию науки и техники, которое вызвано целым рядом причин. Справедливым в этой связи видится мнение Н. Ф. Кузнецовой о том, что в уголовном праве юридическая междисциплинарность и метасистемность, т. е. взаимодействие с другими отраслями науки, разработаны недостаточно» [2, С 232]. Автором настоящего исследования обосновывается в той же степени необходимость достижения гармонизации терминологии УК РФ с точки зрения смежных наук с целью приведения их в единообразную форму понимания.

Считаем правильным рассмотреть следующие проблемы и несоответствия законодательного регулирования:

С точки зрения законодательного конструирования нормы ст. 272 УК РФ неправомерный доступ субъекта преступления направлено на исключительно к охраняемой компьютерной информации. Однако по смыслу, заложенному при конструировании ст. 272 УК РФ неправомерность доступа может быть направлено кроме компьютерных систем на информационные системы спутниковой связи, радиорелейной связи, систем мобильной связи или технического оборудования иного доступа. Считаем не совсем корректным использования определения, закрепленного в примечании, хотя и довольного объемного, но все же ограниченного компьютерными системами определения.

Решая данную проблему, обосновывается необходимость более общего понятия устройств, систем, а также сетей взаимодействия цифровой информации. Также предлагается дать классификацию и дифференциацию цифровой информации с точки зрения ее продуцирования в информационных системах.

Считаем, что уголовным законом РФ недостаточно уделено внимания деяниям по перехвату цифровой информации. Считаем такое упущение недопустимым, поскольку не охватывает уголовно-правовой охраной крайне важные общественные отношения.

«Отмечается, что в ст. 272 Неправомерный доступ к компьютерной информации УК РФ необходимо предусмотреть дополнительные квалифицирующие признаки, которые бы предусматривали дифференциацию способа получения доступа к компьютерной информации» [3, С. 104].

Сложившаяся теоретической и практической действительности трактует способ совершения преступлений в сфере компьютерной информации как неправомерное получение доступа к компьютерной информации.

Термин неправомерного доступа с точки зрения диспозиции ст. 272 УК РФ не должен быть единственным и ограничивающимся с точки зрения способа совершения и цели преступления. Развитие современных технологий позволило получить доступ к наиболее различным системам, в связи с чем расширяется способ совершения преступлений. Также расширяется и сфера возможного преступного технологического воздействия, например, на системы спутниковой связи, радиосистем, благодаря перехвата информации в которых осуществляется неправомерное получение доступа.

Ключевым отличием процедуры перехвата информации от иных форм неправомерного доступа. При этом важно подчеркивать, что в случае цифровой информации доступ может быть получаться посредством в том числе электромагнитного перехвата, неправомерный доступ к информации в нашем случае законодательством ограничивается информационно-телекоммуникационным системам.

Данные преступления с точки зрения объекта преступления характеризуются предметом в виде цифровой информации, нормативными источниками которой установлен режим правовой охраны.

Анализ современных теоретических и практических положений позволяет сказать, что программы разработки вредоносных систем на современном этапе позволяют получить доступ помимо к компьютерным системам еще и доступ к средствам связи. Получить доступ к Wifi сети как направление вреда злоумышленников является с той же степени распространенным, как и само по себе получение неправомерного доступа к информации.

Главным функцией получения информации с использованием перехвата информации является возможность достижения преступного результата высоколатентным способом.

Преступный результат, выраженный перехватом цифровой информации, достигается субъектами преступления посредством следующего набора действий:

– анализ средств беспроводной коммуникации с целью обнаружения объекта осуществляемой атаки (цифровой информации);

– осуществление мероприятий по взаимодействию с обнаруженной цифровой информации и ее последующая фиксация;

– процесс дешифрования, как правило с использованием специальных технических средств, полученной информации с последующей обработкой информации в наиболее удобной для интерпретации формы;

Ключевым видом перехват информации является в контексте объективных ситуаций судебно-следственной практики – электромагнитный перехват, направленный на получение несанкционированного доступа в недвижимых помещениях к информационным системам. Такой вид перехвата дает возможность получения непрямого доступа к цифровым устройствам посредством перехвата электромагнитного излучения, являющегося функциональной особенностью работы устройств.

При этом важно упомянуть возможность легального перехвата цифровой информации, распространяемой в формате радиоконтроля. Согласно законодательству ФЗ «О связи» уполномоченные органы государственной власти могут осуществлять запись источников распространения радиоэлектронных устройств для фиксации доказательств нарушения режима и порядка использования режима радиообмена. Использование таких записей с точки зрения закона не допустимо иным образом кроме как с целями, описанными в законе. Лица распространившие такие сведения подлежат уголовной ответственности в соответствии с уголовным законом, как распространении тайны, охраняемой законом.

Незаконный перехват информации возможен не только в каких-либо ограниченных системах, но и наиболее распространенных – мобильной системы связи. В частности, на одной из самых распространенных конференциях специалистов по компьютерной безопасности Chaos Communication Congress представлена технология получения неправомерного доступа к информационным системам, в частности, к мобильному телефону. Смысл такого криптографического воздействия направлялось на перехват радиосигналов между устройством и базовой станции сотового оператора. Взаимодействие посредством предотвращения передачи сигналов радиочастот в 80 спектре каналов.

В соответствии с вышесказанным с точки зрения сравнения уровня общественной опасности, вред, причиняемый общественным отношениям в результате неправомерного доступа к цифровой информации соразмерен с опасностью получения незаконного доступа к перехватам такой информации, в том числе распространяемой с использованием иных средств передачи информации.

В примечании 2 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «перехват цифровой информации» в следующей редакции:

Информационный перехват при необходимости можно определить посредством смежных источников информации, технической литературой, и специальными нормативными источниками. В широком смысле это действия, с помощью которых достигается несанкционированное получение информации в момент передачи процесса коммуникации. Информация получается не в результате взаимодействия с конечным устройством, а в результате взаимодействия с каналом коммуникации.

Обязательным признаком объективной стороны преступления, предусмотренного ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, являются последствия в виде уничтожения, блокирования, модификации либо копирования информации.

Это означает, что, несмотря на то что доступ к компьютерной информации может быть неправомерным, если он не повлек за собой перечисленных в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ последствий, он не может считаться преступлением.

В связи с этим обнаруживается не способность уголовного закона регулировать смежные деяния, при которых неправомерный доступ к информации получается не в следствии активных действий, а посредством случайных актов получения, например вследствие наблюдения экрана компьютера несанкционированный образом, в следствие халатности или нарушений правил охраны информации. Такое деяние помимо прочего, предоставляет возможность причинение большого ущерба владельцу информации, поскольку не исключает комплекс неправомерных взаимодействий.

«Неправомерный доступ к компьютерной информации УК РФ в виде ознакомления с информацией исследовались двумя учеными: В. Н. Щепетильниковым и С. А. Яшковым. В. Н. Щепетильников справедливо указал, что незаконный доступ к компьютерной информации включает в себя ознакомление с ней [8, С. 6]. В свою очередь, С. А. Яшков считает необходимым включить в УК РФ деяние, повлекшее полное либо частичное ознакомление с компьютерной информацией» [9, С. 8].

С точки зрения авторов настоящей работы, нормативные положения ч. 1 ст. 272 У РФ не устанавливает необходимого режима уголовно-правовой охраны несанкционированного и неправомерного ознакомления с цифровой информации, что недопустимо с точки зрения достижения целей уголовного закона. Незаконное ознакомление с цифровой информации может позволить субъекту получить возможность использо-

вания полученной не несанкционированным образом информации в личных целях, причиняя вред обладателю такой информации.

«Поддерживая позицию С. А. Яшкова и учитывая, что ч. 1 ст. 272 Неправомерный доступ к компьютерной информации УК РФ не содержит указания на такой способ преступления, как ознакомление с цифровой информацией, предлагаем дополнить данную норму словом ознакомление» [9, С. 21].

Ключевой проблемой законодательного конструирования ст. 272 УК РФ наблюдается противоречивость упоминаемых терминов в нормативных источниках и терминологического аппарата научно-технической документации, регулирующих вопросы технической сущности. Противоречивость терминов порождают ошибки в понимания одной и той же ситуации, что в точки зрения эффективности реализации уголовного права недопустимо.

Для этого следует обратиться к основному закону, регулирующему отношения в сфере информации. Ст. 15 «Использование информационно-телекоммуникационных сетей» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» говорит об использовании информационно-телекоммуникационных сетей на территории Российской Федерации [1].

Полагаем такую дефиницию ограничения сферы взаимодействия цифровой информации подходящим, поскольку оно отвечает требованиям современности к единообразию терминологического аппарата нормативного регулирования.

Теоретик С.П. Кушниренко расширяет возможность использования дефиниции информационно-коммуникационных технологий, применяющиеся наиболее часто в информационной сфере как наиболее базовым. В рамках данного понятия понимаются средства технологий, позволяющих реализовывать механизм взаимодействия с информацией [4, С. 43].

В ч. 2 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ указаны такие квалифицирующие признаки, как причинение деянием крупного ущерба или совершение его из корыстной заинтересованности. Причем законодатель определил, что крупным признается ущерб, сумма которого превышает один миллион рублей.

Считаем такую тенденцию в конструировании нормы уголовного закона отвечающим общей направленности на дифференциацию уголовного закона. Однако разработка размера в тех определенных пределах, закрепленных настоящей редакцией закона, не позволяют дать

возможность достаточной степени охраны. Ущерб в несколько десяток или сотен тысяч рублей для разных участников экономического оборота может нанести совершенно различный урон. В связи с этим считаем разрешить данную проблему либо внесением суммы в сто тысяч рублей в размер крупного ущерба, либо разработку оценочных критериев ущерба, не являющегося устойчивой единицей.

Считаем также возможным внести в действующие редакции компьютерных преступлений ряд квалифицирующих признаков, позволяющих дифференцировать уголовную ответственность по признакам совершения преступлений из хулиганских побуждений, с использованием специальных технических средств, специально разработанных для получения цифровой информации. Такой набор квалифицирующих признаков наиболее пригоден для действующей ситуации компьютерных преступлений.

Уголовным кодексом в части диспозиции ч. 4 ст. 272 УК РФ подразумевается уголовная ответственность за материальный признак вреда в виде преступных последствий. Однако указывается на необходимость хотя бы частичного перечисления перечня альтернативных действий что облегчило бы практическую процедуру применения данного уголовного закона. Считаем также необходимым отнесения к тяжким последствиям причинения вреда здоровью при совершении преступления.

С точки зрения статистической характеристики применения ст. 272 УК РФ наиболее частым составляет корпус преступлений, выраженных кражей данных для получения доступа к сети Интернет. Альтернативные варианты преступлений – приходятся на случае получения доступов для неправомерного завладения информации.

«Так, Трусовским районным судом г. Астрахани вынесен приговор по обвинению гр. Ш. в совершении преступления, предусмотренного ч. 1 ст. 272 Неправомерный доступ к компьютерной информации УК РФ. Суд установил, что гр. Ш. совершал незаконный доступ к компьютерной информации с целью получения бесплатных услуг по доступу к сети Интернет. Так, гр. Ш. через сервер провайдера путем вышеуказанных подключений и внесения учетных записей посредством пароля и логина, принадлежащих гр. М., неправомерно подключился к серверу провайдера для выхода в сеть Интернет и к информации, хранящейся в указанной сети» [6].

С целью закрытия пробела в регулировании процедуры перехвата информации, в связи с повышенной общественной опасностью как получения неправомерного доступа, так и перехвата цифровой информации. В связи с чем в действующую редакцию УК РФ предлагается

включить новые редакции ст. 272 УК РФ в диспозицию ч. 1 следующего содержания.

«Статья 272. Неправомерный доступ к охраняемой законом цифровой информации или ее перехват

1. Неправомерный доступ к охраняемой законом цифровой информации, а равно незаконный ее перехват, если это деяние повлекло уничтожение, блокирование, модификацию, копирование цифровой информации либо ознакомление с ней, нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, – наказывается…».

Научно-технический прогресс привнес в современный мир крайне разнообразные способы цифрового и информационного взаимодействия. Все больше информационно-телекоммуникационных сетей задействованы в поддержании критических систем функционирования государства. В связи с чем, крайне актуальным является как можно более своевременные коррекции действующих норм уголовного закона с целью предотвращения последствий преступной активности злоумышленников.

Рассматриваемая норма является бланкетной и отсылает, как правило, к нормативно-правовым актам, инструкциям и правилам, устанавливающим требования к средствам хранения, обработки или передачи компьютерной информации, так как компьютерные технологии используются в различных сферах деятельности человека, то указанные правила должны быть как унифицированными, так и учитывающими особенности этих сфер.

С точки зрения характеристики вопросы о хранении компьютерной информации как совокупность инструментов взаимодействия с информацией, выраженных размещением их на каких-либо материальных носителях, например, в персональном компьютере, или иных формах материального носителя. В данном случае верным с точки зрения достижения целей уголовного закона было бы указание данного перечня альтернативных действий в ст. 274 УК РФ как нарушения правил эксплуатаций систем и технологий, а не более узкое понятие, действующее в данный момент.

Механизмы государственного правового регулирования понятий Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предлагает определенный перечень дефиниций, позволяющих установить нормативную границу понимания информационных и информационно-телекоммуникационных сетей.

Термин «информационные-телекоммуникационные устройства их системы и сети», определяемый специальными нормативно-правовыми актами вошел в правовой оборот и используется научным аппаратом в качестве единого и наиболее принятого определения в различных смежных науках.

Необходимо подчеркнуть в данный момент важность выводов теоретика В.С. Соловьева, подчеркивающего необходимость приведения положений уголовного кодекса к единой системной формулировки терминов и дефиниций диспозиций, характеризующие системность информационно-телекоммуникационных сетей.

Рассматривая профилактические меры компьютерной преступности, можно отметить следующее. В соответствии со ст. 13 Международного пакта об экономических, социальных и культурных правах международное сообщество признает право каждого человека на образование. Данный принцип является основополагающим в процессе ресоциализации, так как должен быть положен в основу социальной адаптации в период освобождения из мест принудительного содержания [7, С. 56].

Современные модели законодательств, в основе которых отражены международные принципы, в соответствии с которыми лица, совершившие преступление могут быть лишены свободы, т.е. в некоторой степени ограничены на период исполнения наказания, но индивидуальные права не могут быть ограничены даже в период отбывания наказания, ч. 1 ст. 26 Всеобщей декларации прав человека, ст. 2 Протокола № 1 к европейской Конвенции о защите прав человека и основных свобод, ст. 14 Хартии Европейского Союза об основных правах.

Образование в МПС, отраженная в Международном пакте об экономических, социальных и культурных правах является неотъемлемым правом, но также и стимулом к УДО.

Национальная система уголовного наказания в образовании следуя из анализа итогов ФСИН России, в соответствии со ст. 43 Конституции Российской Федерации, каждый имеет право на образование, является эффективной мерой ресоциализации.

Рекомендации и методические пособия о реализации данного права на практике отражены в Федеральном законе от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Уголовно-исполнительным кодексом Российской Федерации, а также иными нормативными правовыми актами, содержащими нормы.

Гуманизм как философское понятие, стал основным принципом демократии, а это предоставило возможность человеку обрести права и посредством прав, реализовывать свои интересы. Данные права декларированы основным НПА действующей Конституцией РФ и гаранти-

рованы их защитой на государственном уровне. Следует добавить, что права несколько шире у гражданина, чем у человека, а если учитывать тот факт, что осужденного нельзя лишить гражданство в период исполнения наказания, то говорить можно исключительно об ограничении некоторых прав.

Самая большая нерешенная проблема мировой пенитенциарной педагогики является вопрос рецидивной преступности, не осталась в стороне, и наша страна по открытым данным ФСИН РФ совершение повторных преступлений лицами, имеющими предыдущий срок составляет более 60%.

Причин тому множество, но одна из основных, состоит в некачественной работе, которая строится на нерегулярной, разовой работе с освободившимися в период их социальной адаптации на воле.

Основополагающие документы разработаны и приняты после их утверждения на международных пенитенциарных Конгрессах и включены в Рекомендации Евросоюза «Об образовании в тюрьмах».

Данные рекомендации указывают, что основу должны составлять:

- общая доступность и обеспечение осужденному поддержки;
- обеспечение полного комплекса программного и технического обеспечения;
- получение не только образования по профессии, но главное приобщение к мировым достижениям науки, культуры, общества;
- снижение и компенсации денежных средств в образовательной сфере;
- подбор качественного состава преподавателей для работы со спецконтингентом;
- обеспечить получение образования и соответствующей профессии, наиболее востребованной в современных условиях труда и региональной направленности.

Важно не поливать грязью ФСИН РФ, необходимо создать условия, которые бы стимулировали сотрудников на качественное выполнение своих профессиональных задач, для этого необходимо провести реформирование кадровой политики при работе с кандидатами. Повысить престиж службы для тех, кто проходит службу в настоящий момент, а также выстроить механизм хорошего пенсионного обеспечения ветеранам службы, например, предоставления путевок в пансионаты и другие формы социального обеспечения.

Что касается условий содержания осужденных, то сегодня исходя из докладов они улучшаются с каждым годом, если провести анализ жалоб осужденных за прошлый период, то происходит ежегодное уменьшение обращения осужденных на питание, также уменьшаются жалобы

на социальное обеспечение, возможность пользоваться душем и прочие социально-бытовые условия. Однако, при общем снижении обращений-жалоб, количество их на медицинское обслуживание не только не снижается, а наоборот увеличивается, примером может служить нехватка медицинских работников в целом, а узких специалистов критически.

Но существует сфера, где права осужденного не ограничены даже в условиях изоляции от общества, данная область получения образования.

Таким образом, права осужденных в этом вопросе не ограничиваются, даже более того с каждым годом данная сфера расширяется, сегодня осужденный может получить не только профессию, но и диплом о высшем образовании.

А вот применить полученную профессию, чтобы был опыт работы, который даст шанс устроится на работу после освобождения невелик.

Например, в любом пенитенциарном учреждении работает ПТУ (профессионально-техническое училище), где можно получить профессии по самым востребованным на сегодня профессиям, например, электрик, каменщик, столяр, плотник, автомеханик, слесарь-сантехник.

Однако, при столь обширном перечне заявленных профессий, осужденные выбирают самые на наш взгляд самые не востребование, например, стропальщик. Если в обычной жизни на гражданке по профессии «стропальщик» найти работу можно, то в условиях исполнительной колонии проблематично. Вопрос, как получить опыт работы по специальности в условиях изоляции.

Другой вопрос, который необходимо решать, состоит в том, что получение высшего образования предусматривает удаленную формат, т.е. система дистанционного обучения. Когда студент получает задание, выполняет его и отсылает на проверку, для этого необходимо оборудование, компьютер и доступ к сети «Интернет». Если мегаполисы не имеют проблемы с устойчивой работы сети «Интернет», но пенитенциарные учреждения существуют в регионах, где «Интернет» слабый, что не дает возможность качественной связи, что делать, необходимо проводить оптоволокно.

Хороший результат, который стал показателем эффективной работы с осужденными по итогам года, что каждое исправительное учреждение имеет возможность обучать осужденных по всем видам образования.

Также можно констатировать снижение количества поданных обращений на нарушение прав, осужденных в сфере получения образования.

При этом необходимо акцентировать внимание, что было указано в нашем исследовании – это снижение стремления получить как про-

фессию, кроме указанной «стропальщик» или «повар», так и высшего образования.

Но не менее важной стороной учебного процесса является педагогические кадры, которые по достижению пенсионного возраста уходят на пенсию, а пополнение молодых учителей в пенитенциарной нет.

Если сотрудников для ФСИН РФ готовят специализированные учебные заведения, то педагогический состав в них не обучается.

Таким образом, образование как один из основных принципов ресоциализации осужденных находится в трудном положении, что необходимо сделать, чтобы вывести данный институт из крена?

Приводить работу в соответствие с требованиями законодательных актов, региональной потребности в кадрах, поднимать престиж рабочего человека и т.д. В исправительных учреждениях необходимо создавать рабочие места, где, получив профессию, осужденным мог получить опыт, навыки полученных знаний [5, С. 202].

Для более качественной работы в сфере получения образования в местах принудительного содержания, сегодня необходимо перестроить модель, которая должна соответствовать достижениям НТР на принципах работы искусственного интеллекта, чтобы после освобождения человек не попадал в среду, которая бы отторгала его, т.к. он её не знает.

Значит не стоит боятся новых компьютерных технологий, тем более что пока осужденные каким-то образом имеют «сотовые» телефоны, которые запрещены для спецконтингента. Необходимо принимать меры для строгого учета времени работы на компьютере, что не так сложно сделать в условиях изоляции и постоянного контроля.

Список цитируемой литературы:

1. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ (в ред. от 23 ноября 2024 г.) // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ч. I. – Ст. 3448.

2. Бессонов, В.А. История и зарубежный опыт правовой регламентации компьютерной преступности / В.А. Бессонов// Территория науки. – 2013. – № 2. – С. 231–237.

3. Денисов, Н. Л. Несоответствие современным реалиям существующей уголовной ответственности за неправомерный доступ к компьютерной информации / Н.Л. Денисов // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов межвуз. науч.-практ. конф., 19 апреля 2018 г. – Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018. – С. 104–107.

4. Кушниренко, С. П. Цифровая информация как самостоятельный объект криминалистического исследования /С.П. Кушниренко // Вестник криминалистики. – 2006. – №4. –С. 43–47.
5. Морозов, А. В. Профессионально-техническое обучение осужденных в зарубежных странах и его значение для их социальной адаптации и ресоциализации / А.В. Морозов// Вестник Владимирского юридического института. – 2009. – № 4. – С. 202.
6.Приговор Кировского районного суда г. Саратова от 22 июня 2012 г. по уголовному делу № 1–168/2011. [Электронный ресурс] – Судебные и нормативные акты РФ. – URL: https:// https://sudact.ru (дата обращения: 23.12.2024).
7. Уголовно-исполнительное право: учебник для вузов / под ред. И.Я. Козаченко, А.П. Деткова. 2–е изд. – М.: Юрайт, – 2022. – 476 с.
8.Щепетильников, В. Н. Уголовно-правовая охрана электронной информации: автореф. дисс. … канд. юрид. наук /В.Н. Щепетильников. – Рязань, 2006. – 24 с.
9. Яшков, С. А. Информация как объект преступления: дисс. … канд. юрид. наук / С.А Яшков. – Екатеринбург, 2005. – 203 с.

Матвеев А.В., канд. юрид. наук, преподаватель
ФГКОУ ВО «Санкт-Петербургский университет МВД России»
Ленинградский областной филиал, п. Мурино

Роль органов внутренних дел Российской Федерации в противодействии киберпреступности

Аннотация

Статья посвящена роли органов внутренних дел Российской Федерации в противодействии киберпреступности. Определена отличительная особенность киберпреступлений от иных видов преступлений. Проанализированы статистические данные, позволяющие оценить вклад органов внутренних дел Российской Федерации в борьбу с киберпреступлениями. Сделан вывод о мерах, необходимых к принятию в целях повышения уровня раскрываемости киберпреступлений.

Ключевые слова: преступление; киберпреступление; информационно-коммуникационные технологии; правоохранительная система; правоохранительные органы; органы внутренних дел; кибербезопасность; оперативно-розыскная деятельность.

В последние годы информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех

сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности является повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям [3].

Об актуальности исследования вопросов противодействия преступлениям, совершаемым с использованием информационных технологий (далее – киберпреступления, киберпреступность), красноречиво свидетельствует статистика. Согласно характеристике состояния преступности в Российской Федерации за январь – декабрь 2023 года, в Российской Федерации за указанный период зарегистрировано 677,0 тысяч киберпреступлений, что на 29,7% больше, чем за аналогичный период 2022 года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5% в январе – декабре 2022 года до 34,8% [6]. За 10 месяцев 2024 года почти 60% в общем количестве тяжких и особо тяжких преступлений составили киберпреступления. Общее число зарегистрированных рассматриваемых преступлений возросло на 14,6% по сравнению с 10 месяцами 2023 года [7]. Приведенные данные свидетельствуют о высоких темпах роста киберпреступлений, и об острой необходимости противодействия им со стороны правоохранительных органов.

Исследуя вопросы противодействия киберпреступности, следует отметить, что само понятие киберпреступления на сегодняшний день нормативного закрепления не получило. Различные подходы к формулировке определения киберпреступления предложены исследователями данной проблематики. По мнению П. А. Пикалова, под киберпреступлением следует понимать противоправные действия, совершаемые с использованием информационно-телекоммуникационных сетей или средств автоматизации, которые направлены на незаконное проникновение в информационную систему, хищение, уничтожение, блокирование, изменение или копирование данных, а также нарушение норм функционирования информационных систем или создание программного обеспечения для совершения таких действий [10, С. 106]. С. В. Тимофеев и Р. Р. Абидов под киберпреступлением понимают уголовно наказуемое деяние, где предметом и (или) средством совершения преступления являются цифровые технологии [11, С. 295].

К. Н. Евдокимов в своем исследовании приходит к выводу о том, что понятие «киберпреступление» применимо к совокупности компьютерных преступлений, совершенных в пространстве информационно-телекоммуникационных сетей, либо с использованием информационно-телекоммуникационных сетей, в сети «Интернет», для достижения преступных целей [5, с. 23–24]. Таким образом, в качестве отличительной особенности киберпреступлений следует выделить использование информационных технологий при их совершении.

Уголовным кодексом Российской Федерации киберпреступления в отдельную категорию не выделены, однако, учитывая вышеуказанную отличительную особенность, в структуру киберпреступлений следует включить: преступления против жизни и здоровья (статьи 110, 110.1, 110.2, 119), преступления против свободы, чести и достоинства личности (статья 128.1), преступления против половой неприкосновенности и половой свободы личности (статьи 133, 135), преступления против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 146), преступления против семьи и несовершеннолетних (статьи 150, 151, 151.2), преступления против собственности (статьи 158, 159, 159.3, 159.6, 163), преступления в сфере экономической деятельности (статьи 171.2, 174, 174.1, 183, 185.3, 186, 187), преступления против общественной безопасности (статьи 205.1, 205.2, 207, 207.1, 207.2, 207.3, 210, ст. 222, 222.1, 222.2), преступления против здоровья населения и общественной нравственности (статьи 228, 228.1, 228.2, 228,3, 228.4, 229, 230, 234, 234.1, 238, 238.1, 240, 242.1, 242, 242.2, 245), преступления в сфере компьютерной информации (статьи 272, 272.1, 273, 274, 274.1, 274.2), преступления против основ конституционного строя и безопасности государства (статьи 283, 283.1, 284.2), преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления (статьи 288, 292), преступления против правосудия (статьи 296, 298.1, 311), преступления против порядка управления (статьи 327, 327.1), преступления против мира и безопасности человечества (статьи 354, 354.1) [1].

Согласно статистическим данным, наиболее распространенными киберпреступлениями на сегодняшний день являются кража и мошенничество. В 2023 году среди правоохранительных органов наибольшее количество киберпреступлений раскрыто органами внутренних дел Российской Федерации (далее – органы внутренних дел) – 149 933 киберпреступления. Следственными органами Следственного комитета Российской Федерации раскрыто 20 645 киберпреступлений, органами Федеральной службы безопасности – 1 298 киберпреступлений [6]. Приведенные данные свидетельствуют о существенном вкладе органов внутренних

дел Российской Федерации в противодействие киберпреступлениям и в обеспечении кибербезопасности Российской Федерации в целом [9, С. 41].

Согласно статье 13 Федерального закона «Об оперативно-розыскной деятельности» [2] (далее – Федеральный закон об ОРД), оперативным подразделениям органов внутренних дел предоставлено право на осуществление оперативно-розыскной деятельности на территории Российской Федерации. Статья 3 Федерального закона об ОРД устанавливает в качестве задачи оперативно-розыскной деятельности выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших [2]. Таким образом, учитывая статистику раскрытых киберпреступлений, а также полномочия, возложенные на органы внутренних дел положениями действующего законодательства, именно органы внутренних дел «принимают на себя основной удар» в борьбе с киберпреступлениями посредством осуществления оперативно-розыскной деятельности.

В целях реализации возложенных на органы внутренних дел полномочий по противодействию киберпреступлениям, в 2022 году в структуре Министерства внутренних дел Российской Федерации создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России), которое призвано организовывать противодействие противоправным деяниям, совершаемым с использованием (в сфере) информационно-коммуникационных технологий, в том числе путем осуществления оперативно-розыскной деятельности [4].

Несмотря на принимаемые в настоящее время органами внутренних дел правовые и организационные меры по противодействию стремительно развивающейся киберпреступности, раскрываемость киберпреступлений составляет 26% [6], что является низким показателем. В качестве причин низкого уровня раскрываемости киберпреступлений выделяется недостаточность технического и технологического обеспечения органов внутренних дел, а также отсутствие у сотрудников органов внутренних дел необходимой для эффективного раскрытия киберпреступлений квалификации и опыта [8, с. 112].

Таким образом, с учетом изложенного, следует сделать вывод о том, что органы внутренних дел играют ключевую роль в противодействии киберпреступности в Российской Федерации, однако, имеющиеся проблемы раскрытия киберпреступлений свидетельствуют о необходимости принятия дополнительных мер по повышению уровня технического и технологического обеспечения органов внутренних дел, а

также по совершенствованию системы подготовки кадров органов внутренних дел и повышению их квалификации.

Список цитируемой литературы:

1. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 13 декабря 2024 г.) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
2. Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ (в ред. от 29 декабря 2022 г.) // Собрание законодательства Российской Федерации. – 1995. – № 33. Ст. 3349.
3. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Рос. Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.
4. Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: приказ Министерства внутренних дел Рос. Федерации от 29 декабря 2022 г. № 1110 [Электронный ресурс]. – Справочно-правовая система «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_439373/1ed25cd98138eb129996818fe8e19b784078aa6a/?ysclid=m4zl6j185n111777265 (дата обращения: 06.01.2025).
5. Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореф. дисс. … док. юрид. наук. – Москва, 2022. – 73 с.
6. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. [Электронный ресурс]. – Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 06.01.2025).
7. Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2024 года [Электронный ресурс]. – Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф/reports/item/57279296/ (дата обращения: 06.01.2025).
8. Михайлова, И.А., Лимарь, А.С., Гилаев, Р.И. О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий/ И.А. Михайлова, А.С. Лимарь, Р.И. Гилаев // Вестник экономики, права и социологии. – 2024. – № 2. – С. 109–114.

9. Осипенко, А. Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации / А.Л. Осипенко // Общество и право. – 2018. – № 3(65). – С. 35–43.
10. Пикалов, П. А. Криминализация незаконных действий в цифровой среде в Российской Федерации: теория и практика / П.А. Пикалов // Совершенствование науки и образования в новых реалиях: Сборник статей XI Всероссийской научно-практической конференции для преподавателей, аспирантов, магистрантов и студентов. г. Москва, 29 февраля 2024 года. – Москва: Общество с ограниченной ответственностью «РОСТПОЛИГРАФ», 2024. – С. 105–110.
11. Тимофеев, С.В., Абидов, Р. Р. Проблемы противодействия киберпреступности: вопросы теории и практики / С.В. Тимофеев, Р.Р. Абидов // Вестник Восточно-Сибирского института МВД России. – 2024. – № 1(108). – С. 292–300.

Пестрецов И.О., аспирант
ФГКОУ ВО «Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева»,
лейтенант юстиции, г. Москва

СПОСОБ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ ПРЕКРАЩЕНИЯ УГОЛОВНОГО ДЕЛА И УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ В ОТНОШЕНИИ УЧАСТНИКА СВО

Аннотация

В статье рассматривается влияние законодательной новеллы по модификации института прекращения уголовного дела и уголовного преследования в отношении участников специальной военной операции на противодействие киберпреступности. Выявляются возможные способы борьбы с киберпреступностью после возвращения участников СВО.

Ключевые слова: киберпреступность, специальная военная операция, институт прекращения уголовного дела (уголовного преследования).

Цифровые технологии, как неотъемлемая часть жизни современного общества, подтолкнули к модификации социальных отношений, а вместе с тем к модификации способа совершения преступлений. Так, в эпоху глобализации общество постоянно сталкивается с таким термином как «киберпреступность».

Термин «Киберпреступность» официально в нормативных нормах не закреплен, вместе с тем, исходя из правовой практики под киберпре-

ступностью пониманиются те противоправные деяния, которые направлены против целостности, тайны компьютерной и цифровой информации и доступности сетей. Иными словами, это те противоправные деяния, которые направлены на неправомерный сбор, хранение и распоряжение информации, полученной посредством IT-технологий.

Если обратить внимание на статистику, то можно заметить, что в период с 2013 по 2020 гг. киберпреступность в России выросла в 20-ти кратном размере [4, С. 212-217], что за собой повлекло значительный ущерб, как для граждан, так и для банковского сектора экономики. По данным Банка России в 2019 году злоумышленники, путем злоупотребеления доверием, похитили порядка 6,4 млрд. рублей у клиентов российских банков, а спустя год объем ущерба вырос до 9,77 млрд. рублей, что составило рост на 52 %, из которых всего 11,3% удалось возместить потерпевшим.

Такой неумолимый рост киберпреступности заставляет правоохранительные органы активизировать свою работу в области совершенствования оперативно-следственной практики раскрытия и борьбы с данными видами преступлений.

Однако, как должен действовать следователь в условиях совершеноствования уголовно-процессуального законодательства?

Уголовно-процессуальное законодательство РФ также претерпело ряд измений, были введены нормы, модифицирующие институт прекращения уголовного дела и уголовного преследования.

Так, УПК РФ дополнен статьей 28.2, согласно которой суд, а также следователь с согласия руководителя следственного органа или дознаватель с согласия прокурора прекращает уголовное преследование в отношении лица, подозреваемого или обвиняемого в совершении преступления, в отношении которого производство по уголовному делу было приостановлено по ходатайству командования воинской части (учреждения), при получении информации от уполномоченных органов о случаях, предусмотренных частью первой статьи 78.1 Уголовного кодекса Российской Федерации (далее по тексту – УК РФ) [2]. Данная норма является отсылочной, в связи с чем, раскроем сами случаи принятия такого решения.

Согласно ст. 78.1 УК РФ должностное лицо может принять решение о прекращении по ст. 28.2 УПК РФ при следующей конструкции:

1. Лицо совершило преступление, за исключением преступлений против половой неприкосновенности несовершеннолетних либо преступлений террористической направленности или против порядка управления;

2. Лицо призвано на военную службу в период мобилизации или в военное время в Вооруженные Силы Российской Федерации либо за-

ключило в период мобилизации, в период военного положения или в военное время контракт о прохождении военной службы в Вооруженных Силах Российской Федерации, либо лицо, совершившее преступление в период прохождения военной службы в Вооруженных Силах Российской Федерации в период мобилизации, в период военного положения или в военное время, в отношении которых производство по уголовному делу приостановлено по ходатайству командования воинской части (учреждения);

3. Лицо награждено государственной наградой, полученной в период прохождения военной службы или со дня увольнения с военной службы в связи с достижением предельного возраста пребывания на военной службе, по состоянию здоровья либо отмене оснований, подлежащих призыву лица в Вооруженные Силы Российской Федерации (отмена мобилизации, военного положения и др.) [1].

При этом в обязательном порядке следственными органами выясняется позиция стороны защиты, поскольку в случае не согласия подозреваемого и обвиняемого с таким решением органов предварительного расследования, то досудебное производство продолжается в обычном порядке.

Согласно вновь введенной норме процедура прекращения уголовного дела и уголовного преследования выглядит следующим образом: обращение с ходатайством в орган предварительного расследования либо в суд командования воинской части Вооруженных Сил Российской Федерации, принятие решения по существу ходатайства следователем, дознавателем либо судом, в случае удовлетворения ходатайства следователь, дознаватель либо судья принимает решение о приостановлении уголовного дела и уголовного преследования по основанию, предусмотренному п. 3.1 ст. 208 УПК РФ, то есть призыв подозреваемого или обвиняемого на военную службу в период мобилизации или в военное время в Вооруженные Силы Российской Федерации либо заключение ими в период мобилизации, в период военного положения или в военное время контракта о прохождении военной службы в Вооруженных Силах Российской Федерации, а также прохождение ими военной службы в Вооруженных Силах Российской Федерации в период мобилизации, в период военного положения или в военное время, по возвращению подозреваемого, обвиняемого или подсудимого к месту производства по уголовному делу принятие решения о прекращении уголовного дела и уголовного преследования в порядке, предусмотренным ст. 28.2 УПК РФ.

Данная законодательная новелла предусмотрела новое основание для освобождения от уголовной ответственности. При этом это норма фактически является директивной, то есть орган предварительного рас-

следования или суд, в случае заключения подозреваемого и обвинямого контракта с Вооруженными Силами Российской Федерации и при наличии оснований, предусмотренных ст. 78.1 УК РФ, прекращает уголовное дело и уголовное преследование. При этом, не смотря на реакцию правоохранительных органов в виде возбуждения уголовного дела и предварительного расследования, подозреваемые и обвиняемые могут продолжить совершение преступлений, в том числе в киберпространстве.

Вместе с тем, мер по соблюдению баланса интересов, в перечень которых входит публичные интересы государства на сохранение действующего правопорядка не принято. Мер по пресечению совершения преступлений в будущем участниками специальной военной операции не принято.

Фактически освобождая лиц от уголовной ответственности по анализируемой новелле, государства принимает на себя риск в виде возможного продолжения совершения преступлений. При этом резонно указать, что киберпреступления относятся к категории латентных и трансграничных преступлений. Преступники могут заниматься противоправной деятельностью на дальних расстояниях от места, где фактически наступили общественно-опасные последствия, где наносится реальный ущерб.

В Российской Федерации разработан ряд мер, позволяющих бороться с киберпреступностью, так модифицируется Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), AntiFraund-системы банковских организаций, которые позволяют распознавать подозрительные операции с банковским счетом и обеспчить временную блокировку банковского счета или операции, проводятся просветительские мероприятия об алгоритмах мошеннических операций и порядке действий в случае столкновения с ними, а также производится совершенствование российского законодательства для правильной квалификации данного типа правонарушений.

Вместе с тем, согласно данным судебной статистики в 2023 году за преступления, предусмотренные ст.ст. 159-159.6 УК РФ осуждено 27 483, для сравнения в 2022 – 23 738 лиц [5], то есть наблюдается увеличение осужденных лиц за мошенничество, в том числе совершенного с использованием информационных технологий на 15%. Это может свидетельствовать о том, что действующие меры не позволяют в полной мере справиться с киберпрестуностью. Резонно указать, что модификация института прекращения уголовного дела и уголовного преследования, позволяющая лицам уйти от уголовной ответственности, создает риск увеличения указанного показателя.

Вместе с тем, при разработке мер противодействия киберпреступности можно обратиться к опыту зарубежных коллег. Так, полиция Японии и США применяет практику привлечения «этичных» хакеров для борьбы с киберпреступностью в банковском секторе [3, С.1]. Полагаем, что данный способ успешен при условии того, что «этичные» хакеры привлекаются государством из преступной среды, что позволит фактически киберпреступности бороться с самой собой, поскольку бывшие киберпреступники, как никто, знают слабые места информационных технологий.

В целях поддержания тенденции к заключению контракта с Вооруженными Силами Российской Федерации для участия в военных действиях в зоне специальной военной операции законодатель разработал массу возможностей после возвращения с фронта – это и льготное обучение в образовательных организациях, и трудоустройство. Однако не факт, что киберпреступники воспользуются данными льготами и станут законопослушными гражданами.

На наш взгляд, в целях исключения возможного риска наиболее действенными мерами будут привлечение киберпреступников, в отношении которых уголовное дело прекращено по основанию, предусмотренному ст. 28.2 УПК РФ, к «этическому» хакерству, то есть таким образом переманить криминальный контингент в правоохранительную деятельность, также в обязательном порядке ставить всех на учет в системе МВД России для проведения профилактической работы, как предусмотренно приказом МВД России №1166 от 31.12.2012 «По организации деятельности участковых уполномоченных полиции». Резонно будет проводить работу с членами семьи киберпреступника, а также привлечь их к исправлению лица и вовлечение его в жизнь общества.

Таким образом, можно сделать вывод, что киберпреступность – это вид преступлений, совершенных с применением IT-технологий. В условиях модернизации процессуального законодательства, а именно введение новой дерективной нормы, направленной на прекращение уголовного дела и уголовного преследования, а вместе с тем освобождение лиц от уголовной ответственности создает ряд рисков для сохранения действующего правопорядка в обществе. В целях минимазации социальных рисков требуется совершенствование действующих и введение новых способов борьбы с киберпреступностью.

Список цитируемой литературы:

1. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 2 октября 2024 г.) // Со-

брание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. №174-ФЗ (в ред. от 2 октября 2024 г.) // Собрание законодательства Российской Федерации. – 2001. – № 52. – Часть. I. – Ст. 4921.
3. Коломыченко, М. В интернет ввели кибервойска / М. Коломыченко // Коммерсантъ. – 2017. – № 2. – 10 янв. [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/3187320 (дата обращения: 30.12.2024)
4. Приходько А. А., Керопян, Г. Б. Потери банков от киберпреступности. / А.А. Приходько, Г.Б. Керопян // StudNet. – 2020. – Т. 3. – № 12. – С. 212–217.
5. Судебная статистика [Электронный ресурс]. – URL: https://stat.xn----7sbqk8achja.xn--p1ai/ (дата обращения: 30.12.2024).

Польшиков А.В., канд, юрид. наук, доцент, доцент кафедры ФГКОУ ВО «Воронежский институт МВД России», полковник полиции, г. Воронеж

Пучнина М.Ю., канд. юрид. наук, ст. преподаватель ФГКОУ ВО «Воронежский институт МВД России», майор полиции, г. Воронеж

Противодействие вовлечению в проституцию несовершеннолетних посредством использования сети Интернет

Аннотация

В представленной научной статье авторами производится изучение форм и проявлений проституции как социально-негативного явления. Рассматривается вебкаминг как современный цифровой вид проституции. Отдельное внимание уделено вопросам, связанным с вовлечением в проституцию несовершеннолетних.

Ключевые слова: проституция, вебкаминг, несовершеннолетние, вовлечение, оказание сексуальных услуг.

Занятие проституцией рассматривается в нашей стране с юридической точки зрения исключительно как административное правонарушение, предусмотренное ст. 6.1.1 Кодекса об административных правонарушениях Российской Федерации (далее – КоАП РФ). Причем за совершение указанного аморального и асоциального по своей сути и

содержанию административного правонарушения предусмотрено наказание в виде административного штрафа в размере от 1,5 до 2 тыс. рублей, что по мнению большинства экспертов, негативно сказывается на реализации общей и частной превенции предупреждения таких повторных деяний на практике. С учетом прибыли и ее сравнительной легкости, масштабов криминальной деятельности и появления онлайн-сферы оказания интимных услуг посредством сети Интернет – так называемого «вебкаминга» (фактически в настоящий момент организован целый сектор теневой экономики – бизнес различных агентств и студий, которые осуществляют поиск моделей, предоставление помещений и технических средств доступа к сети Интернет [1]), «увлечением» которым массово захватывает молодежь как в России, так и в мире [2]. В УК РФ в настоящее время установлены основания и пределы уголовной ответственности, во-первых, за организацию занятием проституцией (ст. 241 УК РФ), во-вторых, за вовлечение в занятие проституцией (в том числе несовершеннолетних) (ст. 240 УК РФ); в-третьих, за потребление сексуальных услуг подростка за материальное и иное вознаграждение (ст. 240.1 УК РФ). Эти нормы законодательства России образуют «фундамент» уголовно-правовой борьбы с проституцией в стране [3].

Современные технологии позволяют осуществлять деятельность в сфере проституции посредством использования сети Интернет. Речь идет о проблеме массового вовлечения молодежи и лиц более старшего возраста в занятие проституцией через вебкаминг (онлайн-трансляции и переписку). Этот вид проституции менее заметен для правоохранительных органов и достаточно сложен для выявления.

Важно отметить, что проституция как социальное явление имеет множество форм и проявлений, что требует комплексного подхода к ее изучению и разработке эффективных мер противодействия. Важность правового и криминологического анализа проституции заключается в необходимости выявления и устранения факторов, способствующих её распространению, а также в разработке мер профилактики и реабилитации лиц, вовлеченных в данную незаконную деятельность. При этом проституция характеризуется следующими ключевыми признаками:

- возмездность: сексуальные услуги предоставляются за определенное вознаграждение (деньги, материальные блага и т.д.);

- систематичность: занятия проституцией носят регулярный характер, а не являются разовыми случаями;

- отсутствие эмоциональной привязанности: взаимоотношения между сторонами строятся исключительно на коммерческой основе, без личных или эмоциональных связей;

- анонимность: часто участники таких отношений остаются анонимными, что позволяет сохранять конфиденциальность и минимизировать риски для обеих сторон.

В этой связи справедливо указывается, что «…именно признак возмездности, определяющий коммерческий характер полового акта, переводит его в статус секс-услуги, которая, в отличие от беспорядочных сексуальных сношений, предполагает обязательную предварительную договоренность о плате за нее, поэтому главными признаками проституции следует признать систематичность действий и предварительную договоренность об оплате, хотя цена может быть заранее и не названа. Форма же расчета (деньги, ювелирные украшения), способ или момент передачи вознаграждения (до или после сексуального акта) могут быть самыми разнообразными» [4].

Следует признать, что отношение к проституции в различных странах мира существенно различается, что приводит к разным подходам к её легализации или криминализации. В некоторых странах проституция легализована и регулируется государством (например, в Нидерландах, Германии, Новой Зеландии), что позволяет контролировать деятельность, обеспечивать права работников и уменьшать негативные последствия [4].

В других странах (например, в США, за исключением некоторых округов Невады) проституция запрещена и преследуется по закону, что направлено на борьбу с социальными и нравственными проблемами.

Каждый подход имеет свои плюсы и минусы. Легализация позволяет создать более безопасные условия для тех, кто занят в этой сфере, но может также привести к росту количества вовлеченных лиц и увеличению спроса на сексуальные услуги. Криминализация, с другой стороны, ставит целью уменьшение предложения и спроса на сексуальные услуги, но может способствовать маргинализации и увеличению уязвимости тех, кто продолжает заниматься проституцией. Современные технологии и глобализация внесли значительные изменения в способы организации и занятия проституцией. Интернет и мобильные технологии позволяют облегчить контакт между клиентами и поставщиками услуг, делают деятельность менее заметной для правоохранительных органов и создают новые вызовы для их работы. Также наблюдается общемировая тенденция к более «профессиональному» и «организованному» подходу к предоставлению разрешенных сексуальных услуг. Создаются специализированные агентства, предоставляющие услуги эскорта и досуга, функционируют онлайн-платформы и форумы для обмена информацией и отзывами. Налицо подмена понятия «любви» и «любовь за деньги», где де-факто монетизация отно-

шений между людьми, вступающих в интимную связь, одновременно выступает в роли определяющего фактора. Целые страны, например, Таиланд, стал мировой столицей оказания сексуальных услуг, куда стремятся попасть люди не столько для отдыха на океанском побережье, сколько получить незабываемые «ощущения» [3].

Важным аспектом является также проблема увеличения числа случаев «принудительной» и «детской» проституции, что требует особого внимания со стороны государственных органов и международного сообщества. Причем понимание понятия, видов проституции, ее основных признаков и факторов вовлечения является основополагающим для разработки эффективных мер борьбы с этим явлением с позиции противодействия совершению преступлений в данной сфере. Разнообразие форм и проявлений проституции требует комплексного подхода при ее изучении и оценки криминального потенциала, включающего правовые, социальные, экономические и психологические аспекты [5]. Только через всесторонний уголовно-правовой и криминологический анализ проституции как феномена и формы проявления маргинального поведения для разработки и применения многоуровневых мер можно добиться снижения количества фактов и масштабов последствий распространения проституции в нашей стране, а также защиты прав и интересов лиц, вовлеченных в эту противоправную, антисоциальную и аморальную по своей сути деятельность.

Список цитируемой литературы:

1. Кочкина М.С. Вебкам-услуги: пробелы уголовного законодательства Российской Федерации / М. С. Кочкина // Традиции и новации в системе современного российского права : Материалы Международного конгресса молодых ученых. В 3-х томах, Москва, 05–06 апреля 2024 года. – Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. – С. 472–474.
2. Кондраткова Н.В. Зарубежный опыт как отправная точка для построения российской модели противодействия проституции / Н.В. Кондраткова, Е.А. Бартенев // Расследование и предупреждение преступлений, совершенных несовершеннолетними или в отношении несовершеннолетних: сб. матер. всерос. науч.-практ. конфер. (Москва, 20 декабря 2023 года). – Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – С. 74–77.
3. Быкова Е.Г. Некоторые особенности правовой оценки торговли людьми в целях сексуальной эксплуатации // (Москва, 31 марта 2023 г.). – Москва: Московская академия Следственного комитета Российской Федерации, 2023. – С. 92–94.

4. Минстер М.В. Определение понятия и признаки проституции: проблемные аспекты в теории и юридической практике / Бюллетень науки и практики. – 2023. – Т. 9. – № 4. – С. 452–459.
5. Рыбина О.Ю. О некоторых аспектах квалификации преступлений, предусмотренных статьей 240 Уголовного кодекса Российской Федерации // Безопасность личности, общества и государства: теоретико-правовые аспекты: сб. науч. ст. XVI междунар. науч. конфер., проводимой в рамках III междунар. молодежного науч. форума «Северная Пальмира: территория возможностей» (Санкт-Петербург, 31 мая 2023 г.). – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2023. – С. 530.

Скобелин С.Ю., канд. юрид. наук, доцент, доцент кафедры ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева», полковник юстиции, г. Москва

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация

На основе изучения следственной практики расследования развратных действий и смежных с ними преступлений в отношении несовершеннолетних, совершенных с использованием сети «Интернет» и мобильной телефонии за 2020-2024 годы, выделяются признаки и формы таких противоправных деяний. Определена структура криминалистической характеристики указанных преступлений, которая раскрыта через такие значимые для их выявления, раскрытия, расследования и предупреждения элементы, как обстановка совершения преступлений, характеристика личности жертвы и преступника, способ и механизм следообразования.

Ключевые слова: криминалистическая характеристика, развратные действия, сеть «Интернет», половая неприкосновенность, несовершеннолетние, раскрытие, расследование, профилактика.

Современная следственная практика свидетельствует о том, что сеть «Интернет» и мобильная телефония стали способами совершения преступлений против половой неприкосновенности несовершеннолетних.

Их своевременное раскрытие, полное и объективное расследование требует от сотрудников правоохранительных органов соответствующих знаний, умений и навыков.

Речь идет о таких преступлениях, как:

- насильственные действия сексуального характера (п. «б» ч. 4, п. «а» и (или) «б», ч. 5 ст. 132 УК РФ);

- понуждение к действиям сексуального характера (ч. 2 или п «б» и (или) «в» ч.3 ст. 133 УК РФ);

- развратные действия (ст. 135 УК РФ).

Нередко преступники по совокупности совершают также такие преступления, как нарушение неприкосновенности частной жизни (ст.137 УК РФ); вымогательство (ст.163 УК РФ); получение сексуальных услуг несовершеннолетнего (ст. 240.1. УК РФ); изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242, ст. 242.1, ст. 242.2 УК РФ).

Если в 2013 году было зарегистрировано 52 сообщения о преступлениях указанной категории, в 2014 году уже 276, а в последующие годы их количество только росло и в 2023 было зарегистрировано уже около тысячи подобных преступлений, при этом 1/3 из них остается нераскрытыми [1, с.112].

Общими признаками для них являются:

1) использование сети Интернет (социальные сети, мессенджеры, компьютерные игры, сайты знакомств и т.п.) или телефонной связи (соответственно простых телефонов, смартфонов или компьютеров с SIM-картой);

2) дистанционность (преступник и жертва находятся в разных местах, порой даже странах);

3) отсутствие физического контакта с телом потерпевшего (интеллектуальные развратные действия в отношении лиц, не достигших 16 лет (путем переписки, голосовых или видеозвонков, бесед, отправки фотографий) или иные действия сексуального характера в отношении детей, находящихся в беспомощном состоянии, в том числе не достигших 12 лет);

4) длящийся характер (порой многоэпизодность) переписки и (или) звонков;

лица, совершающие данные преступления часто страдают различными формами парафилии (в частности педофилией – расстройством сексуального предпочтения), могут иметь иные психические отклонения сексуального характера) [2, с.19];

5) естественная латентность (несовершеннолетние жертвы и их близкие не желают огласки подобных деяний).

В соответствии с п.17 Постановления Пленума Верховного Суда РФ от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» к развратным действиям относятся любые действия, кроме полового сношения, мужеложства и лесбиянства, совершенные в отношении лиц, достигших двенадцатилетнего возраста, но не достигших шестнадцатилетнего возраста, которые были направлены на удовлетворение сексуального влечения виновного, или на вызывание сексуального возбуждения у потерпевшего лица, или на пробуждение у него интереса к сексуальным отношениям.

При этом, развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети Интернет, иных информационно-телекоммуникационных сетей.

Интернет-разврату присущи следующие формы:

- цинично-вульгарные разговоры (переписка) на темы сексуального характера;

- прикрепление ссылок, файлов или демонстрация в онлайн режиме эротических или порнографических фотографий или видеозаписей (возможно половых органов, актов мастурбации или половых актов самого преступника с иными лицами). Не имеет значения для уголовного преследования сделаны ли фотографии самим преступником, скопированы из других источников или сгенерированы с помощью искусственного интеллекта;

- склонение потерпевшего к демонстрации своего обнаженного тела (половых органов), актов мастурбации, половых контактов с иными лицами путем уговоров, угроз применения насилия к самому потерпевшему либо его близким, распространения сведений, позорящих потерпевшего или его близких;

Для привлечения виновных к уголовной ответственности не имеет значения, имел ли потерпевший опыт половых отношений, степень его осведомленности об этом, а также его половая зрелость и даже тот факт, что инициатором таких действий мог выступать сам потерпевший, а виновный, осознавая, что общается с лицом, не достигшим 16 лет, дал согласие и продолжил развращать ребенка.

В тоже время беседы на тему сексуальных отношений совершеннолетних лиц с детьми с использованием информационных технологий и даже демонстрирование им фотографий, предметов, картин, видеофильмов с изображением обнаженных людей, половых органов и актов, вовсе не обязательно образуют признаки анализируемых составов преступлений. Это зависит от формы, мотивов и целей таких действий.

Например, такие беседы, предметы, фото или видео материалы могут предоставляться несовершеннолетним в воспитательно-просветительских, научных, медицинско-профилактических целях, либо обладать эстетической, исторической, художественной или культурной ценностью.

Также должны исключать уголовную ответственность провокационные действия сотрудников правоохранительных органов или близких несовершеннолетних потерпевших, поддерживающих переписку с целью искусственного создания доказательств противоправной деятельности лица.

Особенности структуры криминалистической характеристики:

Обстановка совершения рассматриваемых нами преступлений (время, место) характеризуется следующей спецификой.

Преступления совершаются чаще всего в домашней обстановке (если в доме или квартире проживают другие люди – в отдельной закрытой комнате), в которой и преступник, и жертва чувствуют себя защищенно, комфортно и расслаблено. Встречаются случаи, когда преступники совершали развратные действия, находясь в местах лишения свободы, отбывая уголовное наказание за другие (чаще подобные) преступления. После того, как преступник выявляет в социальных сетях будущую жертву и устанавливает с ней коммуникацию, не исключены сессии связи с помощью смартфона и на открытой местности.

Преступления совершаются в вечернее или ночное время. Какой-либо корреляции активности исследуемой преступной деятельности с временами года, праздничными и выходными днями не установлено.

Личность преступника. Преимущественно подобные преступления совершают лица мужского пола, в возрасте 25-45 лет, без высшего образования, имеющие психические отклонения на почве сексуальных отношений. Уголовной ответственности за развратные действия подлежат лица, достигшие ко времени совершения преступления восемнадцатилетнего возраста. Групповой способ совершения преступлений не свойственен для развратных действий, совершенных с использованием информационных технологий.

Не редко они состояли или состоят на учетах в психоневрологических диспансерах, ранее уже привлекались к уголовной или административной ответственности за деяния, смежные или подобные рассматриваемым.

Говоря о возрасте преступника, необходимо помнить и использовать данный момент в ходе установления психологического контакта с преступником о том, что в соответствии с п.2 примечания к ст.134 УК РФ в случае, если разница в возрасте между потерпевшей (потерпев-

шим) и подсудимым (подсудимой) составляет менее четырех лет, к последнему не применяется наказание в виде лишения свободы. Однако, данное правило распространяется только на лиц, в действиях которых усматривается основной состав развратных действий – только часть 1 ст.135 УК РФ. Также лицам, осужденным за преступления против половой неприкосновенности несовершеннолетних, не достигших четырнадцатилетнего возраста, не может быть назначено условное осуждение (ст.73 УК РФ).

Такие лица редко имеют глубокие познания в сфере высоких технологий, пользуются смартфоном и (или) компьютером на бытовом уровне, однако принимают меры к анонимизации путем вымышленных анкетных данных при регистрации в социальных сетях, приобретают и используют одноразовые SIM карты, фэйковые аккаунты, VPN или прокси серверы.

Ими движет сексуальное влечение к несовершеннолетним, удовлетворение своих необузданных половых потребностей, возбуждение от общения или наблюдения за детьми.

Способ. Следственная практика свидетельствует о том, что при подготовке к развратным действиям, виновные осуществляют поиск будущей жертвы по определенным, возбуждающих их признакам. Это могут быть определенные имена детей, их цвет волос или глаз, антропометрические данные и др. В не крупных населенных пунктах жертва подыскивается из других регионов и городов.

Преступники, как правило, инициируют общение и знакомство с жертвой. Для того, чтобы заинтересовать несовершеннолетних, могут использоваться виртуальные подарки, бонусы, баллы, стики, эмодзи, подписки, игрушки и т.п.

В частности, в социальной сети «В контакте» в качестве виртуальной валюты предусмотрены так называемые «голоса», рассчитываясь которыми можно приобрести стикеры, подарки, игры, либо Premium-статус в приложении VK Знакомства. В «Telegram» такой внутренней валютой являются Telegram Stars «звёзды», в «Tik Tok» - монеты, предусмотрены платные реакции (донаты) на трансляции, которые лицо может обналичить. Иногда жертвам перечисляются и реальные денежные средства. При этом и тот, и другой могут использовать вымышленное имена, никнеймы, аватарки, менять реальную дату, год и место рождения, место жительства и работы (учебы).

Непосредственно развратные действия начинаются далеко не сразу. Преступник может по несколько недель или месяцев ежедневно общаться с потерпевшим на различные темы и лишь убедившись в доверии, а иногда и в искренней дружбе (любви) к нему – переходит к

намекам или разговорам на сексуально-интимные темы. Само общение часто имеет накопительно-нарастающий эффект: от безобидных шуток и фото, до циничных, откровенных бесед, фото-видео эротического или порнографического характера. При этом следует учитывать, что даже с одним потерпевшим в действиях виновного может быть совокупность нескольких самостоятельных преступных действий: идеальная совокупностью (развратные действия путём направления (распространения) изображений порнографического содержания) или реальная совокупность (несколько отдельных эпизодов преступлений, предусмотренных ст.135 УК РФ, либо последующее вымогательство (ст.163 УК РФ), собирание или распространение сведений о частной жизни лица (ст.137 УК РФ).

Для выхода в сеть Интернет-преступник чаще использует ноутбук, стационарный компьютер (моноблок), реже планшет или смартфон. Марка и модель устройства (которую можно определить при осмотре метаданных отправленных или изготовленных с его помощью файлов. Фотографий, видео контента) имеет значение для последующего обыска, их осмотра с использованием высокотехнологичной техники или назначения компьютерно-технической экспертизы.

Отметим еще раз. При совершении развратных действий с использованием сети Интернет, преступник зачастую осознавая аморальность и противоправность своих действий, тщательно скрывает факты общения с жертвой. Использует VPN соединения, режим «Инкогнито», чистит историю браузера, удаляет переписку, фото и видеофайлы.

Изучение жертвы рассматриваемых преступлений имеет криминалистическое значение для организации и проведения с ними таких следственных действий как допрос, очная ставка, проверка показаний на месте, предъявления для опознания, а также юридической оценки содеянного, назначения в отношении несовершеннолетних потерпевших комплексных психолого (сексолого)-психиатрических и иных видов экспертиз.

В своем большинстве это дети от 7 до 15 лет, женского пола из благополучных семей, испытывающие потребность в общении, дружбе проявляющие первые признаки полового созревания и интерес к своему телу и сексуальным темам. По характеру они доверчивы, меланхоличны, с высоким уровнем эмпатии. В заключениях комплексных психолого-психиатрических экспертиз таких потерпевших часто отмечаются такие качества, как нерешительность, ведомость по отношению к сильным личностям, впечатлительность, недостаточная способность отстоять свою позицию в споре.

Имеют в своем пользовании смартфоны и ноутбуки, обладают некоторыми познаниями в области IT-технологий. Самостоятельно регистрируются в социальных сетях, заводят электронные кошельки, могут осуществлять денежные переводы преступникам под угрозой распространения порочащих сведений.

Встречаются факты развратных действий, совершенных одновременно в отношении двух или более несовершеннолетних.

В соответствии с примечанием к ст.131 УК РФ, развратные действия (в форме иных действий сексуального характера), совершенные в отношении лица, не достигшего двенадцатилетнего возраста, следует квалифицировать по п. «б» ч.4 ст.132 УК РФ, как насильственные действия сексуального характера, поскольку такое лицо в силу возраста находится в беспомощном состоянии, то есть не может понимать характер и значение совершаемых с ним действий.

Между тем, на основании п. 21 Постановления Пленума Верховного Суда РФ от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» указанная квалификация возможна лишь при доказанности умысла на совершение развратных действий в отношении лица, не достигшего двенадцатилетнего возраста, то есть когда виновный знал или допускал, что потерпевшим является лицо, не достигшее 12 лет. Данное обстоятельство следует учитывать при подготовке и проведении следственных и иных процессуальных действий (допрос, осмотр места происшествия, предметов, запросы в социальные сети) и назначении соответствующих экспертиз.

Следы преступлений. Как и по другим преступлениям, которые совершаются с помощью информационно-коммуникационных технологий, основными следами их подготовки, совершения и сокрытия являются цифровые следы:

- сам факт использования компьютера (смартфона), имеющего выход в сеть Интернет в установленные временные промежутки (MAC (физический) адрес данных устройств, маршрутизатора, через который раздается сеть WI-FI или EMAI смартфона, марка, модель устройств, IP используемый в момент выхода с сеть);

- цифровые фото, видео файлы (их метаданные) обнаженных частей тел жертвы, преступника (возможно изображение его лица) или посторонних людей, направленные потерпевшему или подозреваемому, часто сделанные смартфоном или камерой ноутбука (планшета) участников уголовного судопроизводства или иным устройством;

- текстовые (печатные) или аудио-видеосообщения, развратного содержания в мессенджерах и социальных сетях (речевые следы в виртуальном пространстве);

- ID-адрес личной страницы пользователя, время и IP-адрес регистрации профиля, номер мобильного телефона, адрес электронной почты, история смены имени пользователя и прикрепленного номера мобильного телефона, время и IP адрес размещения определенного контента, история и перечень IP-адресов для входа на страницу;

- транзакции денежных переводов;

- биллинги телефонных соединений и GPRS сессий между потерпевшим и преступником или иными лицами, их детализация;

- установление места локации - нахождения цифровых устройств участников уголовного процесса с помощью базовых станций операторов связи, GPS, ГЛОНАСС модулей или зоны покрытия WI-FI сети;

- записи с видеокамер (реже).

Материальными следами могут выступать биологические (следы спермы, потожировые, ДНК, запаховые следы); следы пальцев рук, ладоней на периферийных устройствах или экране гаджета; микроволокно одежды подозреваемого на компьютерном стуле и т.д.

Самыми распространенными конечно же выступают идеальные следы – показания потерпевшей, свидетелей, специалистов, экспертов и подозреваемого. Свидетелями по таким делам могут выступать не только близкие потерпевшего (родители, бабушки, дедушки, братья, сестры, друзья), но и их педагоги, медицинский персонал, психолог, к которому пришлось обращаться за помощью и консультацией и др. Со стороны подозреваемого свидетелями могут быть также его родственники, коллеги по работе, знакомые, врачи, сотрудники правоохранительных органов, раскрывшие преступление и др.

Непосредственно выявить и идентифицировать лицо, совершившее данные преступления достаточно сложно. Это возможно при визуальном или голосовом контакте подозреваемого и жертвы (путем предъявления для опознания). Также этому способствует автороведческая экспертиза по печатной речи (при наличии достаточного для исследования количества свободных или условно-свободных образцов печатного текса, выполненного преступником).

Список цитируемой литературы:

1. Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. – Москва: ЮНИТИ-ДАНА, 2023. – 279 с.

2. Иващенко, М.А. Расследование преступлений против половой неприкосновенности и половой свободы несовершеннолетних, совершенных с использованием сети Интернет: практическое пособие. – Москва: Московская академия СК России, 2022. – 100 с.

Солодина С.А., адъюнкт
ФГКОУ ВО «Воронежский институт МВД России»,
старший лейтенант полиции, г. Воронеж

О НЕКОТОРЫХ ВОПРОСАХ ИСПОЛЬЗОВАНИЯ АЗАРТНЫХ ИГР В СЕТИ «ИНТЕРНЕТ» ДЛЯ ОТМЫВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ, ПРИОБРЕТЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

Аннотация

Статья посвящена проблеме использования азартных игр в сети Интернет для отмывания денежных средств, полученных преступным путем. Рассматриваются основные схемы и механизмы, применяемые преступниками для легализации незаконных доходов через онлайн-казино и букмекерские конторы. Анализируются трудности, возникающие при контроле и регулировании данного сектора, а также предложены возможные пути решения проблемы. Особое внимание уделено необходимости усиления международного сотрудничества и внедрения современных технологий для выявления и предотвращения подобных преступлений.

Ключевые слова: азартные игры; индустрия развлечений; незаконная организация и проведение азартных игр; криптовалюта; онлайн-казино.

Отмывание денег или легализация доходов, полученных преступным путем, остается актуальной проблемой для мирового сообщества. Распространение азартных игр в сети Интернет обусловлено непрерывным развитием технологий, которые упрощают доступ к онлайн-ресурсам. Азартные игры в сети Интернет стали использоваться для маскировки незаконных финансовых операций. Следует отметить, что данная деятельность носит трансграничный характер, поскольку серверы, необходимые для функционирования интернет-сайтов, могут располагаться в любой точке земного шара, в том числе и в оффшорных зонах и это, в свою очередь, приводит к возникновению законодательных и правовых пробелов.

Гемблинг-индустрия пользуется популярность в различных странах, так как в большинстве случаев этот бизнес легален или частично легален и приносит значительный доход. В последнее время наблюдается рост преступной деятельности, связанной с отмыванием денег через азартные онлайн-игры. «Благодаря» Covid-19, в 2020 году игорный рынок для мобильных устройств в глобальном объеме оценивался почти в 80 млрд. долларов США. Около 30% от всего объема было сконцентрировано в США, на втором месте расположился Китай, где огромной популярностью пользуется покер. Основными конкурентами на мировой арене бирж ставок являются две компании: Betfair Group PLC (британская компания, занимающаяся азартными играми) и Ladrokes Coral Group (британская игровая компания). На фоне стремительного роста глобального рынка онлайн-азартных игр многие государства приняли решение легализовать гемблинг, вводя при этом жесткие меры для борьбы с незаконными практиками. Тем не менее, преступники стали использовать эту систему для отмывания средства, полученных незаконным путем.

С развитием Интернета и ростом популярности азартных онлайн-игр, платформы для их использования стали привлекательным инструментом для преступников. Они используют несколько основных схем для легализации своих доходов:

1. Создание фиктивных выигрышей. Преступники могут использовать подконтрольные им аккаунты для создания видимости крупных выигрышей.

2. Использование нескольких счетов. Злоумышленники открывают множество аккаунтов в различных онлайн-казино или букмекерских конторах, распределяют средства между ними и совершают многократные переводы, затрудняя отслеживание происхождения денежных средств.

3. Партнерские программы. Некоторые онлайн-казино предлагают партнерские программы, позволяющие получать "бонусы" (денежные средства) за привлечение новых игроков. Преступники могут создавать фальшивые сайты и привлекать пользователей, получая "легальный" доход.

4. Биржа ставок. На некоторых платформах пользователи могут делать ставки "против". Игрок, сделавший такую ставку, автоматически превращается в букмекера и при выигрыше прибыль будет исчисляться из поставленных денег другим участником - комиссия биржи.

5. Криптовалюта. Использование криптовалют, например Bitcoin (BTS) или Earth Operating System (EOS). позволяет еще больше скрыть

следы финансовых транзакций, поскольку они анонимны и децентрализированы.

Чтобы минимизировать риски, преступники предпочитают выводить средства с помощью криптовалюты, так как идентифицировать владельца кошелька в таких случаях практически невозможно. В своем отчете, компания по кибербезопасности «Trend Micro» указала, что: «Игроки должны осознавать значимость своей роли в киберпреступности каждый раз, когда участвуют в онлайн-обмене цифровыми валютами. DDos-атаки, кражи учетных данных и финансовое мошенничество – лишь часть тех негативных последствий, которые наносят вред различным компаниям и организациям с помощью игровых валют».

На данный момент рынок криптовалют не подлежит регулированию и понятия в правовом поле «криптовалюта» тоже не существует. Но большинство стран рассматривают принятие криптовалют как средство оплаты на законном уровне. Сегодня, из-за популярного использования блокчейна и наступающей метавленной, единственным доступным способом оплаты различных товаров и услуг, является как раз-таки криптовалюта. Незаконный оборот криптовалюты в сфере азартных игр осуществляется через несколько этапов. На начальном этапе злоумышленник сосредоточен на добыче игровой валюты. Этот процесс может включать в себя кражу валюты у других пользователей, эксплуатацию уязвимостей онлайн-казино или онлайн-игр с применением различных схем, а так же внедрение вредоносных программ. Ключевыми факторами, способствующими широкому распространению отмывания денег через онлайн-казино, являются недостаток строго законодательного регулирования и высокая степени анонимности пользователей данной сферы. Казино легко обходят меры блокировки, которые к ним применяются, а реклама азартных игр в сети Интернет является повсеместной. В результате, фактического исполнение законодательства о запрете азартных онлайн-игр, оказывается затруднительным. Объясняется это тем, что законодательство в области игорной деятельности разных странах разнообразно и оно варьируется от полной легализации до тотального запрета азартных игр [1]. Привлечь к ответственности некую онлайн-компанию, зарегистрированную в стране, где азартные игры легализованы, представляется невозможным. Эффективным решением данной проблемы может стать ужесточение регулирования и мониторинг финансовых операций. На втором этапе осуществляется продажа полученной игровой валюты на определенных площадках. После этого правонарушитель получает выплату, в виде криптовалюты, что еще больше вызывает трудность в слежке дальнейших переводов.

В итоге можно сделать вывод, что строгое регулирование сферы азартных онлайн-игр является одним их основных факторов, значительно уменьшающих вероятность возникновения незаконной деятельности в данной области, включая использование криптовалют. Для минимизации таких рисков важно обеспечить выполнение следующих условий:

1. Лица, желающие создать свои онлайн-платформы для предоставления услуг в сфере азартных игр, должны пройти тщательную проверку со стороны лицензирующих органов. Это поможет значительно снизить риск возникновения условий для незаконной деятельности на данных онлайн-платформах;

2. Операторы азартных онлайн-игр обязаны информировать надзорные органы о фактах выявлений злоупотреблений и угроз;

3. Услуги могут предоставляться только в том случае, если денежные средства переводятся через лицензированные и регулируемые кредитно-финансовые учреждения.

Также можно ввести дополнительные меры в отношении поставщиков услуг азартных онлайн-игр для снижения указанных выше рисков. Например, установить ограничения на суммы переводов между счетами или запретить проведение транзакций между игровыми счетами пользователей онлайн-платформы, возможно еще предотвратить создание и использование более одного игрового счета одному пользователю.

Запреты Центрального банка Российской Федерации (далее – ЦБ РФ), касающиеся переводов с интернет-кошельков ЮMoney в адрес иностранных интернет-магазинов, оказались действенными, в связи с чем данную компанию оштрафовали на сумму крупную сумму денег. ЦБ РФ проводил проверки банков, участвующих в данной операции с онлайн-казино, в результате чего пострадали не только QIWI банк, но и АО Банк «Онего» и ООО «КБ «Финтех»», утратив после этого свои лицензии. Данные транзакции проходят с использованием схемы p2p-переводов (peer-to-peer). Средства массовой информации обнаружили, что онлайн-казино «Azino 777» принимает платежи через «Сбербанк», несмотря на блокировку счетов и карт подозрительных пользователей. Онлайн-казино могут использовать логотипы известных брендов для создания ложной информации о легальности данного заведения.

Проблема использования онлайн-гемблинга для отмывания денег требует комплексного подхода и совместных усилий со стороны государственных органов и финансовых учреждений. Вопрос применения других видов ответственности, таких как административной и финансовой, в дополнение к уголовной до сих пор носит актуальный харак-

тер [2]. Противодействие такого рода преступлениям возможно только в случае, когда оно будет одновременно проводиться на национальном и международном уровнях. Исходя из этого, можно сделать вывод, что легализация доходов, полученных преступным путем, имеет не только негативные последствия для макроэкономики страны в целом (так как преступные доходы попадают в легальный оборот), но и представляет угрозу для ее экономической и национальной безопасности. Данный вид преступления носит международный характер, даже если легализация преступных доходов имела место исключительно в рамках национальной экономики одного государства.

Список цитируемой литературы:

1. Абазехова, З.И. Проблема использования азартных игр в информационно-телекоммуникационной сети Интернет для отмывания денежных средств, приобретенных преступным путем / З. И. Абазехова // Вестник Московского университета МВД России. – 2021. – № 5. – С. 143–146.
2. Елизарова, В.В. Воздействие легализации преступных доходов на экономику страны / В. В. Елизарова // Вестник Московского финансово-юридического университета МФЮА. – 2021. – № 4. – С. 38–45.

Соломонова В.В., преподаватель
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОЙ РОССИИ: МАСШТАБЫ И ПОСЛЕДСТВИЯ

Аннотация

В данной статье представлена краткая характеристика состояния киберпреступности в текущий период, а также выделены уникальные особенности преступлений, связанных с использованием информационных технологий, что приводит к увеличению, как общего числа таких преступлений, так и их скрытости. Особое внимание уделяется характеристикам киберпреступности, таким как анонимность преступника, транснациональный характер и высокая скорость распространения информации среди пользователей Интернета, что способствует использованию высоких технологий злоумышленниками для сокрытия следов своих преступлений.

Ключевые слова: киберпреступность, виртуальное пространство, анонимность, интернет, защита данных.

На нынешнем этапе развития общества наблюдается широкое внедрение современных телекоммуникационных технологий [1, С. 144] во все сферы жизни. К сожалению, злоумышленники всё чаще применяют информационные технологии в преступных целях, это обусловлено особыми характеристиками виртуального пространства и технологий, используемых для передачи и обработки данных.

Развитие новых технологий принесло в нашу жизнь негативные явления, такие как киберпреступность. Это преступления, совершаемые в виртуальном пространстве, где зачастую злоумышленникам не требуются специальные навыки, достаточно быть обычным пользователем компьютерной техники. Современные программные средства обеспечивают простоту в использовании, что позволяет даже детям без труда осваивать новые приложения. Для анализа использовались нормативные акты, регулирующие уголовную ответственность за преступления с использованием информационных технологий, а также специализированная литература. Исследование базируется на общенаучных методах, анализе теоретических источников и статистике.

Киберпреступления обладают особенностями [2, С. 87], отличающими их от традиционных преступлений, такими как транснациональность, анонимность и мгновенное распространение информации.

Транснациональность подразумевает возможность совершения преступлений в одном месте с причинением ущерба на другом конце мира. Анонимность позволяет злоумышленникам действовать без особого риска, что создает ложное чувство безнаказанности [3, С. 277]. Также важно отметить, что информация может распространяться мгновенно с минимальными затратами, достигая значительного числа пользователей, что делает киберпреступления особенно опасными.

В 2023 году МВД России зарегистрировало свыше 100 тысяч киберпреступлений. По сравнению с 2022 годом, количество таких правонарушений увеличилось на 29,7%. Доля преступлений, связанных с высокими технологиями, сохраняется на уровне 25% от общего числа дел. Растущая популярность телекоммуникационных услуг и социальных сетей, наряду с недостаточными мерами по защите, способствовала увеличению числа кибератак. Согласно более ранним исследованиям [4, С. 137], типичный киберпреступник — мужчина около 30 лет, холост, с среднем образованием, который живет в городе и занимается мошенничеством. Жертвами становятся пользователи устройств, не заботящиеся о своей кибербезопасности, при этом более трети пользователей столкнулись с атаками злоумышленников. В 2023 году 55,4%

пострадавших составили женщины. Основным способом связи с жертвами остаются телефонные звонки. Растет и мошенничество через мессенджеры, где злоумышленники часто маскируются под представителей банковской сферы или госструктур. Эффективные методы борьбы с кибермошенничеством включают информацию для граждан и повышение их грамотности в вопросах безопасности.

Исследование показало, что 4,3% опрошенных перевели мошенникам суммы свыше миллиона рублей. Интересно, что люди, столкнувшиеся с киберпреступниками, помнили о правилах безопасности. Одним из признаков мошенничества является разговор о деньгах и требование быстрого принятия решения.

В последнее время участились DDoS-атаки *(Distributed Denial of Service, «распределённый отказ от обслуживания»)* [5, С. 190] - это форма кибератаки на веб-системы с целью вывести их из строя или затруднить доступ к ним для обычных пользователей, в том числе направленные на конкретные цели. Для борьбы с этой угрозой в Оренбургском государственном университете создан центр Национального киберполигона. Здесь специалисты моделируют кибератаки и отрабатывают навыки противодействия им.

Международное сотрудничество в борьбе с киберпреступностью основано на Конвенции о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [6]. Российское законодательство старается адаптироваться к новым видам преступлений в цифровой сфере. Помимо главы 28 УК РФ, посвященной преступлениям в сфере компьютерной информации, в Уголовный кодекс были внесены статьи 159.6 (Мошенничество в сфере компьютерной информации) и 159.3 (Мошенничество с использованием электронных средств платежа).

Для эффективной борьбы с киберпреступностью необходимо анализировать методы и тактику злоумышленников, понимать их мотивы, цели и стратегии. Также важно изучать уязвимости информационных систем, разрабатывать средства защиты и стратегии предотвращения кибератак. Предупреждение кибермошенничества включает информирование граждан через социальную рекламу, образовательные программы и повышение финансовой и информационной грамотности.

В настоящее время наблюдается значительный рост числа преступлений, происходящих в киберпространстве с применением современных информационных технологий, что приводит к увеличению угрозам информационной безопасности и вызывает глобальное беспокойство. Для обеспечения кибербезопасности необходимо строгое соблюдение норм защиты информации на всех уровнях, разработка стра-

тегий, направленных на снижение рисков, а также повышение уровня компьютерной и информационной грамотности среди сотрудников и граждан.

Решение вопросов по кибербезопасности требует целостного подхода и совместных усилий всех государств и организаций. Важно разрабатывать действенные стратегии и программы, которые будут способствовать устойчивому экономическому развитию и охране национальных интересов. Также необходимо укрепление международного сотрудничества и координации действий для обеспечения надежной защиты интересов всех стран.

Список цитируемой литературы:

1. Хоменко, А.Н. К вопросу о виктимизации жертв киберпреступлений / А.Н. Хоменко // Виктимология. – 2021. – Т. 8. – № 2. – С. 143–148.
2. Мордвинов, К.В., Удавихина, У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью / К.В. Мордвинов, У.А. Удавихина // Теоретическая и прикладная юриспруденция. – 2022. – № 1 (11). – С. 83–88.
3. Шевко, Н.Р. Мошенничество в киберпространстве: реальный ущерб в виртуальном мире / Н.Р. Шевко // Вестник Восточно-Сибирского института МВД России. – 2023. – № 3 (106). – С. 276–284.
4. Шевко, Н.Р. Особенности киберпреступности: состояние и тенденции / Н.Р. Шевко // Уголовная политика в условиях цифровой трансформации: сборник материалов II Всероссийской научно-практической конференции (Казань, 27 апреля 2023 г.). Казань: Отечество, 2023. С. 135–141.
5. Ляпин А. Е. Новые угрозы кибербезопасности как следствие цифровизации в топливно-энергетическом комплексе // Цифровая трансформация промышленности: современные формы устойчивого развития: сборник научных трудов по материалам 4-й Всероссийской научно-практической конференции (Москва, 09 ноября 2023 г.). Москва: Русайнс, 2023. С. 188–195.
6. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). // PPC World. URL: https://base.garant.ru/4089723/ (Дата обращения: 12.01.2025).

Татаринова А.С., магистрант
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Научный руководитель – Брусенцева В.А., канд. юрид. наук, доцент,
доцент кафедры
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОГО ПРОСТРАНСТВА

Аннотация

Предупреждение преступлений в сети интернет требует комплексного подхода со стороны правоохранительных органов, включающего как образовательные инициативы, так и технические меры защиты. Создание специализированных подразделений, мониторинг и аналитика сетевой активности, сотрудничество с интернет-компаниями и международными правоохранительными структурами, а также совершенствование законодательства — все это является ключевыми компонентами эффективной стратегии.

Ключевые слова: информация, Интернет, предупреждение преступлений, расследование

Информационные технологии являются обыденной частью современного общества. Как административные, так и социально-экономические процессы в государстве характеризуются внедрением технологий машинного обучения, социальных сетей, технологий блокчейн, математического программного вычисления или искусственного интеллекта и др.

Данное обстоятельство прямо влияет на динамику преступности в сфере информационно-телекоммуникационного пространства. Современное состояние свидетельствует о недостаточности раскрытия и расследования данной категории преступлений.

Так, согласно отчету ГИАЦ МВД России [2] о состоянии преступности в январе - июне 2024 г., зарегистрировано 368,8 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, из них раскрыто 3,4%.

Практически все такие преступления (98,7%) выявляются органами внутренних дел. Почти половина таких преступлений (47,1%) отно-

сится к категориям тяжких и особо тяжких (173,6 тыс.), четыре преступления из пяти (82,4%) совершаются с использованием сети Интернет (304,0 тыс.; +24,6%), почти половина (46,4%) - средств мобильной связи (171,1 тыс.; + 19,9%).

Такие низкие показатели являются следствием практических проблем в области расследования, в частности, преступления являются, как правило, длящимися, поэтому факт начала совершения преступного деяния не удается точно определить; отсутствие специалистов, обладающих специальными знаниями в области информационных технологий и принципов их обнаружения и расследования; большое количество качественно новых способов совершения преступлений в данной сфере; недостаточное межгосударственное взаимодействие в сфере расследования и пресечения преступлений, поскольку место совершения, в большом количестве случаев, носит межгосударственный характер и др.

Одной из важных проблем предупреждения является недостаточная технически-программная обеспеченность сотрудников правоохранительных органов. Деятельность по расследованию преступлений в сфере информационных технологий требует обработки большого количества материалов (графического, системных кодов). Так обработка следа программного кода требует высоких системных нагрузок, поэтому старое оборудование с ними не справляется. Также большинство процессов требуют автоматизации, например, при помощи блокчейн технологий, которые позволяют автоматически обработать программный код и выявить первоисточник.

Не во всех линейных подразделениях правоохранительных органов, на данный момент времени, образованы специализированные подразделения, занимающиеся расследованием исключительно преступности в сфере информационно-телекоммуникационного пространства. Данные подразделения могут стать эффективным механизмом, как расследования, так и предупреждения уже готовящихся преступлений. Кроме того, данные подразделения могут осуществлять постоянный мониторинг преступности в сфере информационно-телекоммуникационного пространства, исследование новых форм совершения преступлений в данной области, а также заниматься разработкой эффективной стратегией защиты, обращаясь к правоприменительному опыту.

Также разумным будет осуществлять сотрудничество с производителями программного обеспечения для создания систем, которые помогут предотвратить преступность в сфере информационно-телекоммуникационного пространства, такие как, например, фильтрация вредоносного контента и блокировка фишинговых сайтов [3, С. 32].

Внедрение искусственного интеллекта, анализа больших данных, распределенных реестров в объединенную систему правоохранительных органов позволит оперативно осуществлять мониторинг сетевой активности и выявлять новые преступные схемы, а также даст синергетический эффект в виде снижения издержек на правоохранительную деятельность, а также защищенности информационно-телекоммуникационного пространства [1, С].

Таким образом, применение этих методов в совокупности может значительно повысить эффективность правоохранительных органов в предупреждении и расследовании преступлений, совершенных в сети интернет. Создание специализированных подразделений, мониторинг и аналитика сетевой активности, сотрудничество с интернет-компаниями и международными правоохранительными структурами, а также совершенствование законодательства — все это является ключевыми компонентами эффективной стратегии. Важным аспектом также является поддержка жертв преступлений через горячие линии и консультационные службы, что способствует созданию безопасной и устойчивой интернет-среды. Согласованность действий и готовность адаптироваться к новым угрозам позволит правоохранительным органам эффективно бороться с киберпреступностью и защищать пользователей онлайн.

Список цитируемой литературы:

1 Бурчук, А.Г. Практические проблемы противодействия преступлениям, совершаемым в информационно-телекоммуникационном пространстве / А.Г. Бурчук // Российский следователь. – 2024. – № 10. – С. 51–55.

2 Отчет ГИАЦ МВД России о состоянии преступности в январе - июне 2024 г. [Электронный ресурс] – МВД России: сайт. – URL: https://xn--b1aew.xn--p1ai/reports/item/53218362 (дата обращения: 08.12.2024).)

3 Чекунов, И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества / И.Г. Чекунов // Российский следователь. – 2015. – № 17. – С. 29–33.

Тетерина М.Н., магистрант
ФГБОУ ВО «Донской государственный технический университет»
(ДГТУ), г. Ростов-на-Дону

Правовые аспекты кибербезопасности в банковском секторе

Аннотация

В данной работе рассматриваются ключевые аспекты обеспечения кибербезопасности в банковском секторе с правовой точки зрения. Исследуются современные механизмы защиты банковских информационных систем, анализируются правовые меры противодействия киберугрозам. Особое внимание уделяется совершенствованию методов выявления и расследования киберпреступлений, а также профилактическим мерам их предупреждения. Работа содержит практические рекомендации по повышению эффективности правового регулирования в сфере кибербезопасности банковского сектора.

Ключевые слова: кибербезопасность, банковский сектор, правовые аспекты, киберугрозы, киберпреступления, информационные системы.

В эпоху интенсивного развития цифровых финансовых технологий обеспечение кибербезопасности банковского сектора становится критически важной задачей. Нормативно-правовой фундамент защиты базируется на ключевых федеральных законах, регламентирующих банковскую деятельность и информационную безопасность, а также директивах Центрального банка Российской Федерации [3].

Фундаментальным аспектом юридической защищенности выступает императивное требование к имплементации комплексных систем информационной безопасности в финансовых институтах. Регуляторные предписания обязывают кредитные организации использовать исключительно сертифицированные защитные механизмы и систематически проводить комплексную оценку их эффективности.

Приоритетное внимание уделяется сохранности конфиденциальных сведений о клиентах и соблюдению режима банковской тайны. Действующее законодательство предъявляет повышенные требования к процедурам обработки и хранения подобной информации, устанавливая серьезную ответственность за допущенные нарушения. Финансовые учреждения должны обеспечивать многоступенчатую систему защиты, включающую современные криптографические решения.

Существующая правовая база предусматривает обязательное уведомление регулятора о зафиксированных нарушениях кибербезопасности. Данный механизм обеспечивает своевременное реагирование на

возникающие угрозы и эффективную координацию защитных мероприятий в масштабах банковской системы страны.

Согласно статистическим данным ЦБ РФ, календарный 2021 год характеризовался 773 тысячами эпизодов несанкционированного изъятия денежных средств с клиентских счетов, причем совокупный материальный ущерб достиг отметки 13,6 млрд рублей. Последующий 2022 год продемонстрировал негативную динамику с приростом в 23,5%, достигнув показателя 16,8 млрд рублей при 945 тысячах зарегистрированных инцидентов.

Календарный 2023 год отметился существенной интенсификацией кибернетических атак на банковскую инфраструктуру - зафиксировано свыше 1,2 млн попыток несанкционированного проникновения в банковские системы. Объем предотвращенного ущерба составил приблизительно 42 млрд рублей, превысив аналогичный показатель 2022 года на 35%. Существенно возросла результативность защитных механизмов - процент успешно отраженных атак достиг 84%.



Рисунок 1 – Динамика объема хищений в банковском секторе

Анализ первого полугодия 2024 года свидетельствует о трансформации характера кибернетических угроз – наблюдается значительное увеличение числа целенаправленных атак на системообразующие кредитные организации (прирост составил 47% относительно аналогичного периода 2023 года). Среднестатистический ущерб от единичной успешной атаки возрос до 3,2 млн рублей [1, С 23].

Детальный анализ векторов кибернетических атак в период 2021-2024 годов демонстрирует устойчивое доминирование методов социальной инженерии, составляющих почти две трети (63%) от общего числа зафиксированных инцидентов. Второе место в структуре угроз занимают

фишинговые кампании (18%), за которыми следуют распределенные атаки типа "отказ в обслуживании" (12%) и различные варианты вредоносных программных продуктов (7%). Исследование выявляет значительное усложнение технического инструментария злоумышленников – частота использования многоуровневых атакующих механизмов продемонстрировала прирост в 156% за исследуемый временной интервал.

Аналитические материалы ФинЦЕРТ свидетельствуют о кардинальной трансформации географической локации источников кибернетических угроз: если в 2021 году зарубежное происхождение имели 45% атак, то к 2024 году данный индикатор существенно возрос, достигнув отметки 72%. Особенно заметна интенсификация вредоносной активности со стороны государств Юго-Восточной Азии (увеличение на 234%) и латиноамериканского региона (прирост составил 167%).

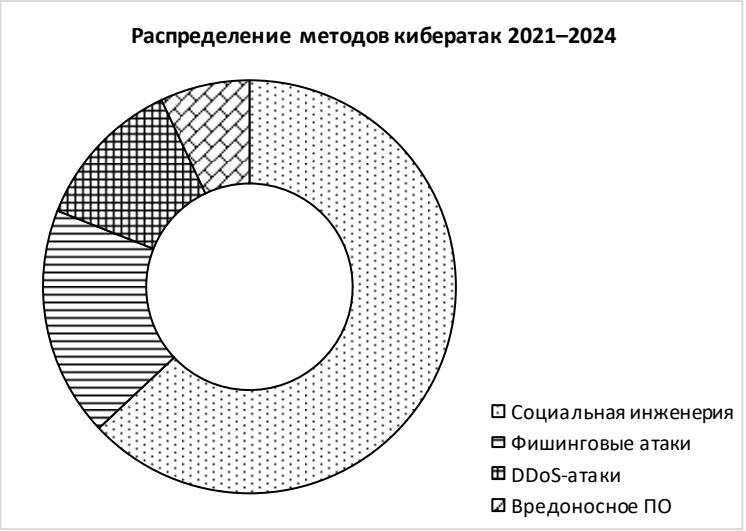


Рисунок 2 – Распределение методов кибератак 2021–2024

Результативность правоприменительной практики в сфере противодействия киберпреступности демонстрирует устойчивый прогресс. Показатель раскрываемости преступлений в банковском секторе увеличился с 27% в 2021 году до 41% к началу 2024 года. Количественный показатель успешно завершенных следственных мероприятий продемонстрировал рост на 52%, при этом средняя продолжительность расследования сократилась с 197 до 134 суток. Финансовый объем

возмещенного ущерба существенно возрос – с 3,2 млрд рублей в 2021 году до 7,8 млрд рублей в 2023 году [2, с. 55].

Эффективное противодействие киберпреступности требует постоянного совершенствования методов выявления и расследования противоправных действий. Важнейшим направлением является развитие системы мониторинга и анализа подозрительных транзакций с использованием технологий искусственного интеллекта.

Существенное значение имеет межведомственное взаимодействие правоохранительных органов, служб безопасности банков и регулятора. Создание единых информационных систем и баз данных позволяет повысить эффективность выявления и расследования киберпреступлений.

Особую роль играет международное сотрудничество в сфере противодействия киберпреступности. Трансграничный характер многих преступлений требует координации усилий правоохранительных органов разных стран, обмена информацией и опытом.

Совершенствование нормативно-правовой базы должно учитывать появление новых видов киберугроз и способов совершения преступлений. Требуется регулярная актуализация составов преступлений и санкций за их совершение [5, с. 128].

Фундаментальным компонентом архитектуры кибернетической безопасности выступает превентивная деятельность по предотвращению противоправных действий. Кредитно-финансовые учреждения несут обязательства по систематическому повышению квалификации сотрудников в области информационной защищенности и противодействия методам социально-инженерного воздействия.

Существенным аспектом превентивной деятельности является планомерное повышение финансовой образованности и осведомленности клиентской базы относительно потенциальных кибернетических угроз. Банковские структуры призваны осуществлять систематическое информирование пользователей о принципах безопасной эксплуатации дистанционных сервисов и эффективных механизмах противодействия мошенническим схемам.

Принципиальное значение приобретает совершенствование комплексной системы раннего обнаружения потенциальных угроз кибербезопасности. Оперативный обмен информационными данными между финансовыми институтами относительно идентифицированных попыток несанкционированного доступа способствует предотвращению распространения вредоносной активности на иные организации сектора.

Эффективная профилактика киберпреступности требует имплементации интегрированного подхода, охватывающего технологические, организационно-управленческие и нормативно-правовые ин-

струменты. Ключевую роль в превентивной деятельности играет налаженное взаимодействие банковских структур с правоохранительными органами в сфере предупреждения противоправных действий.

Процесс технологической модернизации защитных механизмов должен осуществляться параллельно с совершенствованием законодательной базы и оптимизацией организационных процедур. Исключительно комплексная стратегия способна обеспечить результативное противодействие современным кибернетическим угрозам в банковско-финансовом секторе [6].

В заключение следует отметить, что обеспечение кибербезопасности банковского сектора требует постоянного совершенствования правовых механизмов и практических мер защиты. Развитие технологий приводит к появлению новых угроз, что требует своевременной актуализации нормативной базы и методов противодействия киберпреступности.

Эффективная защита банковского сектора от киберугроз возможна только при условии тесного взаимодействия всех заинтересованных сторон: банков, регулятора, правоохранительных органов и клиентов. Комплексный подход к обеспечению кибербезопасности должен включать как технические, так и правовые механизмы защиты.

Список цитируемой литературы:

1. Лопатин, В.Н. Правовые риски информационной безопасности для банков и их клиентов / В.Н. Лопатин // Право и цифровая экономика. – 2023. – № 2. – С. 23–31.
2. Савельев, А.И., Петров, М.В. Кибербезопасность банковского сектора России: правовое регулирование и практика применения / А.И. Савельев, М.В // Вестник Московского университета. Серия 11: Право. – 2024. – № 1. – С. 45–58.
3. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ (в ред. от 10 июля 2023 г.) // Собрание законодательства Российской Федерации. – 2017. – № 31. – Ч. I. – Ст. 4736.
4. Карпова Д.Н., Сидоренко Э.Л. Правовые механизмы противодействия киберпреступности в банковской сфере: монография. – М.: Проспект, 2022. – 256 с. ISBN 978-5-392-35647-8.
5. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России за 2023 год [Электронный ресурс]. – Официальный сайт Банка России. – URL: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения: 09.01.2025).

Толочко А.В., канд. полит. наук, доцент, доцент кафедры
ФГБОУ ВО «Липецкий государственный технический университет»,
г. Елец

Толочко Н.С., преподаватель
ГБПОУ «Елецкий колледж инновационных технологий»,
г. Елец

СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ КАК СРЕДСТВА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Аннотация

В статье делается попытка анализа современных информационно-коммуникационных технологий в системе образования, которые представляют собой комплекс сложных информационных взаимосвязей, которые присутствуют в процессе изучения коммуникационных каналов. Они существуют как при применении классических методов поиска, обработки, хранения и передачи информации, так и при внедрении новых компьютерных технологий и выступают средством противодействия киберпреспупности в молодежной среде.

Ключевые слова: ИКТ; дистанционные технологии; мобильное обучение; тренинговые технологии; кейс-технологии.

Применение информационно-коммуникационных технологий в образовательном процессе играют положительную роль.

Большое количество трактовок в педагогической науке имеют понятия «ИКТ», «компьютерные технологии» и «информационные технологии». Их применение зависит не только от сущности представленного явления, но и от контекста, в котором они используются. В работах И.Г. Захаровой [3], Е.С. Полат [5], И.В. Роберт [6], М.П. Лапчик [4] и др. подробно представлены данные понятия и вопросы, связанные с ними. В настоящее время термин «ИКТ» заменил используемые ранее использовавшийся термин «информационные технологии» в научно-педагогической литературе [7, с. 26].

ИКТ выполняют пять ключевых функций в образовательном процессе:

1. Обучающая функция – изучение и закрепление нового материала, объяснение нового материала с помощью иллюстраций, проведение практических занятий, контроль и самообразование.

2. Воспитывающая функция – воспитание личностных и нравственных качеств обучающихся и др.

3. Развивающая функция – формирование творческих и интеллектуальных способностей и др.

4. Познавательная функция – получение данных, установление информационных связей и др.

5. Мотивирующая функция – объяснение через жизненный опыт целесообразности изучения материала, побуждение учащихся к достижению поставленной цели и др. [8, с. 67].

Различают следующие аспекты пользования ИКТ в образовательном процессе:

1. Учебно-методический аспект. В качестве учебно-методического обеспечения учебного процесса применяются информационные и электронные ресурсы.

2. Содержательный аспект. ИКТ могут быть использованы для создания тестов, таблиц, диаграмм, иллюстраций, тренажеров, интерактивных домашних заданий по темам и разделам учебного предмета, как для групповой работы учеников, так и самостоятельной.

3. Организационный аспект. ИКТ применяются как при фронтальной или групповой работах, так и при обучении на основе определенного плана в соответствии с индивидуальной программой каждого учащегося.

4. Мотивационный аспект. При использовании ИКТ возможен выбор форм, содержания и темпа проведения урока.

5. Контрольно-оценочный аспект. «Тестовые задания, которые позволяют реализовывать различные виды контроля, являются в ИКТ ключевым средством оценки и контроля образовательных результатов» [9, с. 1136].

Электронные учебные пособия содержат в себе большое количество учебных и наглядных материалов и содействуют развитию качественно новых методов обучения, что значительно обогащают классические формы обучения. Электронный учебник отличается от печатного и имеет ряд отличительных особенностей – это наличие гипертекста, гипермедиа, аудио- и видео-лекций, практических и тестовых заданий. Учитель может легко адаптировать электронный учебник под свою программу обучения, изменить некоторые его части или объединить несколько электронных пособий в одно. В любое время можно передать учебник ученикам, отправив его по электронной почте.

Интерактивная доска представляет собой сенсорный экран, подключенный к компьютеру, с которого проектор передает изображение на доску. Специальное программное обеспечение дает возможность работать с текстами, объектами, аудио- и видеоматериалами, Интернет-ресурсами. На доске, возможно, разместить большое количество информации разного

плана. Тактильное управление облегчает восприятие новой информации, что выводит визуальную составляющую процесса обучения на гораздо более высокий уровень. Интерактивная доска предлагает уникальные возможности для работы и творчества учителя и ученика.

Мультимедийная презентация – это самый доступный и распространенный способ ярко и наглядно представить учебный материал. Презентация может включать в себя тексты, аудио- и видеофрагменты, схемы, тесты и практические задания, работу с которыми можно организовать как во фронтальном взаимодействии со всем классом, так и в парной или групповой работе. Педагоги и учащиеся выступают авторами презентаций. В первом случае презентация является средством эффективной подачи нового материала, во втором – формой самостоятельной творческой деятельности.

На современном этапе ИКТ совершенствуются, на новый уровень выходят традиционные технологии, появляются новые технологии в педагогике. Среди новых технологий можно выделить: дистанционные технологии, тренинговые технологии, мобильное обучение [2] и case-технологии.

Дистанционные образовательные технологии (ДОТ) – это образовательные технологии, которые реализуются преимущественно с использованием информационно-телекоммуникационных технологий при опосредованном (на расстоянии) или частично опосредованном взаимодействии обучающегося и преподавателя. Предоставление учащимся доступа к качественному изучения учебных дисциплин независимо от места жительства или временного пребывания ученика, его состояния здоровья и социального статуса является целью применения ДОТ учебными заведениями.

ДОТ применяются как при дистанционном обучении, так и в традиционном образовательном процессе. Они осуществляются в работе с обучающимися в ходе проведения семинаров, консультаций, аудио- и видеоконференций, удаленных встреч и экскурсий и др. ДОТ могут быть применены при организации самостоятельной работы учащихся.

Среди преимуществ ДОТ можно выделить: гибкость, доступность, вариативность и массовость обучения; отсутствие временных и географических границ; равные возможности получения образования независимости от статуса человека; обучение по индивидуальным учебным планам; возможность обучения людей с инклюзией; оптимизация работы учителя; повышение уровня ИКТ-компетенции и др. Образовательный процесс с помощью ДОТ становится открытым, технологичным, нацеленным на формирование информационно-коммуникационных компетенций обучающихся.

Тренинговые технологии – это комплекс различных методов и приемов, направленные на формирование у обучающегося определенных навыков и умений [1, с. 306]. Тренинг в методике обучения представляет собой планомерный процесс совершенствование ЗУН обучаемого.

Тренинг имеет ряд значительных отличий от классической формы обучения. Традиционное обучение больше направлено на правильность ответа и является формой передачи информации и приобретения знаний. Тренинговые технологии сосредоточены на постановке вопросов и поиске ответов. Тренинг всецело охватывает потенциал обучающегося, в отличие от традиционных форм обучения.

Мобильное обучение представляет собой форму организации образовательного процесса, в основе которой лежит использование мобильных ИКТ и беспроводной связи. Особое внимание уделяется мобильности обучающихся и их взаимодействию с портативными устройствами, такими как мобильные телефоны, планшеты, карманные персональные компьютеры, персональные аудиоустройства и др. Устройства многофункциональны. Они поддерживают чтение, письмо, разговорную речь, воспроизведение аудио- и видеоматериалов, поиск информации, выполнение вычислений, выход в Интернет, геймификацию и т.п. Выбор устройства зависит от возраста и местонахождении учащегося, целей и задач обучения и иных факторов.

Основными преимуществами применения мобильного обучения являются: простота размещения мобильных устройств в классе по сравнению со стационарными компьютерами; использование мобильных устройств в любом месте и в любое время; визуализация обучения, позволяющая активно применять интерактивные наглядные пособия; мобильные устройства легче и занимают меньше места, чем учебники и тетради. Благодаря современным беспроводным технологиям возможна передача учебного материала между пользователями. Педагоги и обучающиеся могут вырезать, копировать и редактировать текст, отправлять данные по электронной почте, работать совместно и передавать устройства внутри группы. Мобильное обучение дает возможность получать образование людям с ограниченными возможностями здоровья и др. [2, с. 242].

Кейс-технология – это интерактивная технология обучения, направленная на развитие у обучающихся ЗУН и личностных качеств на основе анализа и решения реальной или смоделированной проблемной ситуации, представленной в виде кейса.

Кейс-технология является активным методом обучения. К его преимуществам относятся: применение принципов проблемного обучения; приобретение навыков решения различных проблемных ситуа-

ций; развитие навыков групповой деятельности; развитие коммуникативных навыков; повышение мотивации к обучению и др.

Данная технология ориентирована на формирование у обучаемых свободного мышления, умения высказать собственное мнение, слушать и учитывать альтернативную точку зрения. Кейс-технология дает возможность проявить и улучшить свои аналитические и оценочные навыки и находить наиболее правильное решение сложившейся проблемы.

Таким образом, современные ИКТ повышают качество обучения и образования, помогают обучающимся получать новые знания в области информационных ресурсов и новых компьютерных технологий, что дает им возможность лучше ориентироваться в информационной и компьютерной среде. Они позволяют более эффективно и быстро адаптироваться к происходящим социальным изменениям.

Современные ИКТ предоставляют дополнительные возможности для формирования и развития информационно-коммуникативной компетенции, которая вместе с компьютерной грамотностью помогает противостоять кибермошенничеству и киберпреступлениям в целом. Активное и эффективное внедрение этих технологий в образовательный процесс является важным фактором создания системы образования, отвечающей требованиям информатизации образования.

Список цитируемой литературы:

1. Ахмадова, Т.Х, Озиева, С.С., Цороев, С.С. Особенности использования тренинговых технологий в профессиональном образовании студентов / Т.Х. Ахмадова, Л.С. Озиева, С.С. Цороев // Мир науки, культуры, образования. – 2020. – № 2 (81). – С. 306–308.
2. Голицына, И.Н., Половникова, Н.Л. Мобильное обучение как новая технология в образовании / И.Н. Голицына, Н.Л. Половникова // Образовательные технологии и общество. – 2011. – Т. 14. – № 1. – С. 241–252.
3. Захарова, И.Г. Информационные технологии в образовании: учебное пособие / И.Г. Захарова. – Москва: Изд. центр «Академия», 2011. – 188 с.
4. Лапчик, М.П. Информатика и информационные технологии в системе общего и педагогического образования: Ист.-методол. аспект / М.П. Лапчик. – Омск: Изд-во Ом. гос. пед. ун-та, 1999. – 295 с.
5. Новые педагогические и информационные технологии в системе образования: учебное пособие / под ред. Е.С. Полат. – Москва: Академия, 2009. – 268 с.
6. Роберт, И.В. Современные информационные и коммуникационные технологии в образовании / И.В. Роберт // Информатика и образование. – 1997. – № 4. – С. 87−90.

7. Розина, И.Н. Педагогическая компьютерно-опосредованная коммуникация: теория и практика / И.Н. Розина. – Москва: Логос, 2005. – 456 с.
8. Шкильменская, Н.А. Основные функции современных информационно-коммуникационных технологий в условиях гуманитаризации образования / Н.А. Шкильменская // Известия Российского государственного педагогического университета им. А. И. Герцена. – 2009. – № 83. – С. 58–69.
9. Ямалетдинова, А.М. Современные информационные и коммуникационные технологии в учебном процессе / А.М. Ямалетдинова, А.С. Медведева // Вестник Башкирского университета. – 2016. – № 4. – С. 1134–1140.

Уздемир А.Н., магистрант
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Научный руководитель – Чуносов В.С., канд. юрид. наук, доцент
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Основные риски и предупреждение кибератак в банковском секторе

Аннотация

В статье рассматриваются основные риски и методы предупреждения киберпреступлений в банковском секторе. Анализируется роль государственных органов при регулировании защиты финансовых организаций от киберугроз. Выявляется причинно-следственная связь между видами кибератак и развитием информационных технологий.

Ключевые слова: банковский сектор, киберриск, информационная система, кибератака.

Современность характеризуется серьезными проблемами безопасности банковского сектора в онлайн-пространстве, поскольку большинство транзакций осуществляется через платформы цифровых платежей.

Специалисты выделяют три основных киберриска в банковском секторе. Первый риск – неправомерный доступ к информации путем различных способов взлома данных. Второй киберриск – это получе-

ние доступа к личной информации посредством мобильных приложений, в случае если пользователь не защитил свое устройство дополнительным программным обеспечением. Третьим риском является несанкционированный доступ к криптовалюте, поскольку многие децентрализованные рынки не имеют надлежащей защиты этого относительно нового явления финансовой действительности. Построение систем управления описанными киберрисками важно для всех организаций банковской сферы, поскольку современность обуславливает необходимость защиты денежных средств с точки зрения цифровых технологий.

Общество все больше претерпевает влияние кибератак, которые становятся сложнее, поскольку киберпреступники постоянно совершенствуют свои методы для обхода систем безопасности. Финансовые учреждения наиболее часто сталкиваются с фишингом – замаскированные под официальные письма от банка сообщения, с целью получения доступа к личным данным. Такие атаки часто используют социальную инженерию, убеждая пользователей раскрыть информацию. Второй вид кибератаки может происходить, когда клиент подключается к открытому Wi-Fi и заходит в свой интернет-банкинг, где злоумышленник перехватывает связь и получает возможность управлять данными пользователя. DDoS-атаки направлены на перегрузку серверов банка огромным количеством запросов, что приводит к недоступности сервисов для клиентов, отвлекая тем самым службы безопасности, пока может происходить другое киберпреступление, например несанкционированная транзакция через другой канал. Еще одним видом кибератак является шпионское программное обеспечение, при котором злоумышленники внедряют вредоносные программы на устройства пользователей для отслеживания и сбора конфиденциальных данных. Одна из наиболее опасных угроз – утечка персональных данных клиентов. Эти данные могут включать имена, адреса, номера счетов, карты и другую чувствительную информацию. Утечки могут происходить как вследствие внешних атак, так и из-за действий инсайдеров.

На данном этапе кибербезопасность одно из системообразующих звеньев жизнеспособности банковской структуры, поскольку это позволяет предотвратить финансовые потери, защитить данные клиентов, сохранить репутацию банка и избежать штрафных санкций регулятора.

В России действуют правила и нормы, направленные на защиту клиентов банков и их вкладов, и, если эти правила нарушаются или игнорируются, банки сталкиваются со штрафными санкциями и отзывом лицензий. Восстановиться после таких событий очень сложно, и будущие клиенты могут усомниться в честности банка, с которым они

сотрудничают. Если банк станет жертвой киберугроз и факты нарушения требований в области защиты данных клиентов станут известны, регулятор может вмешаться и применить санкции в отношении банка. [1, С. 45]

Механизмами защиты финансового учреждения от киберпреступности является обучение сотрудников, включающее информирование обо всех потенциальных угрозах, с которыми они могут столкнуться. Банковское учреждение должно гарантировать знание работников правил защиты от разных тактик взломов данных клиентов. Постоянный мониторинг всех информационных систем и регулярный аудит помогут определить, насколько оперативно работает система безопасности сети, какие элементы сети необходимо обновить, обеспечив защиту от будущих киберугроз.

Банки используют оптимальные решения, которые автоматизируют процесс сканирования и мониторинга транзакций, чтобы фильтровать и блокировать любой подозрительный трафик. Если подозрительная активность обнаружена, определяется ее характер, блокируется доступ к сети и, как следствие, купируются связанные риски, также это позволяет расширять периметр знаний об угрозах.

Страхование киберрисков – еще один действенный механизм защиты финансовой организации. Банки являются одними из самых известных предприятий, действующих по всему миру и ориентированных как на корпоративных клиентов, так и на частных лиц. Чтобы повысить степень защищенности банка от киберугроз, обеспечить стабильность финансовых потоков и возмещение потерь в случае реализации киберрисков, во всем мире используется такой инструмент, как страхование. Полис страховой защиты, покрывающий ущерб от киберрисков, позволяет возместить финансовые и репутационные издержки банка в случае реализации киберрисков, поддержать стабильность и устойчивость банка на рынке. [4, С. 71]

Надзор за киберугрозами в банковской сфере осуществляется на нескольких уровнях, начиная от государственных регуляторов до самих финансовых учреждений. Рассмотрим ключевые аспекты надзора и регулирования в этой области. Среди государственных органов ключевую роль играет Центральный банк Российской Федерации, устанавливая требования к обеспечению информационной безопасности и кибербезопасности, проводит проверки и аудиты, разрабатывает нормативные акты и рекомендации по борьбе финансовых организаций с киберпреступлениями.

Среди его функций: - разработка стандартов и рекомендаций по защите информации;

- проведение проверок соблюдения требований информационной безопасности;

- контроль за выполнением нормативных актов и инструкций;

- координация взаимодействия с другими государственными органами и международными организациями;

Важную роль в обеспечении технической защиты информации в государственных органах и организациях, работающих с государственной тайной играет Федеральная служба по техническому и экспортному контролю. Однако ее компетенции распространяются и на коммерческие структуры, включая банки, когда речь идет о защите критической инфраструктуры. Среди задач данной службы следует отметить: лицензирование деятельности по защите информации, аттестацию объектов информатизации, сертификацию средств защиты информации, мониторинг состояния информационной безопасности.

Также вопросы национальной безопасности в сфере защиты информационных ресурсов контролирует Федеральная служба безопасности Российской Федерации, участвуя в расследовании инцидентов, связанных с кибератаками, оказывая содействие в предотвращении таких угроз.

Важной для банковских структур является работа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, которая занимается контролем за соблюдением законодательства в области обработки персональных данных.

Каждый банк обязан иметь собственную службу информационной безопасности, которая отвечает за мониторинг, анализ и реагирование на инциденты. Среди основных задач внутренней службы следует выделить: разработку и внедрение политики информационной безопасности, проведение регулярных тестов на проникновение и оценки уязвимостей, обучение персонала основам кибербезопасности, анализ и расследование инцидентов.

С целью предупреждения и профилактики киберпреступлений действуют международные стандарты и инициативы. Первым среди таковых является стандарт под названием ISO/IEC 27001. Это международный стандарт управления информационной безопасностью, который применяется многими финансовыми институтами по всему миру. Он определяет требования к созданию, внедрению, поддержанию и постоянному улучшению системы менеджмента информационной безопасности. Вторая программа - PCI DSS (Payment Card Industry Data Security Standard). Стандарт безопасности данных индустрии платежных карт обязательный для всех компаний, обрабатывающих платеж-

ные карты. Банки должны соответствовать требованиям этого стандарта, чтобы обеспечить безопасность операций с картами [2, С. 26].

Третья в списке инициатив – SWIFT CSP (Customer Security Programme). Программа безопасности клиентов SWIFT, направленная на повышение уровня защиты участников финансовой системы, использующих платформу SWIFT для межбанковских переводов и включающая в себя обязательные элементы контроля и регулярные аудиты.

Важно помнить, что профилактика и усиление защиты от киберугроз должны быть регулярными и систематическими, поскольку злоумышленники постоянно совершенствуют свои методы атак. Только таким образом можно обеспечить надежную защиту информационных систем и данных пользователей.

Список цитируемой литературы:

1. Дерюгин, Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы / Р. А. Дерюгин // Вестник Уральского юридического института МВД России. – 2019. – №2. – С. 45.
2. Коломасова, Р.А. Мировые тенденции страхования информационных рисков и проблемы его внедрения в российскую практику / Р.А. Коломасова // E-Scio. – 2019. – №6 (33). – С. 21–34.
3. Кумышева, М.К., Геляхова, Л.А. К вопросу о киберпреступности в России и мире / М.К. Кумышева, Л.А. Геляхова // Пробелы в российском законодательстве. – 2018. - №4. – С. 25–26.
4. Просветова, А.А., Дубкова, Е.В. Кибер-страхование как способ обеспечения информационной безопасности / А.А.Просветова, Е.В. Дубкова // Международный журнал гуманитарных и естественных наук. – 2020. – №4-3. – С. 70–72.

Утегенова Г.А., аспирант
Кыргызская Республика, Юридического институт
Кыргызского Национального университета имени Ж. Баласагына,
г. Бишкек

Интерактивные развлечения как фактор, способствующий семейно-бытовому насилию: анализ и меры предупреждения

Аннотация

Статья рассматривает влияние интерактивных развлечений на рост семейно-бытового насилия, исследуя механизмы воздействия виртуального контента на поведение, включая формирование агрессии. Проанализированы вопросы регулирования видеоигровой индустрии для защиты граждан, особенно несовершеннолетних, от потенциального вреда. Предлагаются профилактические меры: нормативное регулирование, просветительские инициативы, системы возрастного контроля. Обоснована необходимость создания единых стандартов и методик оценки, а функцию экспертной оценки предлагается возложить на Управление по борьбе с киберпреступностью Российской Федерации, что позволит укрепить общественную безопасность и систематизировать развитие отрасли.

Ключевые слова: интерактивные развлечения, семейно-бытовое насилие, видеоигровая индустрия, регулирование, профилактика, киберпреступность.

В современную эпоху цифровизации и стремительного распространения интерактивных технологий, таких как видеоигры, виртуальная реальность и геймерские приложения, интерактивные развлечения стали неотъемлемой частью повседневной жизни миллионов людей. Вышеуказанные формы досуга открывают новые возможности для самовыражения, обучения и общения, однако их влияние на социальное поведение и семейно-бытовые отношения все еще актуальна [1]. Одной из таких проблем является возможная связь интерактивных развлечений с формированием агрессивного поведения, которое может проявляться в форме семейно-бытового насилия.

Популярность интерактивных развлечений, включающих элементы насилия, реалистичных конфликтов и соревнований, могут влиять на восприятие агрессии [2]. Тем самым вызывая необходимость анализа их роли в формировании динамики семейно-бытовых конфликтов. Несмотря на существующие исследования в области психологии и криминологии, правовые аспекты данной проблемы до сих пор оста-

ются недостаточно изученными. Особый интерес представляет вопрос о том, каким образом виртуальная агрессия, потребляемая в цифровой среде, может оказывать влияние на реальное поведение пользователей в семейно-бытовой среде.

Данное исследование предлагает комплексный подход к изучению связи между интерактивными развлечениями и семейно-бытовым насилием. В нем объединяются криминологический, правовой и социальный анализ, позволяющий глубже понять механизмы влияния цифровых технологий на поведение людей. Важной частью работы является разработка мер предупреждения как для пользователей, так и для разработчиков интерактивного контента. В рамках исследования также рассматриваются перспективы совершенствования законодательства, направленного на регулирование геймерских продуктов, которые могут способствовать агрессивному поведению.

Понимание воздействия интерактивных развлечений на семейно-бытовые отношения и разработка эффективных механизмов профилактики играет ключевую роль в укреплении семейных ценностей и устойчивости социальной среды. Исследование данной научной темы на наш взгляд поможет создать условия для минимизации влияния интерактивного развлечения в семейно-бытовой сфере, а также послужит основой для разработки нормативно-правовых и организационных стратегий, направленных на снижение уровня семейно-бытового насилия в условиях цифровой эпохи.

В современном информационном пространстве нередко появляются сообщения о трагических инцидентах, связанных с насильственными действиями несовершеннолетних, мотивированных их вовлеченностью в геймерские развлечения. Особенно остро общество реагирует на случаи, когда подростки совершают тяжкие преступления, включая убийства, под влиянием игровой зависимости или конфликтов, связанных с ограничением доступа к интерактивным технологиям [3,4,5].

Подобные трагедии поднимают вопросы о необходимости изучения влияния интерактивных развлечений на психоэмоциональное состояние несовершеннолетних и их способность адекватно регулировать свое поведение в стрессовых ситуациях. Более того, актуальной становится разработка мер профилактики игровой зависимости, которая в некоторых случаях становится триггером для агрессивных действий.

При анализе данной тематики в научном мире выделяются две основные теории, объясняющие влияние насилия в интерактивных играх на пользователей. Первая теория утверждает, что интерактивные игровые платформы могут способствовать повышению уровня насилия, так как они формируют у игроков навыки агрессивного поведения

и усиливают предрасположенность к насилию у тех, кто уже имеет склонность к подобным действиям [6].

Вторая теория предполагает противоположное: игроки используют жестокие интерактивные развлечения как способ выплеснуть агрессию, что помогает снизить уровень напряжения и даже положительно влияет на их психическое здоровье [6].

Обе теории остаются предметом активных дискуссий. Например, аналитический ресурс ProCon.Org провел сравнительный анализ аргументов за и против теории о том, что насилие в игровых платформах способствует агрессивному поведению. Результаты показали равное количество аргументов – девять в поддержку этой идеи и девять против [7].

Интересно, что научные исследования по этому вопросу зачастую дают противоречивые результаты. Одни работы показывают связь между видеоиграми с элементами насилия и ростом агрессии среди игроков, тогда как другие исследования демонстрируют обратное: видеоигры могут способствовать развитию эмпатии и просоциального поведения у пользователей [8,9].

Интерактивные развлечения часто оказываются в центре общественной критики, особенно в контексте трагических событий, таких как стрельба в Ижевской школе [10]. В данном случае в 2022 году Министерство просвещения Российской Федерации инициировало обсуждение совместно с Министерством цифрового развития вопроса о необходимости регулирования интерактивных игр. Высказываются предположения, что такие меры могут включать ограничение доступа к отдельным жанрам игр или даже более радикальные шаги, вплоть до полного запрета шутеров. Данные инициативы вновь поднимают важный вопрос: насколько оправдано возложение ответственности за насильственные действия на интерактивные развлечения [10].

Тем самым, 12 декабря 2024 года в Государственную Думу Российской Федерации был внесен проект закона, направленный на регулирование видеоигровой индустрии. Проект предусматривает обязательную маркировку видеоигр по содержанию, включая сцены насилия, употребление алкоголя, наркотиков и нецензурную лексику, с учетом интересов не только несовершеннолетних, но и чувствительных категорий граждан, таких как пожилые люди. Законопроект вводит ключевые термины, такие как «видеоигра», «игровое имущество» и «распространитель видеоигр», что создает базу для дальнейшего правового регулирования этой сферы [11].

Кроме того, предусмотрены меры по информированию пользователей о содержании игр, установлению возрастных категорий и введе-

нию требований для распространителей, включая публикацию правил совершения платежей, возврата средств и разрешения споров. Также предлагается проводить экспертную оценку содержания видеоигр аккредитованными специалистами для минимизации возможного вреда здоровью пользователей, особенно несовершеннолетних [11].

Законопроект предполагает адаптацию национальной системы маркировки к международным стандартам, что, по мнению авторов инициативы, будет способствовать развитию отечественной игровой индустрии, защите нравственности и прав граждан.

В данном аспекте, авторы отмечают, что инициатива проведения экспертной оценки содержания видеоигр аккредитованными специалистами для минимизации возможного вреда здоровью пользователей, особенно несовершеннолетних, представляет собой важный шаг в регулировании видеоигровой индустрии. Однако необходимо отметить, что предлагаемые меры не являются полностью достаточными. Одной из ключевых проблем является отсутствие четких механизмов контроля за процессом проведения экспертиз, что может снизить их эффективность.

Экспертиза, как предполагается, должна выявлять потенциально опасный контент, включая сцены насилия, употребление алкоголя, наркотиков, а также нецензурную лексику, чтобы обеспечить защиту интересов граждан, особенно детей. Однако без прозрачного процесса аккредитации экспертов и постоянного мониторинга их работы существует риск субъективности, а также несоответствия оценок реальным рискам. Кроме того, нет гарантий, что выявленные нарушения повлекут за собой оперативное принятие мер, таких как внесение изменений в игру или ограничение ее распространения.

Также отсутствие четко прописанных стандартов и процедур экспертизы может привести к разногласиям между разработчиками, распространителями и экспертами, что в свою очередь осложнит внедрение новых требований. Они также указывают на необходимость создания независимой системы контроля, которая будет оценивать качество и объективность проведенных экспертиз.

Для решения проблемы регулирования содержания видеоигр предлагаются следующие меры:

1. Разработка нормативных актов. Необходимо создать детализированные нормативные документы, регулирующие процесс проведения экспертиз видеоигр. Они должны содержать четкие критерии оценки контента, включая сцены насилия, употребление алкоголя и наркотиков, а также механизмы отчетности по результатам экспертизы. Тем самым позволяя обеспечить единообразие и прозрачность оценки.

2. Внедрение системы общественного мониторинга. Предлагается создать систему общественного мониторинга и регулярно обновлять методики экспертизы с учетом новых вызовов и тенденций в индустрии видеоигр. Такой подход обеспечит адаптацию законодательства к быстро меняющейся реальности цифрового контента.

3. Передача функций мониторинга Управлению по борьбе с киберпреступностью Российской Федерации. Функцию мониторинга и экспертной оценки видеоигр целесообразно возложить на Управление по борьбе с киберпреступностью Российской Федерации. Данная структура обладает значительным опытом в анализе цифрового контента, включая выявление потенциально вредоносной информации. Делегирование данных обязанностей позволит использовать существующие механизмы контроля и мониторинга для эффективной оценки содержания видеоигр.

В заключение следует отметить, что передача функций проведения экспертиз содержания видеоигр специализированному ведомству обеспечит прозрачность процесса и минимизирует риски возникновения конфликта интересов. Управление по борьбе с киберпреступностью сможет разработать единые стандарты и методики оценки, что гарантирует объективность, сопоставимость и высокий уровень профессионализма при анализе видеоигр.

Таким образом, делегирование функции экспертной оценки Управлению по борьбе с киберпреступностью Российской Федерации создаст надежную основу для системного подхода в регулировании видеоигровой индустрии. На наш взгляд данная инициатива позволит защитить права и интересы граждан, особенно несовершеннолетних, а также будет способствовать укреплению семейных ценностей, общественной безопасности и поддержанию правопорядка в условиях цифровой эпохи.

Список цитируемой литературы:

1. Ельникова, О.Е., Комлик, Л.Ю., Фаустова, И.В. Компьютерные игры как фактор агрессивности студентов в эпоху цифровизации / О.Е. Ельникова, Л.Ю. Комлик, И.В. Фаустова // Мир науки. Педагогика и психология. – 2021. – № 3. [Электронный ресурс]. – URL: https://mir-nauki.com/PDF/05PSMN321.pdf (дата обращения: 06.12.2024).

2. Попов, В.А., Валькова В.С. Влияние компьютерных игр на уровень агрессивности подростков / В. А. Попов, Л. С. Валькова. // Молодой ученый. – 2014. – № 7 (66). – С. 279–281. [Электронный ресурс]. – URL: https://moluch.ru/archive/66/11076/ (дата обращения: 06.12.2024).

3. Сын убил отца из-за компьютерной игры «Готика». 14 апреля 2010 г. [Электронный ресурс]. – Life.ru.: сетевое издание. – URL: https://life.ru/p/20754 (дата обращения: 06.12.2024).
4. В Челябинской области 15-летний подросток зарезал свою мать, которая запретила ему онлайн-игры. 5 октября 2015 г. [Электронный ресурс]. – Первый канал: официальный сайт. – URL: https://www.1tv.ru/news/2015-10-05/9937-v_chelyabinskoy_oblasti_15_letniy_podrostok_zarezal_svoyu_mat_kotoraya_zapretila_emu_onlayn_igry (дата обращения: 06.12.2024).
5. Мальчик зарубил мать, чтобы свободно играть в компьютерные игры. 7 ноября 2024 г. [Электронный ресурс]. – Дзен: российская блог-платформа – URL: https://dzen.ru/a/ZyyCgeqWahH72naH#malchik_ybil_mat_prichin_chto_izvestno (дата обращения: 06.12.2024).
6. Холл, Р.К.У., Дэй, Т. Призыв к осторожности: жестокие видеоигры, Верховный суд и роль науки / Р.К.У. Холл, Т. Дэй // MayoClinicProceedings. – 2011. – Т. 86. – С. 315.
7. Видеоигры. Способствуют ли жестокие видеоигры насилию среди молодежи? [Электронный ресурс]. – Онлайн-версия «Британской энциклопедии». – URL: https://www.britannica. com/procon/video-games-debate (дата обращения: 08.12.2024).
8. Entertainment Software Association. Основные факты об индустрии компьютерных и видеоигр. [Электронный ресурс]. – URL: https://www.theesa.com/wp-content/uploads/2024/02/2022-Essential-Facts-About-the-Video-Game-Industry.pdf (дата обращения: 08.12.2024).
9. American Psychological Association. Обзор APA подтверждает связь между игрой в жестокие видеоигры и агрессией. – [Электронный ресурс]. – URL: https://www.apa.org/news/press/releases/2015/08/violent-video-games (дата обращения: 08.12.2024).
10. Министр просвещения РФ считает, что компьютерные игры виноваты в сегодняшней стрельбе в ижевской школе [Электронный ресурс]. – Shazoo.ru: русскоязычный новостной веб-сайт. – URL: https://shazoo.ru/2022/09/26/132883/ministr-prosveshheniia-rf-scitaet-cto-kompiuternye-igry-vinovaty-v-segodniasnei-strelbe-v-izevskoi-skole (дата обращения: 08.12.2024).
11. В Госдуму внесли проект о маркировке видеоигр [Электронный ресурс]. – РИА Новости. – URL: https://ria.ru/20241212/gosduma-1988834607.html (дата обращения: 20.12.2024).

Утузикова Т.А., магистрант
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Уральский институт управления – филиал, г. Екатеринбург

ПРОФИЛАКТИКА И ПРЕДУПРЕЖДЕНИЕ КИБЕРПРЕСТУПЛЕНИЙ СРЕДИ МОЛОДЕЖИ: РОЛЬ ГОСУДАРСТВЕННОЙ МОЛОДЕЖНОЙ ПОЛИТИКИ

Аннотация

В данной статье рассматривается актуальная проблема киберпреступности среди молодежи, связанная с активным использованием цифровых технологий и интернета. Автор подчеркивает важность профилактики и предупреждения таких преступлений, акцентируя внимание на необходимости повышения уровня цифровой грамотности молодежи и формировании культуры кибербезопасности. В статье предлагается внесение изменений в статью 272 УК РФ. Рассмотрены существующие образовательные программы, направленные на развитие навыков цифровой гигиены и информирование молодежи о рисках в сети-интернет. Подчеркивается роль государственной молодежной политики в профилактике киберпреступлений через образование, поддержку инициатив.

Ключевые слова: киберпреступление, государственная политика, молодежная политика, молодежь.

На сегодняшний день, цифровые технологии стали неотъемлемой частью жизни, а особенно для такой категории граждан, как молодежь. Интернет открывает нам множество возможностей, а именно: обучение, общение, развлечение и конечно же саморазвитие. Но стоит отметить, что помимо этого всего возрастает риск столкнуться с киберпреступлениями. Именно поэтому необходимо уделить внимание профилактике и предупреждению таких явлений среди молодежи. Даже самые активные пользователи интернет-ресурсов могут не осознавать угрозы, складывающиеся в цифровой среде. Кибербуллинг, онлайн-мошенничество, хакерские взломы — это лишь небольшая часть проблем, с которыми можно столкнуться.

По данным Министерства внутренних дел Российской Федерации, за последние 5 лет число противоправных деяний в киберпространстве увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и составляет около 40 процентов. То есть почти каждое второе преступление [1].

Именно поэтому вопрос о профилактике и предупреждению киберпреступлений актуален. Цель профилактики заключается в том, чтобы не только уберечь молодежь от угроз, но и донести информацию о последствиях. Ведь развитие технологий опережает законы, что создает правовые пробелы, которыми могут воспользоваться киберпреступники. Молодежь зачастую не осознает юридических последствий своих действий.

В качестве примера рассмотрим ситуацию, которая произошла в 2016 году в Новосибирске. Несовершеннолетний получил доступ к системе школьного электронного журнала и решил исправить оценки себе и пару одноклассникам. Подросток не осознавал, что его действия попадают под уголовную ответственность, а именно ст. 272 Уголовного кодекса Российской Федерации [2]. Максимальное наказание по такому обвинению составляет 2 года. Следовательно, школьник, не задумываясь о последствиях попал под уголовную ответственность. Следствие длилось 2 года, но по итогу в действиях школьника не нашли состав преступления.

Так, по словам прокурора, модифицируя охраняемую законом информацию, то есть исправляя отметки в журнале, школьник не нарушил конституционные права потерпевших. Кроме того, его действия не повлияли на итоговые оценки учеников. Всего бывший ученик городской гимназии №5 исправил 51 отметку: помимо своих, он изменил оценки нескольких одноклассников, попросивших его об этом. Однако все оценки были восстановлены [3].

Подобные ситуации показывают необходимость внесения уточнений в законодательство для разделения умышленных и неумышленных действий. Именно поэтому предлагаю дополнить статью 272 УК РФ, а именно добавить часть 5, которая будет звучать следующим образом: «Если деяние, предусмотренное настоящей статьей, совершено лицом, не достигшим восемнадцатилетнего возраста, суд может учитывать возраст, уровень осознания последствий преступления, а также возможность исправления без применения лишения свободы». Считаю, что необходимо добавить эту специальную норму для несовершеннолетних по следующим основаниям.

Во-первых, приведённая выше поправка соответствует принципам гуманизации, поскольку будет не только наказание, но и исправление, что особенно важно в отношении несовершеннолетних граждан.

Во-вторых, снижение рецидива преступления. Так, несовершеннолетний сможет осознать свои действия и пройти исправительные курсы вместо лишения свободы, что в дальнейшем может уменьшить вероятность повторных преступлений.

В-третьих, учет индивидуальных характеристик и обстоятельства каждого дела, т.е. целенаправленно ли совершили преступление или нет.

Именно поэтому необходимо внести изменения, чтобы повысить гибкость правоприменения и достижения целей справедливого и гуманного наказания.

Что касаемо профилактики преступлений, то здесь необходимо отметить некоторые уже существующие программы, которые направлены на обучение молодежи.

Федеральный проект «Цифровая образовательная среда» направлен на создание и внедрение в образовательных организациях цифровой образовательной среды, а также обеспечение реализации цифровой трансформации системы образования. В рамках проекта ведется работа по оснащению организаций современным оборудованием и развитию цифровых сервисов и контента для образовательной деятельности [4]. Благодаря этой программе молодёжь может повысить уровень цифровой грамотности и быть более осведомлёнными. Так, они могут узнать все о кибергигиене, защите персональных данных, узнают о рисках в интернете.

Следующая программа «Международная Школа Интернет-Безопасности молодежи», которая проводится в образовательном центре Мастерская управления «Сенеж». Именно там молодежь может улучшить свои компетенции в сфере цифровизации и права. Участники могут самостоятельно выбирать секции лекций.

Вышеперечисленные программы способствуют формированию культуры кибербезопасности среди молодежи и готовят новое поколение к безопасной работе в цифровой среде. Но эти программы они носят рекомендательный характер, те желающие могут принять участие.

Какую роль может играть государственная молодежная политика в профилактике киберпреступлений среди группы молодежи? Одна из главных задач – повышение уровня цифровой грамотности. Ведь молодежь должна быть не только активным пользователем, но и осознавать риски, которые связаны с использованием. Кроме того, можно поддерживать различные проектные инициативы, гранты на проведение форума о безопасности, создание центров помощи и поддержки людям, которые столкнулись с кибербуллингом и т.д.

Следовательно, государственная молодежная политика играет немаловажную роль в профилактике киберпреступлений. Поскольку именно через образование, воспитание правосознания, поддержку инициатив и предоставление психологической помощи она помогает формировать у молодежи ответственный подход к цифровому пространству.

Подводя итоги, можно сделать вывод, что тема киберпреступлений среди молодежи требует особого внимания со стороны государства. образовательных учреждений, общественных организаций для повышения цифровой грамотности и профилактики таких видов преступления.

Именно эффективная молодежная политика может существенно снизить уровень киберпреступности, повышая осведомленность молодежи о цифровой безопасности и предлагая альтернативные пути развития в информационной среде. Это способствует формированию законопослушного и осознанного поведения среди молодежи, что, в свою очередь, укрепляет общую цифровую культуру в обществе.

Список цитируемой литературы:

1. За пять лет число киберпреступлений увеличилось более чем вдвое. [Электронный ресурс]. – Российская газета. – URL: https://rg.ru/2024/09/25/policiia-v-seti.html (дата обращения: 15.12.2024).
2.Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 13 декабря 2024 г.) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
3. Новосибирская прокуратура отказалась от преследования юного хакера // Российская газета. – 2019. – 11 фев. [Электронный ресурс]. – https://edu.gov.ru/national-project/projects/cos/https://rg.ru/2019/02/11/regsibfo/novosibirskaia-prokuratura-otkazalas-ot-presledovaniia-iunogo-hakera.html (дата обращения: 16.12.2024).
4.Министерство просвещения. [Электронный ресурс]. – URL: https://edu.gov.ru/national-project/projects/cos/. – (дата обращения: 15.12.2024).

Фалахеева А.Г., аспирант
ФГАОУ ВО «Казанский (Приволжский) федеральный университет»,
г. Казань

Особенности участия защитника по уголовным делам в отношении отдельных категорий лиц

Аннотация

В настоящей работе рассматривается специфика участия защитника в уголовном судопроизводстве в отношении отдельных категорий лиц. Особое внимание уделено правовым гарантиям, являющимся неотъемлемой частью их правового статуса. Исследуются теоретико-практические подходы к методам защиты на различных стадиях и этапах процесса. Автором выдвинуты новаторские суждения и рекомендации, относительно развития тактики адвокатской деятельности при производстве данных дел.

Ключевые слова: адвокат-защитник, специальный субъект, особое производство, отдельная категория лиц.

В российской доктрине уголовного процесса сложилось определенное понимание «специального субъекта» [1, С. 129]. Некоторые ученые к данной дефиниции относят лица, участвующие в особых видах уголовного судопроизводства.

Помимо несовершеннолетних лиц и лиц страдающих психическими расстройствами, закон устанавливает исключения из общего порядка уголовного судопроизводства для широкого круга субъектов, занимающихся публичной деятельностью. Вышеуказанное определено главой 52 Уголовно-процессуального кодекса Российской Федерации (далее - УПК РФ).

Так, в статье 447 УПК РФ обозначены категории лиц, в отношении которых применяется особый порядок производства по уголовным делам. Исходя из положений данной статьи к таким лицам относятся: члены выборных органов законодательной власти (сенаторы Совета Федерации, депутаты Государственной думы, депутаты законодательного (представительного) органа государственной власти субъекта Российской Федерации, депутаты, члены выборных органов местного самоуправления, выборных должностных лиц органов местного самоуправления); судьи (судьи Конституционного Суда Российской Федерации, судов общей юрисдикции, мировых судов субъектов Российской Федерации, а также арбитражных судов Российской Федерации) и присяжные и арбитражные заседатели, в период осуществления ими правосудия; Председатель Счетной палаты Российской Федерации, его

заместитель и аудиторы Счетной палаты Российской Федерации; Уполномоченный по правам человека в Российской Федерации; Президент Российской Федерации, прекративший исполнение своих полномочий, а также кандидат в Президенты Российской Федерации; прокурор; Председатель Следственного комитета Российской Федерации; руководитель следственного органа; следователь; адвокат; член избирательной комиссии, комиссии референдума с правом решающего голоса; а также зарегистрированный кандидат в депутаты Государственной Думы и зарегистрированный кандидат в депутаты законодательного (представительного) органа государственной власти субъекта Российской Федерации. Данный перечень является закрытым. Представляется, что это обусловлено наличием особого правового статуса, который характеризуется специфической ролью в политической, правовой, судебной и избирательной сферах жизни общества. Более того, при общем порядке рассмотрения уголовных дел с участием данных субъектов неизбежно будут нарушены как процессуальный иммунитет - то есть, гарантии предусматривающие неприкосновенность или невмешательство при осуществлении данными субъектами их профильной публичной деятельности, так и базовые принципы уголовного процесса. Вышеназванное может существенно ограничить законные права и свободы указанных лиц.

Так, к примеру, Н.В. Романенко, отметил существенные аспекты уголовного преследования в отношении судей, связав их с гарантией независимости, в число которых включил: «(1) признание функции по отправлению правосудия в качестве основной исключительной конституционной функции уголовно преследуемого судьи; (2) запрет отмены или умаления самостоятельности судов и независимости судей, причинения ущерба репутации судей, оказания давления на них путем уголовного преследования за их профессиональную деятельность; (3) повышенный уровень уголовно-правовой охраны судей как носителей судебной власти; (4) обеспечение независимости уголовно преследуемого судьи; (5) недопущение умаления авторитета правосудия, обеспечение укрепления престижа должности судьи, повышения уровня доверия населения к судебной власти даже в условиях уголовного преследования ее представителей» [2, С. 54-55].

Совершенно оправданным в этом понимании является и система сдержек и противовесов. Гарантия независимости не должна приводить к злоупотреблению властью.

При этом же, в обывательском понимании, происходит некая гиперболизация понятия «независимость». В обществе складывается впечатление о том, что якобы все чиновники злоупотребляют властью,

«отмахиваются служебными удостоверениями» и т.д., что на наш взгляд не является истинным. В действительности, широта гарантии независимости складывается довольно-таки в узком аспекте.

Так, законодательством предусмотрены особенности проведения процессуальных действий на различных стадиях с участием отдельных категорий лиц.

Например, в соответствии с положениями части 1 статьи 448 УК РФ вопрос о возбуждении уголовного дела в отношении отдельных категорий лиц на уровне Российской Федерации решается Председателем Следственного комитета (в некоторых случаях его заместителем), а на уровне субъектов Российской Федерации — руководителем следственного органа соответствующего субъекта. В отношении некоторых лиц, обладающих неприкосновенностью, требуется согласие вышестоящих уполномоченных органов. Так, при возбуждении уголовного дела в отношении сенатора Российской Федерации и депутата Государственной Думы решение принимается Председателем Следственного комитета Российской Федерации с согласия соответственно Совета Федерации или Государственной Думы, полученного на основании представления Генерального прокурора Российской Федерации.

То есть говорить о какой-то невозможности привлечения к уголовной ответственности указанных лиц и о тождественности понятий «независимости» и «освобождения от уголовной ответственности» не приходится.

Это подтверждается и статистикой. Так, к примеру, «в 2023 г. Высшая квалификационная коллегия судей (далее - ВККС) дала согласие на возбуждение уголовных дел в отношении 22 судей» [3, С. 37].

Переходя к самому процессу уголовного судопроизводства в отношении отдельных категорий лиц, стоит упомянуть следующее. Согласно части 1 статьи 140 УПК РФ поводами для возбуждения уголовного дела служат: 1) заявление о преступлении; 2) явка с повинной; 3) сообщение о совершенном или готовящемся преступлении, полученное из иных источников; 4) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании. Основанием для возбуждения уголовного дела в соответствии с частью 2 той же статьи является исключительно наличие достаточных данных, указывающих на признаки преступления. Именно на стадии возбуждения дела защитник приобретает свой статус, вступая в дело.

При этом, не стоит забывать про деятельность адвоката, которая происходит при доследственной проверке сообщения о преступлении. Что и при общем порядке основная задача адвоката здесь - противо-

действие и опровержение доводам органов предварительного расследования. Адвокату необходимо понимать, что этот этап играет «на руку» лицу, участвующему в производстве процессуальных действий при проверке сообщения о преступлении, которое еще не имеет как такового статуса, но «условно подозревается» в совершенном преступлении. У органов предварительного расследования крайне сжаты сроки, в которые они должны принять соответствующее решение.

Так, по статистике, в органах Следственного комитета России, постановление об отказе в возбуждении уголовного дела или о возбуждении уголовного дела принимается на 10-е сутки. То есть изначальный материал принимается и регистрируется в КРСП, в течение 3-х суток следователь не успевает его вовремя «отработать» и в дальнейшем ходатайствует перед руководителем следственного органа о продлении. Более того, процессуальные действия, которые им представляются возможными произвести, в рамках материала проверки, также ограничены (указаны в части 1 статьи 144 УПК РФ).

Однако, не стоит забывать про категорию лиц, которая исследуется в данной работе и про сложность дел связанных с ними. В основном это должностные преступления, которые в действительности трудно расследовать. Так, при необходимости производства документальных проверок, ревизий, судебных экспертиз, исследований документов, предметов, трупов, а также проведения оперативно-розыскных мероприятий руководитель следственного органа по ходатайству следователя, а прокурор по ходатайству дознавателя в соответствии с частью 3 статьи 144 УПК РФ вправе продлить этот срок до 30 суток с обязательным указанием на конкретные, фактические обстоятельства, послужившие основанием для такого продления. Следователю ничего не будет препятствовать продлить срок проверки до 30 суток. Адвокат же должен быть готов все это время активно участвовать и содействовать своему клиенту-доверителю.

В рамках материала проверки органы предварительного расследования также должны установить, относится ли лицо к отдельной категории, о которой речь идет в данной работе. Обычно это можно осуществить в рамках опроса/объяснения, в случаях, если ранее эта информация не была где-либо установлена.

Не менее интересной является и процедура задержания.

В соответствии со статьей 91 УПК РФ орган дознания, дознаватель, следователь вправе задержать лицо по подозрению в совершении преступления, за которое может быть назначено наказание в виде лишения свободы. При этом, сенатор Российской Федерации, депутат Государственной Думы, судья федерального суда, мировой судья, про-

курор, Председатель Счетной палаты Российской Федерации, его заместитель и аудитор Счетной палаты Российской Федерации, Уполномоченный по правам человека в Российской Федерации, Президент Российской Федерации, прекративший исполнение своих полномочий, задержанные по подозрению в совершении преступления в порядке, установленном статьей 91 настоящего Кодекса, за исключением случаев задержания на месте преступления, в соответствии со статьей 449 УПК РФ должны быть освобождены немедленно после установления их личности.

На наш взгляд совершенно оправданной является точка зрения Романенко Н. В. о том, что «не при каждом преступлении лицо можно задержать с поличным» [4, С. 20]. Это является определенным преимуществом, так как основной задачей адвоката-защитника (статус или его отсутствие зависит от того возбуждено ли дело или нет) на этапе задержания и при таких обстоятельствах - доходчиво сообщить органам расследования, что задержанное лицо должно быть незамедлительно освобождено. В случае если это возможно, предоставить доказательства статуса, в котором состоит данное лицо. Если же от органов предварительного расследования исходит отказ от данных действий, адвокату-защитнику необходимо в кратчайший срок официально заявить ходатайство, а в случае отказа в требованиях - написать жалобу в вышестоящий орган.

Стоит понимать, что у отдельных категорий лиц, о которых речь идет в данной работе также не допускается личный досмотр, за исключением случаев, предусмотренных федеральным законом в целях обеспечения безопасности других людей.

Если же лицо застигнуто с поличным на месте совершенного преступления ситуация обстоит несколько сложнее. Здесь необходима выработка определенной линии защиты. Адвокату-защитнику стоит уточнить все обстоятельства, которые подлежат доказыванию, у своего клиента, если такая возможность будет предоставлена. Порядок действий адвокатом-защитником здесь, совершенно аналогичен положениям выработанным тактикой адвокатской деятельности.

Аналогичен порядок действий и при избрании меры пресечения. Здесь, хотя и присутствуют определенные положения, описанные в статье 450 УПК РФ, представляется, что они не столь значимы для защитника и самой защиты, не влекут какой-либо выгоды для подзащитного. Например, в части 2 данной статьи говорится, что судебное решение об избрании в отношении судьи Конституционного Суда Российской Федерации, судей иных судов в качестве меры пресечения заключения под стражу исполняется с согласия соответственно Консти-

туционного Суда Российской Федерации или квалификационной коллегии судей. Так, защитник может предоставить в качестве оправдания своего подзащитного какие-либо собранные доказательства по делу в орган дающий согласие на избрание меры пресечения, но данные попытки представляются нам тщетными.

При проведении следственных мероприятий после возбуждения уголовного дела, адвокат-защитник должен понимать, что неприкосновенность с лица снята. На это лицо продолжает распространяться действие главы 52 УПК РФ, однако по своей сути, существенных отличий от защиты в общем порядке не столь много. Так, в соответствии с частью 1 статьи 450 УПК РФ после возбуждения уголовного дела либо привлечения лица в качестве обвиняемого в порядке, установленном статьей 448 настоящего Кодекса, следственные и иные процессуальные действия в отношении такого лица производятся в общем порядке с изъятиями, установленными статьей 449 настоящего Кодекса и настоящей статьей. В остальном ход дела остается прежним.

При этом, в соответствии с положениями Постановления Пленума Верховного Суда Российской Федерации от 1 июня 2017 года № 19 - О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ) [5] в отношении указанных лиц, разрешение на производство следственных действий, осуществляемых не иначе как на основании судебного решения, может быть дано с учетом положений части 5 статьи 450, статьи 450.1 УПК РФ.

Последним хотелось бы отразить нормы содержащиеся в статье 450.1 УПК РФ. Обыск, осмотр и выемка в отношении адвоката производятся только после возбуждения в отношении адвоката уголовного дела или привлечения его в качестве обвиняемого. В случаях же если уголовное дело было возбуждено в отношении других лиц или по факту совершения деяния, содержащего признаки преступления, в порядке, установленном частью первой статьи 448 настоящего Кодекса, на основании постановления судьи о разрешении производства обыска, осмотра и (или) выемки и в присутствии обеспечивающего неприкосновенность предметов и сведений, составляющих адвокатскую тайну, члена совета адвокатской палаты субъекта Российской Федерации, на территории которого производятся указанные следственные действия, или иного представителя, уполномоченного президентом этой адвокатской палаты. В самом постановлении судьи о разрешении производства обыска, осмотра и (или) выемки в отношении адвоката в соответствии с частью 2 статьи 450.1 УПК РФ указываются данные, служащие основанием для производства указанных следственных дей-

ствий, а также конкретные отыскиваемые объекты. Изъятие иных объектов не допускается, за исключением предметов и документов, изъятых из оборота. В ходе обыска, осмотра и (или) выемки в жилых и служебных помещениях, используемых для осуществления адвокатской деятельности, запрещается изъятие всего производства адвоката по делам его доверителей, а также фотографирование, киносъемка, видеозапись и иная фиксация материалов указанного производства.

Видится, что таким образом, законодатель позаботился о двух аспектах – морально-нравственном и юридическом. Решением введения данных норм, он как защитил профессиональные права адвоката, которые непосредственно связаны с доверием общества, сохранением состязательности процесса, воспрепятствованием произвола со стороны органов предварительного расследования, так и гарантировал неприкосновенность адвокатской деятельности.

Список цитируемой литературы:

1. Шаталов, А.С. Специальные субъекты в уголовном судопроизводстве России: порядок уголовного преследования / А.С. Шаталов // Журнал российского права. – 2016. – №1 (229). – С. 128–138.
2. Романенко, Н.В. Концепция совершенствования особого порядка уголовного производства в отношении судей в Российской Федерации : дисс. ... д-ра юрид. наук. – Екатеринбург, 2022. – 432 с.
3. Епихин, А. Ю., Тасаков, С.В., Гришина, Е.П. Защита чести и достоинства судьи при осуществлении в отношении него уголовного судопроизводства / А. Ю. Епихин, С. В. Тасаков, Е. П. Гришина // Вестник Томского государственного университета. Право. – 2024. – № 53. – С. 35–44.
4. Романенко, Н.В. Проблемные вопросы института задержания лиц, обладающих статусом судьи / Н.В. Романенко // Уголовный процесс. – 2018. – № 3. – С. 117–121.
5. О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ) // Российская газета. – 2017. – № 125. – 9 июня.

Хайрусов Д.С., канд. юрид. наук, доцент кафедры
ФГКОУ ВО «Санкт-Петербургский университет
Министерства внутренних дел Российской Федерации»,
г. Санкт-Петербург

НЕКОТОРЫЕ АСПЕКТЫ КРИМИНАЛИСТИЧЕСКОЙ ПРОФИЛАКТИКИ ДЕЯТЕЛЬНОСТИ «ТЕЛЕФОННЫХ» МОШЕННИКОВ И ПОДСТРЕКАТЕЛЕЙ

Аннотация

В статье изучаются вопросы криминалистической профилактики такого опасного для государственной безопасности криминального явления современности как синтез «телефонного мошенничества» и «мобильного терроризма», т.е. подстрекательства к совершению преступлений – диверсий и террористических актов. Определен ряд перспективных направлений криминалистической превенции данных преступных проявлений.

Ключевые слова: телефонное мошенничество, терроризм, криминалистическая профилактика, предупреждение преступлений.

Борьба с киберпреступностью является государственным стратегическим приоритетом: действующая Стратегия национальной безопасности Российской Федерации ставит задачу противодействия «преступлениям и иным правонарушениям, совершаемым с использованием информационно-коммуникационных технологий (ИКТ)» в целях обеспечения государственной и общественной безопасности [1].

В научной и учебной литературе термином «киберпреступления» охватываются как новые формы преступных деяний, совершение которых стало возможно благодаря Интернету, так и традиционные преступления, которые теперь могут совершаться с помощью новых цифровых инструментов (мобильная связь, онлайн банкинг и т.п.).

Согласно Перечню № 25, при формировании статистической отчетности, к преступлениям, совершенным с использованием (применением) ИКТ относятся, в числе прочих те, где средством выступает использование средств мобильной связи [2]. Данные официальной статистики и мнения экспертов свидетельствует об экспоненциальном росте случаев «телефонного мошенничества» [5, с. 3], отмечается, что с 2020 года количество посягательств с использованием информационных технологий увеличилось на треть, в 2023 году полмиллиона россиян пострадали от действий телефонных мошенников [4].

Особую опасность для государственной безопасности представляют случаи синтеза «телефонного мошенничества» и «мобильного» терроризма, т.е. подстрекательства к совершению преступлений – ди-

версий и террористических актов. Так, в течение 2022-2024 годов в России систематически осуществляются поджоги военных комиссариатов. В ходе расследования было установлено, что в ряде случаев поджоги совершат люди, не имеющие политических мотивов. К примеру, Елена Комаричева, 59-летняя жительница Санкт-Петербурга, была осуждена к десяти годам лишения свободы при следующих обстоятельствах. Телефонные мошенники путем обмана практически лишили Комаричеву средств к существованию: сначала убедили ее перевести кредитные денежные средства в размере 3 млн. руб., на якобы «безопасный счёт», затем уговорили жертву продать квартиру, и после этого, заявив, что лицо, похитившее ее денежные средства находится на территории военкомата, посредством телефонных разговоров в мессенджере, спровоцировали Комаричеву на поджог указанного военкомата, предоставив инструкции по изготовлению зажигательной смеси [6]. И это далеко не единичный случай.

С учётом изложенного, вопрос криминалистической профилактики деятельности «телефонных» мошенников и подстрекателей весьма актуален.

За последние годы в области криминалистической профилактики преступности накопился значительный объем знаний. В многочисленных научных исследованиях обосновывается, что профилактические меры, нацеленные на факторы риска, являются одним из самых эффективных способов противодействия преступности. Вместе с тем, криминалистическую профилактику трактуют различно. Ряд исследователей сосредотачиваются на выявлении и последующем устранении (минимизации) причин и условий совершения преступлений конкретного вида [3, с. 47, 48]. Другие, к числу которых относится и автор данной статьи, используют более широкий подход, полагая, что профилактика включает также совокупность технических средств, тактических и методических приемов для оперативного и качественного предотвращения готовящихся противоправных деяний; выявления, раскрытия, расследования конкретных преступлений; преодоления противодействия расследованию [3, с. 48].

В криминалистической профилактике деятельности «телефонных» мошенников и подстрекателей значимое место занимает информирование населения, в том числе и посредством СМИ. Как показывает проведенный нами контент-анализ интернет-СМИ, публикаций, описывающих схемы осуществления преступной деятельности телефонных мошенников и провокаторов, а также способов противодействия им вполне достаточно. Несмотря на это, статистика показывает рост преступлений такого рода. Возможно, совою роль играет тот

факт, что каждый четвертый пострадавший – пенсионер [4], не в полной мере владеющий теми возможностями, которые предоставляют ИКТ. Представляется, что необходимо адресное воздействие. Ориентируясь на людей и группы, подвергающиеся риску быть жертвами, которые могут не только пострадать финансово, но и быть вовлечены в преступление, требуется принимать меры, направленные на уменьшение их виктимизации: во взаимодействии со службами безопасности кредитных организаций создать базу данных, содержащих информацию о ранее пострадавших от телефонных мошенников, и проводить с ними адресную профилактическую работу.

Отметим, что на странице Телеграмм канала официального представителя МВД Ирины Волк – t.me/IrinaVoik_MVD – опубликована информация о задержании пятерых участников группы, которые в течение года работали на телефонных мошенников, выполняя техническую поддержку украинского колл-центра. Таким образом, перспективным представляется направление разработки криминалистической методики противодействия вербовки граждан России зарубежными кураторами для обслуживания колл-центров, на базе которых работают телефонные мошенники и подстрекатели.

Киберпространство представляет собой ячеистую сеть инфраструктур информационных технологий (включая Интернет), телекоммуникационных сетей, компьютерных систем, процессоров и интегрированных механизмов управления. Таким образом, киберпространство состоит из четырех «слоев», то есть разных уровней инфраструктуры. Первый уровень, «аппаратный», состоит из всей физической инфраструктуры, обеспечивающей работу сети. Второй, «когнитивный», объединяет все программное обеспечение, а третий уровень обозначает информацию, данные, которые в конечном итоге передаются благодаря первым двум уровням. Четвертый уровень включает отдельных лиц и группы, участвующих в цифровой деятельности, т.е. социальное измерение киберпространства. Для эффективного противодействия противоправной деятельности «телефонных» мошенников и подстрекателей, криминалистическая профилактика должна охватывать все четыре уровня.

Список цитируемой литературы:

1. О Стратегии национальной безопасности Российской Федерации: указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27. – Часть II. – Ст. 5351.
2. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической

отчетности: указание Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. [Электронный ресурс]. – Справочно-правовая система «КонсультантПлюс». – URL: https://www.consultant.ru/online (дата обращения: 13.12.2024).
3. Брусенцева, В.А. Роль и место криминалистической профилактики в структуре криминалистической науки /В.А. Брусенцева // Таврический научный обозреватель. – 2015. – №2-3. – С. 46–52.
4. Владимир Колокольцев провел заседание коллегии МВД России, посвященное борьбе с IT-преступностью [Электронный ресурс]. – Пресс-центр МВД России. МВД МЕДИА. – URL. https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedanie-kollegii-mvd-rossii-posvyashchennoe-protivodeystviyu-it-prestu/ (дата обращения: 13.12.2024)
5. Машлякевич В.А. Расследование мошенничеств, совершаемых с использованием средств телефонной связи: автореферат дисс. … канд. юр. наук / В.А. Машлякевич. – Омск. – 2024. – 22 с.
6. Объединённая пресс-служба судов Санкт-Петербург. [Электронный ресурс]. – URL. https://t.me/SPbGS/17858. (дата обращения: 13.12.2024).

Чеботарев Д.Д., магистр
ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Липецкий филиал, г. Липецк

Кузнецова Н.Н., канд. юрид. наук, доцент кафедры
ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Липецкий филиал, г. Липецк

К ВОПРОСУ О ПРИМЕНЕНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Аннотация

В статье рассматриваются возможности применения искусственного интеллекта (далее – ИИ) при противодействии киберпреступности. Выделяются положительные и негативные аспекты. В заключении делается соответствующий вывод.

Ключевые слова: ИИ, киберпреступность, противодействие, закон, современные технологии.

Киберпреступность в последние несколько лет стала одной из значительных проблем как для граждан, так и для всего государства в целом.

Согласно данным Tadviser, количество кибератак в Российской Федерации, в частности, заказных кибератак, за 2024 год выросла с 10 до 44 процентов [1], а число кибератак на российские ИТ-компании выросла в 4 раза.

Кроме того, указанная проблема относится и к персональным данным граждан Российской Федерации, поскольку то и дело в средствах массовой информации появляются сведения о том, что произошла так называемая «утечка данных» граждан. Буквально в начале 2025 года в сети «Интернет» появились сведения о масштабной утечке данных из Единого государственного реестра объектов недвижимости [2]. Позднее Росреестр опроверг какую-либо информации об «утечке данных», однако, в любом случае, со стороны недружественных России государств и не только фиксируются действия, направленные на компрометацию данных граждан и государства.

Помимо «утечек данных» большое распространение получили так называемые «дипфейки» [3], «чат-боты» и иные приложения для осуществления незаконной деятельности по получению персональной информации или доступу к банковским и иным счетам.

Стоит сказать, что мошенники очень часто прибегают к помощи ИИ, поскольку он помогает с помощью огромного массива данных обучиться и найти схему и метод достижения мошеннической цели, что, к сожалению, уже не раз происходило.

В связи с этим, применение ИИ для борьбы с киберпреступностью, по словам Сергея Тростьянского, заместителя директора центра компетенций НТИ по большим данным МГУ, станет одним из главных трендов 2025 года [4].

Стоит сказать, что в РФ уже есть яркий пример того, как ИИ защищает личные данные граждан: это ИИ от Сбера, который постепенно внедряется в приложение для смартфона и сайт.

Говоря же об основных задачах для борьбы с киберугрозами, которые можно решить с помощью ИИ, можно отнести:

1) блокировку на основе анализа информации о пользователе подозрительных операций и действий;

2) обучение с целью выявления новых видов киберугроз;

3) быстрое и точное реагирование на любые, даже самые незначительные угрозы;

4) выполнение задач, требующих повышенного внимания или «рутинных задач».

Говоря же о некоторых других платформах ИИ, которые также помогают в борьбе с киберпреступностью, можно отнести Ankey

ASAP. Данная система осуществляет мониторинг доступа, защиту конфиденциальной информации и управления правами пользователей.

Кроме того, активно внедряются программы для борьбы с «дифейками»: это Ghiro, Image Edited и так далее. Стоит отметить, что «Сбер» также работает в этом направлении.

Однако, стоит сказать, что, вне зависимости от того, насколько качественно внедрен ИИ с целью противодействия киберугрозам, человеку также необходимо знать основные принципы защиты от кибератак. К примеру, эксперты РБК выделяют следующие принципы:

1. Повышение уровеня киберграмотности сотрудников.
2. Грамотное использование открытых сетей Wi-Fi.
3. Использование многофакторную аутентификацию (MFA).
4. Ограничение информации в социальных сетях.
5. Использование антифишингого программного обеспечения.
6. Регулярное применение резервного копирования данных.
7. Регулярное обновление программного обеспечения и операционной системы.
8. Использование антивирусного и антишпионского ПО.
9. Применение детекторов дипфейков.
10. Использование услуги информационной безопасности по сервисной модели [5].

В заключение следует отметить, что стремительное развитие технологий искусственного интеллекта ознаменовало собой новый этап в борьбе с киберпреступностью. ИИ-системы демонстрируют впечатляющие результаты в обнаружении вредоносного ПО, анализе сетевого трафика, предотвращении фишинговых атак и расследовании киберпреступлений. Их способность обрабатывать огромные объемы данных с невероятной скоростью и выявлять сложные паттерны, недоступные человеческому аналитику, значительно повышает эффективность кибербезопасности. Автоматизация рутинных задач позволяет специалистам сосредоточиться на более сложных и стратегических аспектах защиты. ИИ-инструменты, такие как системы машинного обучения, способны адаптироваться к постоянно меняющимся тактикам киберпреступников, обеспечивая более проактивную и эффективную защиту.

Однако, несмотря на впечатляющие возможности ИИ, полная зависимость от него в борьбе с киберпреступностью была бы крайне опасной. ИИ-системы, хоть и мощные, остаются всего лишь инструментом, эффективность которого напрямую зависит от качества данных, на которых он обучается, и от компетентности специалистов, которые его используют и интерпретируют результаты. Они уязвимы для обхода и могут быть использованы злоумышленниками для создания

более изощренных атак. Более того, ИИ не способен заменить человеческий интеллект, интуицию и критическое мышление, необходимые для понимания контекста, принятия сложных решений и разработки стратегий противодействия. Человеческий фактор остается ключевым элементом в борьбе с киберпреступностью.

Поэтому, будущее кибербезопасности лежит не в противопоставлении человека и ИИ, а в их синергии. Эффективная защита требует комплексного подхода, сочетающего передовые технологии искусственного интеллекта с опытом, знаниями и этическими принципами работы специалистов в области кибербезопасности. Необходимо продолжать инвестировать в развитие ИИ-технологий для борьбы с киберпреступностью, одновременно уделяя пристальное внимание обучению и развитию профессионалов, способных эффективно использовать эти технологии и противостоять постоянно эволюционирующим угрозам. Только такой интегрированный подход, объединяющий мощь ИИ и человеческий интеллект, сможет обеспечить надежную защиту в цифровой среде.

Список цитируемой литературы:

1. Число кибератак в России и в мире [Электронный ресурс]. – Tadviser.ru: Государство. Бизнес. Технологии: сайт. – URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения: 13.01.2025).
2. Утечка данных Росреестра: чем завладели хакеры и как не стать жертвой мошенников [Электронный ресурс]. – Дзен: российская блог-платформа. – URL: https://dzen.ru/a/Z35EvCbj0llJ9htl (дата обращения: 13.01.2025).
3. Валяева А. Как делают deepfake-видео и почему лучше говорить «face swap» / А. Валяева. [Электронный ресурс]. – Vc.ru: российское интернет-издание о бизнесе, стартапах, инновациях, маркетинге и технологиях. – URL: https://vc.ru/ml/94457-kak-delayutdeepfake-video-i-pochemu-luchshe-govorit-faceswap (дата обращения: 13.01.2025)
4. Применение ИИ для борьбы с киберпреступностью станет одним из главных трендов в 2025 году [Электронный ресурс]. – Spark.ru: блог-платформа. – URL: https://spark.ru/startup/spark-news/blog/241459/primenenie-ii-dlya-borbi-s-kiberprestupnostiu-stanet-odnim-iz-glavnih-trendov-v-2025-godu (дата обращения: 13.01.2025)
5. Как ИИ помогает кибермошенникам и противостоит им [Электронный ресурс]. – РБК: сайт. – URL: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a?from=copy (дата обращения: 13.01.2025)

Шагунова В.М., канд. юрид. наук, доцент кафедры
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте Российской Федерации»,
Липецкий филиал, г. Липецк

Особенности расследования преступлений в сфере экономической деятельности, совершаемых в киберпространстве

Аннотация

Расследование преступлений в сфере экономической деятельности, совершённых в киберпространстве, обладает рядом уникальных особенностей, которые отличают его от традиционных преступлений в этой сфере. В отличие от классических преступлений в сфере экономической деятельности, совершённых в физическом мире, преступления в киберпространстве часто не оставляют явных следов. Следователям при расследовании таких преступлений сложно точно оценить ущерб, который может быть как материальным, так и репутационным. Это требует от следователей не только навыков расследования, но и глубоких знаний в области экономики, информационных технологий и компьютерной безопасности.

Ключевые слова: экономическая деятельность, киберпространство, расследование преступлений, экономической киберпреступностью.

Современное киберпространство представляет собой виртуальную среду, которая создана на основе динамично развивающихся интернет-технологий, в рамках которой могут осуществляться процессы дистанционной коммуникации между различными участниками в самых различных сферах деятельности. В ее структуру входят такие элементы, как доступ в интернет, веб-сайты, социальные сети, облачные сервисы, мессенджеры и т.д. Благодаря технологическим возможностям киберпространства в ней можно распространять информацию, выражать мнения, посещать онлайн-курсы и т.д. Благодаря ускоренной цифровизации и глобализации киберпространство стало средой, в которой люди могут вести предпринимательскую деятельность, развивать собственный бизнес, осуществлять финансовые операции. В связи с такими широкими возможностями такая среда является благодатной почвой для совершения преступлений.

Согласно исследованию, проведенному в 2024 году экспертами от Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, выявлено, что преступность в киберпространстве в последние годы динамично растет (количество та-

ких преступлений в 2023 году выросло в 2,3 раза (с 294 тыс. до 676,9 тыс. преступных деяний) и характеризуется такими чертами, как высокий уровень латентности, повышение уровня профессионализма, организованный и корпоративный характер. Выявлено также, что растет общественная опасность данных преступлений. Если ранее доля тяжких и особо тяжких преступлений в цифровой сфере не превышала 25%, то в настоящее время она составляет более половины всех цифровых преступлений (342 637 в 2023 г.). Негативной тенденцией является рост общественной опасности преступлений, осуществляемых в киберпространстве. В 2019 г. удельный вес тяжких преступлений относительно всех цифровых противоправных деяний не превышал 25%, то по итогам 2023 года – уже более 50% в их структуре. Раскрываемость таких преступлений низкая (на одно раскрытое преступление приходится 4 тыс. нераскрытых) [2].

Согласно информации, представленной в годовом отчете МВД России, В 2023 году каждое третье преступление совершено с использованием информационно-телекоммуникационных технологий (ИКТ), в киберпространстве. В 2023 году количество таких преступных деяний выросло на 7,8% по сравнению с 2022 годом. В 2024 году 40% преступлений были совершены с использованием ИКТ. По итогам 2024 года их количество выросло на 13,1% по сравнению с 2023 годом [3]. Таким образом, темп роста преступлений в киберпространстве растет.

Среди всех цифровых преступлений, совершаемых в киберпространстве, широко распространенной категорией являются преступления в сфере экономической деятельности. Основными их видами являются мошенничество в сфере компьютерной информации, мошенничество с использованием электронных средств платежа, кража [4, С. 48].

Расследование преступлений в сфере экономической деятельности, совершаемых в киберпространстве осуществляется по следующим этапам:

- после поступления от потерпевшего заявления о совершении в отношении него преступного деяния данного характера осуществляются первоначальные следственные действия, в ходе которых:

- проходит опрос потерпевшего, осмотр виртуального места происшествия при помощи изучения данных с того устройства, через которое были похищены средства или информация;

- осуществляется подтверждение факта преступления (запрашиваются выписки по счетам, осуществляется детализация телефонных звонков и т.д.);

- проводится сбор и анализ информационных следов;

- установление личности преступника (в случае, если предыдущий этап был успешным);

- проведение следственных действий в отношении подозреваемого (обыск и выемка электронных носителей информации, которые применялись им для совершения преступления);

- завершение расследования (в случае, если доказано, что обвиняемый в действительности совершил вменяемое ему преступное деяние, - оформляется уголовное дело и передается в суд, где осуществляется судебное разбирательство, по итогам которого преступнику назначаются конкретные меры уголовной ответственности).

Расследование преступлений в сфере экономической деятельности, совершаемых в киберпространстве является проблемным аспектом в деятельности правоохранительных органов. Это связано, главным образом, со следующими особенностями:

1) анонимность сетей, через которые осуществляются преступления (например, использование нейросетей или Deep web, доступ в который в основном осуществляется через TOR-браузер, используя его свойства анонимости);

2) расположение серверов за рубежом и использование VPN-технологии для управления ими, что создает юрисдикционные барьеры в процессе расследования;

3) высокая скорость и множественность транзакций (как правило, если мошенникам дистанционно удалось похитить средства физического лица, находящиеся на его счете в банке, то операции по переводу их на счета похитителей проводятся практически мгновенно, и их очень сложно отследить, поскольку преступники используют многоступенчатую систему переводов, т.е. через множество других счетов, разводняющих похищенную сумму на более мелкие);

4) специфика цифровых доказательств создает ряд сложностей в процессе расследования (в частности, мошенники «зачищать» за собой информационные следы совершенных преступлений; кроме того, не все цифровые доказательства могут быть использованы как улики в судебном разбирательстве);

5) постоянное совершенствование технологий, средств и инструментов преступной деятельности в процессе совершения преступлений в сфере экономической деятельности, совершаемых в киберпространстве;

6) недостаточно высокая квалификация специалистов, которые расследуют такие преступления, а также недостаточная техническая оснащенность отделов, которые расследуют экономические преступления в киберпространстве.

Отметим, что в настоящее время преступления в сфере экономической деятельности, совершаемых в киберпространстве в основном осуществляются при помощи нейросетей, которые позволяют генерировать фишинговые сайты (т.е. сайты, являющиеся практически точной копией сайтов официальных организаций, заходя на которые, люди могут стать жертвой кибер-преступников), а также создавать дипфейки (т.е. создавать поддельные видео- или аудиозаписи) и даже автоматизированные мошеннические схемы (например, через создание фальшивых профилей в интернете или через использование технологий, которыми располагают мессернджеры (в частности, среди используемых в России мессенджеров сложнее всего отследить информацию в Telegram). Нейросети могут быть использованы для кражи информации и фальсификации различных данных (например, создание поддельных документов физических лиц, документов о якобы осуществленных финансовых сделках, документов для легализации доходов и т.д.).

Рассмотрим подробнее такой инструмент для осуществления преступлений в сфере экономической деятельности в киберпространстве, как так называемый глубокий интернет - «Deep web», внутри которой функционирует теневой интернет – «DarkNet» (Даркнет). Эта часть недоступна для обычного поиска в Интернете, контент работает только через подключения, созданные с помощью специального программного обеспечения. Привлекательность данного сегмента для значительного числа пользователей заключается в том, что он позволяет обеспечивать практическую полную анонимность в сети, соответственно, даже если осуществлять преступные действия, можно быть уверенными в безопасности. Поэтому криминальная деятельность преступников в сети Даркнет требует выработки эффективных мер противодействия со стороны правоохранительных органов. В настоящее время выявление и раскрытие деяний, совершаемых в теневой части инета – сложная задача [1, С. 813].

Таким образом, по итогам исследования сделан вывод о том, что основными особенностями расследования преступлений в сфере экономической деятельности, совершаемых в киберпространстве, являются высокий уровень конспирации преступников, что стало возможно на основе использования анонимных сетей или сетей, использующих технологии анонимности; юрисдикционные барьеры в процессе расследования, связанные с расположением серверов преступников в других государствах; высокая скорость и множественность транзакций, сложности поиска цифровых следов ввиду возможностей преступников оперативно и с высокой эффективностью их «зачищать»; постоянное совершенствование технологий, средств и инструментов преступной деятельности; недостаточно высокая квалификация специалистов,

которые расследуют такие преступления; невысокий технический и технологический уровень оснащения отделов, где осуществляется расследование преступлений в сфере экономической деятельности, совершаемых в киберпространстве.

Существующая в настоящее время система борьбы с экономической киберпреступностью недостаточно эффективна не только в связи с проблемами, которые возникают в процессе их расследования, но и в связи с «пробелами» в законодательстве (в частности, признаки использования IT-технологий рассредоточены в настоящее время по многим составам преступлений, изложенным в УК РФ, что создает проблемы в их квалификации). Поэтому необходима системная деятельность по противодействию преступлениям рассматриваемого вида, которая должна включать в себя совершенствование уголовного законодательства, повышение уровня профессионализма сотрудников правоохранительных, расширение структуры, занимающейся выявлением и раскрытием различных преступлений, совершаемых в киберпространстве, а также масштабная деятельность всего государства, во взаимодействии с мировым сообществом, по противодействию преступности в данной сфере.

Список цитируемой литературы:

1. Сабельникова, Г. С. Особенности экономических преступлений, совершенных с использованием Даркнета / Г. С. Сабельникова // Следственная деятельность: проблемы, их решение, перспективы развития : материалы III Всероссийской молодёжной научно-практической конференции (Москва, 25 ноября 2019 г.). – Москва: Московская академия Следственного комитета Российской Федерации, 2020. – С. 810–813.
2. Сидоренко, Э. Л. Цифровая преступность: угрозы и тренды. Топ-10 / Э.Л. Сидоренко [Электронный ресурс]. – Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека. – URL: https://www.president-sovet.ru/members/blogs/post/tsifrovaya_prestupnost_ugrozy_i_trendy_ top_10/ (дата обращения 01.01.2025).
3. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года. [Электронный ресурс]. – МВД Российской Федерации – URL: https://мвд.рф/reports/item/60248328/ (дата обращения 01.02.2025).
4. Сверчкова, А.Д., Гуляева, А.Д. Анализ динамики экономических преступлений с использованием ИКТ в России / А. Д. Сверчкова, А. Д. Гуляева // Научные записки молодых исследователей. – 2023. – № 1. – С. 45–55.

Шаповалов Е.В.,
руководитель следственного управления Следственного комитета
Российской Федерации по Липецкой области,
генерал-майор юстиции,
канд. юрид. наук, зав. кафедрой
ФГБОУ ВО «Липецкий государственный технический университет»,
г. Липецк

КИБЕРПРЕСТУПНОСТЬ: ПРОБЛЕМЫ ПРАКТИКИ РАССЛЕДОВАНИЯ

Аннотация

Развитие информационно-коммуникационных технологий оказывает влияние на количественные и качественные характеристики преступлений. В работе рассматриваются проблемы практики расследования киберпреступлений, среди которых их гиперизменчивость, активное использование социальной инженерии и психологических методов вовлечения в противоправную деятельность, сложность систематизации информации, связанной с совершением киберпреступлений, отсутствие оперативного обмена информацией о киберпреступлениях между правоохранительными органами.

Ключевые слова: киберпреступления, информационно-коммуникационные технологии, угрозы, расследование киберпреступлений, система противодействия кибепреступлениям.

Технологический прогресс и формирование информационного общества способствовали распространению мобильных устройств, беспроводных технологий и сетей связи. Интернет-пространство открыло широкие возможности для межличностного общения, обучения и трудовой деятельности. Тем не менее данные процессы характеризуются не только положительными качественными изменениями в жизни человека, но и вызывают многочисленные деструктивные явления, порождают риски и угрозы различного уровня. Цифровые технологии стали все более активно использоваться для совершения преступлений и достижения криминальных целей. Злоумышленники переориентировались на совершение преступлений в информационной сфере.

Данные официальной статистики свидетельствуют о том, что с каждым годом доля преступлений в сфере информационно-коммуникационных технологий в общей структуре всех зарегистрированных преступлений увеличивается. Если в 2023 году в России было зарегистрировано 676 951 преступлений [1], то за 12 месяцев 2024 года их количество составило 765365 [2]. Таким образом, рост составил 13,1% по сравнению с аналогичным периодом 2023 года. При этом, в

течении последних пяти лет количество преступлений увеличилось более чем в пять раз.

В Липецкой области также отмечается рост указанных противоправных деяний. Так, в 2024 году было зарегистрировано 183 преступления, совершенных с использованием информационно-коммуникационных технологий, а в 2023 - 142.

В структуре киберпреступлений, совершенных на территории Липецкой области, преобладают преступления против половой неприкосновенности несовершеннолетних (53).

Среди иных киберпреступлений следует отметить: сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») (14), нарушение неприкосновенности частной жизни (5), кражи (27), мошенничества (6), неправомерный доступ к компьютерной информации (9), незаконные изготовление и оборот порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (7).

Таким образом, киберпреступность приобрела массовый характер и представляет опасность не только для отдельного человека, но и органов государственной власти, крупных коммерческих предприятий, объектов критической инфраструктуры. Следовательно, данные преступления представляют угрозу и непосредственно национальной безопасности. Такого рода тенденция четко прослеживается в течение последних трех лет.

Следует отметить, что среди киберпреступлений самый низкий уровень раскрываемости. Только 22,8% обозначенных преступлений, совершенных с использованием информационно-коммуникационных технологий были раскрыты правоохранительными органами в прошлом году в России.

Во многом сложившаяся ситуация обусловлена определенными причинами. На наш взгляд, представляется целесообразным выделить среди них наиболее значимые.

1. Способы совершения киберпреступлений, обусловленные цифровой средой быстро трансформируются. Киберпреступники анализируют любые изменения, происходящие в стране. При разработке преступного сценария учитывают социальные, экономические и политические события, а также законодательные изменения (преимущественно затрагивающие финансовое и материальное обеспечение различных групп граждан). В этой связи, такого рода противоправные деяния являются гиперизменчивыми, их достаточно сложно проанализировать,

выявить определенные закономерности механизма преступной деятельности.

2. Преступники быстро подстраиваются под потенциальных жертв, активно применяя социальную инженерию и психологические методы вовлечения в противоправную деятельность. При этом воздействие направлено на конкретную категорию населения, которая соответствует установленным параметрам (пол, возраст, интересы, политические взгляды), а также учитываются географический, тематический, временной факторы.

3. Нейросети и искусственный интеллект стали выступать в качестве важных инструментов для совершения противоправных действий. Широкое распространение среди злоумышленников получила технология по искусственной генерации недостоверной информации (фейков), которая представляет серьезную угрозу для многих общественных процессов. Нередко она используется как инструмент дестабилизации политической обстановки и деятельности органов государственной власти. Фальшивые новости сеют панику, подталкивают к беспорядкам и необдуманным действиям, вводят в заблуждение. Люди, сами того не понимая, становятся распространителями дезинформации, либо участниками преступной деятельности.

4. Преобладает сетевой способ и групповая форма совершения киберпреступлений. Участники преступной группы могут друг друга и не знать лично.

Преступные группы имеют деление на подгруппы (структуры), специализирующиеся на выполнении конкретных задач. Внутри подгрупп имеются корпоративная иерархия, система мотиваций и денежных вознаграждений. Группу возглавляет руководитель (лидер), который взаимодействует с подгруппами, ставит перед ними конкретные задачи: решение технических вопросов, поиск новых участников, либо преступных групп партнеров.

Координация между ними, размещение заказов на написание вредоносного ПО, распространение и продажа скомпрометированной информации (данные кредитных и дебетовых карт, доступы к учетным записям пользователей и тп.) осуществляется через андеграундные форумы, размещенные в «Даркнете», закрытие группы. Преступники стараются минимизировать непосредственное общение (вживую) и исключить использование телефонной связи и электронной почты.

5. Сложность систематизации информации, связанной с совершением киберпреступлений.

Следует отметить, что отсутствие систематизированной информации, связанной с механизмом совершения киберпреступлений и

электронно-цифровых следов, не позволяет получить целостную картину о количестве реально совершенных конкретным лицом противоправных деяний. Правоприменители вынуждены обмениваться взаимными запросами об установлении фактов совершения преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации на территории различных субъектов Российской Федерации. К сожалению, не всегда такие данные могут быть получены в силу своей разрозненности и неоднородности.

6. Отсутствие оперативного обмена информацией о киберпреступлениях между правоохранительными органами, государственными органами и заинтересованными организациями.

Следовательно, выстраивание эффективной системы борьбы с киберпреступлениями предполагает формирования комплексной системы противодействия им.

Правоохранительные органы нуждаются в новых и эффективных средствах и методах выявления и систематизации информации, связанной с киберпреступлениями.

Необходима разработка программных инструментов, позволяющих расследовать преступления в режиме реального времени, обрабатывать большие массивы информации, имеющей криминалистическое значение.

Кроме того, требуется адаптация уголовно-процессуального законодательства к новым информационно-технологическим реалиям.

Тем не менее, определенные шаги, направленные на создание комплексного механизма по противодействию киберпреступлениям сделаны. 30 декабря 2024 г. № 4154-р была утверждена «Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» [3], которая в качестве основной цели устанавливает «защиту государства, общества и граждан от противоправных деяний». Определены задачи, среди которых центральное положение занимают: прогнозирование противоправных деяний; выявление противоправных деяний; повышение результативности расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Кроме того, указан ряд мер, которые, как нам видится, позволяют решить обозначенные ранее проблемы. Так, предлагается создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком Российской Федерации, кредитными организа-

циями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети «Интернет» и иных информационных технологий (за исключением компьютерных атак и компьютерных инцидентов).

Таким образом, проблема противодействия киберпреступности сегодня актуальна и требует широкого обсуждения, с теоретической и практической точек зрения.

Список цитируемой литературы:

1. Состояние преступности в России за январь – декабрь 2023 года. [Электронный ресурс]. – Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://media.mvd.ru/files/application/5095078 (дата обращения: 06.01.2025).
2. Состояние преступности в России за январь – декабрь 2024 года [Электронный ресурс]. – Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://media.mvd.ru/files/application/9209203 (дата обращения: 16.01.2025).
3. Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Рос. Федерации от 30 декабря 2024 г. № 4154-р // Собрание законодательства Российской Федерации. – 2025. – № 2. – Ст. 76.

Научное издание

Современные вызовы и механизмы противодействия киберпреступности

Сборник материалов
всероссийской научно-практической конференции
с международным участием
приуроченной ко Дню образования
Следственного комитета Российской Федерации
(17 января 2025 г., г. Липецк)

Под общ. ред. канд. юрид. наук, доц. В.А. Брусенцевой,
канд. юрид. наук, доц. Е.В. Шаповалова

АНО «НАУКА-ЮНИПРЕСС»
394024, г. Воронеж, ул. Ленина, 86Б, 2
Формат 60×84/16. Бумага офсетная.
Усл. п.л. 13,75. Тираж 500 экз.
Отпечатано в типографии издательства
394024, г. Воронеж, ул. Ленина, 86Б, 2