СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Материалы международной научно-практической конференции

(Москва, 28 апреля 2023 года)

Москва, 2023

УДК 343
ББК 67.5

П 78 **Проблемы противодействия киберпреступности:** материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. – 255 с.

Сборник сформирован по материалам, представленным на международную научно-практическую конференцию, проведённую в Московской академии Следственного комитета Российской Федерации 28 апреля 2023 года. Конференция организована с участием учёных, сотрудников правоохранительных органов России, профессорско-преподавательского состава и аспирантов ВУЗов.

Сборник представляет интерес для обучающихся в Академии, студентов юридических ВУЗов, юристов – учёных и практиков.

Редакционная коллегия обращает внимание на то, что научные подходы, идеи, и взгляды, изложенные в статьях сборника, отражают позиции и оценки их авторов и могут отличаться от мнения редакторов.

А.А. Бессонов

Научное и учебно-методическое обеспечение расследования киберпреступлений в Московской академии Следственного комитета

Аннотация. Для эффективной организации расследования преступлений в сфере информационно-телекоммуникационных технологий или компьютерной информации важное значение имеет научное и учебно-методическое обеспечение этой деятельности. В Московской академии Следственного комитета на системной основе осуществляются научно-исследовательские работы, проводятся научно-представительские мероприятия по вопросам квалификации этих деяний, методики их расследования, особенностей уголовного судопроизводства, международного сотрудничества и пр.

***Ключевые слова*:** киберпреступления, преступления в сфере высоких технологий, преступления в сфере ИКТ, расследование киберпреступлений.

Сегодня крайне актуальны вопросы расследования преступлений в сфере информационно-телекоммуникационных технологий или компьютерной информации, составляющих четверть от общего количества регистрируемых на территории нашей страны преступных деяний, 70% которых, к сожалению, остаются нераскрытыми. Согласно статистике МВД России ежегодно регистрируется более полумиллиона обозначенных преступных деяний. Например, за 2022 год зарегистрировано 522065 таких преступлений, что составило 27% в общей преступности, не раскрыт 71% из них.[1]

Если произвести простой арифметический подсчёт на основе раскрытых преступлений по числу совершённых деяний 1 преступником, то ежегодно от ответственности уходят 180-190 тыс. человек. В этой связи от качественного криминалистического, а именно научного и учебно-методического обеспечения напрямую зависит эффективность противодействия такого рода преступности.

Деятельность Московской академии Следственного комитета Российской Федерации на этот счёт осуществляется по следующим направлениям:

обучение студентов первичным знаниям методики расследования киберпреступлений, их уголовно-правовой характеристики и т.п.;

повышение квалификации действующих сотрудников системы Следственного комитета Российской Федерации, в том числе в части криминалистического сопровождения с учётом самой новейшей информации об особенностях таких деяний;

научно-исследовательская работа по разработке программных средств выявления и фиксации цифровых следов и иной криминалистически значимой информации о таких преступлениях;

[1] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2022 года // URL: https://мвд.рф/reports/item/35396677/ (дата обращения 01.03.2023).

научно-методическое обеспечение в форме разработки учебных и практических пособий, проведения научно-представительских мероприятий и т.д.

Большая роль в реализации обозначенных направлений принадлежит созданной в Московской академии Следственного комитета в 2021 году во исполнение поручения Председателя Следственного комитета Российской Федерации А.И. Бастрыкина кафедре информационных технологий и организации расследования киберпреступлений.

Что касается первого направления, то деятельность этой кафедры направлена на формирование у студентов устойчивых знаний основ информационной безопасности, информационного права, правовой статистики, специфики методики расследования киберпреступлений, процессуального закрепления цифровых следов преступлений, навыков работы с цифровыми технологиями, применительно к будущей профессии, а также проведение научных исследований в области цифровых технологий, используемых в работе следователя.

Кафедрой преподаются следующие учебные дисциплины: «Информатика и информационные технологии в профессиональной деятельности», «Информационное право», «Основы информационной безопасности», «Правовая статистика», «Цифровые следы преступлений против личности», «Расследование киберпреступлений», «Информационные технологии в науке и образовании».

На кафедре организована активная работа с обучающимися академии. Так, команда Московской академии Следственного комитета «След» приняла участие в киберсоревнованиях и конкурсе проектов «Хакатон-2022», проводимом МВД России, заняв второе место с проектом моделирования алгоритма составления цифрового профиля преступника.

11.05.2022 проведён семинар, посвящённый российскому инновационному специальному программному обеспечению в сфере криминалистики и судебной экспертизы. На занятие были приглашены представители российских IT-компаний. Разработчики программных решений в сфере информационной безопасности и цифровой криминалистики представили различные программные продукты по извлечению информации из мобильных устройств, восстановлению паролей к широкому ряду мобильных и иных приложений.

18.05.2022 для обучающихся и профессорско-преподавательского состава Академии была организована публичная лекция доктора юридических наук, профессора, генерал-лейтенанта милиции Ю.Н. Жданова, посвящённая преступности в цифровую эпоху, а 08.06.2022 по его инициативе состоялась экскурсия обучающихся в Департамент кибербезопасности Сбербанка России, где они ознакомились с современным порядком оперативного реагирования на киберугрозы, а также предупреждения хищений денежных средств физических и юридических лиц.

01.06.2022 обучающиеся факультета подготовки криминалистов в процессе освоения дисциплины «Компьютерно-техническое обеспечение расследования преступлений» посетили Судебно-экспертный центр Следственного комитета,

где ознакомились со спецификой производства судебных экспертиз, связанных с изучением компьютерных средств и информации.

В рамках повышения квалификации, как впрочем и при обучении студентов, для проведения занятий привлекаются практические работники: представители Главного управления криминалистики (Криминалистического центра), Судебно-экспертного центра Следственного комитета, ЭКЦ МВД России, отечественных IT-компаний и др.

В рамках реализации программ повышения квалификации для сотрудников Следственного комитета, осуществляющих функции в сфере уголовного судопроизводства, изучаются следующие темы, связанные с расследованием преступлений рассматриваемого вида: «Современные возможности получения и анализа данных, содержащихся в мобильных устройствах», «Технико-криминалистические средства и аппаратно-программные комплексы для получения и анализа билинговой информации», «Использование сети Интернет для раскрытия и расследования преступлений», «Современные возможности раскрытия и расследования преступлений по «цифровым» следам». В 2022 году такие программы реализованы при обучении более шестисот сотрудников системы Следственного комитета Российской Федерации.

В качестве следующего направления работы Московской академии Следственного комитета можно отметить научно-представительские мероприятия по вопросам раскрытия и расследования преступлений в сфере информационно-телекоммуникационных технологий.

За последний год организованы и проведены 2 конференции и 2 круглых стола по данной тематике. К примеру, 02.12.2021 совместно с Санкт-Петербургской академией Следственного комитета проведена международная научно-практическая конференция «Противодействие киберпреступлениям и преступлениям в сфере высоких технологий», а 17.11.2022 всероссийская научно-практическая конференция с международным участием «Противодействие экстремизму в условиях цифровизации и информатизации общества и государства».

К этому следует добавить, что вопросы расследования преступлений, совершаемых с применением современных цифровых технологий, не остаются без внимания при проведении конференций, круглых столов и по другой тематике, так как сегодня цифровизация добралась до всех аспектов нашей жизни.

В целях выявления актуальных потребностей практики, изучения современных криминалистических особенностей такого рода преступных деяний, складывающейся практики их уголовно-правовой квалификации и специфики доказывания Московской академией Следственного комитета осуществляется постоянное тесное взаимодействие с региональными следственными управлениями.

В частности, в 2022 году у руководителей главных следственных управлений и следственных управлений Следственного комитета по субъектам Российской Федерации запрошены актуальные эмпирические данные и методические материалы за последние 3 года по уголовным делам о преступлениях,

совершённых с использованием таких технологий. На основании полученных материалов Академией осуществляется подготовка учебника «Расследование киберпреступлений». Также издано практическое пособие «Получение криминалистически значимой информации из социальной сети «Telegram». В пособии раскрываются основные методы и приёмы установления пользователей мессенджера «Telegram», а также владельцев и администраторов сообществ, существующие программные продукты, предназначенные для подобной работы, приводится алгоритмизированный порядок действий, позволяющих эффективно расследовать типичные виды преступлений, совершаемых с использованием этого мессенджера. Пособие прошло рецензирование в Главном управлении криминалистики (Криминалистическом центре) и Главном следственном управлении Следственного комитета (в отделе по расследованию киберпреступлений и преступлений в сфере высоких технологий). Помимо этого в том же году в академии подготовлено 3 практических пособия и 1 курс лекций по затронутой проблематике по темам: «Вопросы квалификации и расследования доведения до самоубийства несовершеннолетних с помощью сети Интернет», «Особенности квалификации и расследования краж с банковского счёта, а равно в отношении электронных денежных средств», «Расследование преступлений, совершённых с использованием Интернета и мобильной телефонии» и «Расследование преступлений против половой неприкосновенности и половой свободы несовершеннолетних, совершённых с использованием сети Интернет».

Сотрудники Академии также приняли участие в подготовке монографии «Теория информационно-компьютерного обеспечения криминалистической деятельности» под редакцией Е.Р. Россинской (МГЮА). В рамках заключённого соглашения о сотрудничестве с Институтом повышения квалификации и переподготовки Следственного комитета Республики Беларусь, а также совместно с Санкт-Петербургской академией Следственного комитета ведётся работа по написанию монографии «Криминалистические особенности производства процессуальных действий с цифровыми следами». Совместно с Институтом государства и права РАН проводится исследование по теме: «Информационные технологии в уголовно-правовой сфере». Эта коллективная монография охватит вопросы предупреждения цифровой преступности уголовно-правовыми, уголовно-процессуальными и криминалистическими средствами, международный опыт борьбы с ней.

Представители профессорско-преподавательского состава Московской академии Следственного комитета для обсуждения проблемных вопросов практики противодействия этим преступлениям и их расследования, поиска путей разрешения этих проблем взаимодействуют с научным сообществом нашей страны и ближнего зарубежья, принимая участие в различных научно-представительских мероприятиях. К примеру, сотрудники академии приняли участие в:

XI Международном Форуме безопасного интернета–2022;

международном форуме цифровой трансформации безопасности государства «ЦИФРОТЕХ» в ходе XXVI Международной выставки средств обеспечения

безопасности государства «ИНТЕРПОЛИТЕХ-2022» (сделан доклад на тему «Современные возможности технологии поиска информации из открытых источников в расследовании преступлений»);

всероссийской научно-практической конференции с международным участием «Современные проблемы противодействия киберпреступности» (выступление с докладом «К вопросу о некоторых способах совершения компьютерных преступлений»);

тематической секции «Искусственный интеллект на службе Отечества» в рамках Международного военно-технического форума «Армия-2022» (доклад «Искусственный интеллект в противодействии киберпреступности как элемент обеспечения национальной безопасности»);

всероссийской научно-практической конференции «Криминалистика: наука, практика, опыт» (доклад «Некоторые проблемные вопросы расследования киберпреступлений»);

международной научно-практической конференции «Развитие научных идей профессора Р.С. Белкина в условиях современных вызовов» (доклад «Криминалистическая характеристика преступлений в цифровую эпоху»);

II международной научно-практической конференции «Основные направления совершенствования системы национальной безопасности» в г. Минске (доклад «Противодействие киберпреступности как элемент обеспечения национальной безопасности»);

межведомственной научно-практической конференции «Актуальные вопросы деятельности подразделений уголовного розыска в условиях новых вызовов и угроз» (доклад «Использование в раскрытии преступлений информации из открытых источников информации (OSINT)»).

Следует отметить, что в Московской академии Следственного комитета ведётся активная научно-исследовательская работа по изучению применимости современных цифровых технологий, прежде всего искусственного интеллекта в расследовании преступлений, в том числе путём взаимодействия с другими ведомствами и научными организациями.

В частности, по приглашению руководства ФКУ «НПО «Специальная техника и связь» МВД России представители академии совместно с сотрудниками Главного управления криминалистики приняли участие в совещании, посвящённом возможностям методов машинного обучения и анализа данных для выявления признаков серийности (сходства) определённых категорий преступлений. В ходе встречи состоялось конструктивное обсуждение функциональных возможностей разработанного макета информационной системы с её разработчиками.

Имеет место взаимодействие по разработке проблематики применимости искусственного интеллекта и других цифровых технологий в расследовании преступлений с Российской академией наук, например, с Институтом системного программирования имени В.П. Иванникова РАН.

В рамках работы в составе Совета по приоритетному направлению Стратегии научно-технологического развития Российской Федерации «Противодействие техногенным, биогенным, социокультурным угрозам, терроризму и

идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства» осуществляется мониторинг и оценка современных средств и методов противодействия киберугрозам и различным видам преступлений, совершаемых с применением информационно-телекоммуникационных технологий.

Помимо этого в числе достижений Московской академии Следственного комитета в этой сфере можно отметить две компьютерные программы: одна для определения места расположения очага пожара (один из её авторов – заведующий научно-исследовательским отделом Ильин Н.Н., свидетельство о государственной регистрации программы для ЭВМ № 2021667046 от 25.10.2021), а вторая – позволяет произвести оценку угрозы воспламенения поверхности материала от воздействия лучистого теплового потока при пожаре в здании (автор – Ильин Н.Н., свидетельство о государственной регистрации программы для ЭВМ № 2022611149 от 15.06.2022). Вторая программа по итогам Международного грантового конкурса «Research startup», организованного Российским научным обществом «Future Technologies: Science and innovations», в декабре 2022 года заняла 1 место в номинации «Информационные технологии».

В целях совершенствования учебного процесса в Московской академии Следственного комитета прорабатывается вопрос возможности создания современного киберполигона, а также Центра цифровых компетенций в расследовании преступной деятельности. На базе последнего предполагается осуществлять мониторинг современного состояния информационно-компьютерного обеспечения расследования преступлений; изучать применимость самых новейших цифровых технологий в отдельных направлениях деятельности Следственного комитета Российской Федерации; привлекать к научно-исследовательской работе Московской академии Следственного комитета ведущих специалистов в сфере программирования, анализа данных, представителей IT-компаний; оказывать при необходимости помощь практическим работникам в использовании цифровых технологий при расследовании по уголовным делам и проверках сообщений о преступлениях, в том числе с привлечением взаимодействующих с центром внешних специалистов; наконец, обучать следователей, следователей-криминалистов, экспертов специфике цифровых технологий, их использованию для поиска цифровых следов, в конечном итоге – для эффективного расследования преступлений.

И.А. Архипова

Особенности сбыта сильнодействующих или ядовитых веществ через сеть Интернет

Аннотация. В статье рассматриваются особенности, выявленные при сбыте сильнодействующих или ядовитых веществ, акцентируется внимание на бесконтактном способе сбыта, разграничиваются способы совершения уголовно-наказуемых деяний рассматриваемой группы преступлений.

Ключевые слова: незаконный оборот сильнодействующих и ядовитых веществ, сбыт, способы сбыта, дистанционный способ распространения.

Сегодня российским государством предпринимаются попытки к достаточно жесткому регулированию порядка обращения с сильнодействующими или ядовитыми веществами независимо от сфер применения (медицина, химическая отрасль, научная область либо промышленность и прочие сферы деятельности человека). Направлено такое регулирование, прежде всего, на исключение какой-либо возможности их неправомерного использования.

Средства такого рода состоят в основном из снотворных, седативных, а также нейролептических препаратов. В своем большинстве они обладают угнетающим воздействием на непосредственную деятельность разных отделов центральной нервной системы человеческого организма. Продажа такого рода препаратов и фармацевтических средств без рецепта врача на территории Российской Федерации строго запрещена.

Вызывает тревогу широкое распространение незаконного оборота указанных средств с использованием глобальной сети Интернет, а также путем создания интернет-площадок, что затрудняет выявление и пресечение уголовно-наказуемых деяний такого рода.

Деятельность, связанная с незаконным оборотом сильнодействующих, а также ядовитых веществ с целью их сбыта, в большинстве случаев осуществляется с применением мер конспирации разного рода. Кроме того, ей присущ довольно длящийся характер.

Зачастую сбыт осуществляется только отдельным лицам, которые именуются в соответствующих кругах «проверенными» покупателями. В случае осуществления незаконного оборота сильнодействующих и ядовитых веществ под прикрытием легальной предпринимательской деятельности, следы преступления зачастую нужно искать в документах бухгалтерского и инвентаризационного учета хозяйствующих субъектов, поскольку ограниченные в обороте соответствующие вещества имеют в основном названия, которые не соответствуют содержимому конкретной упаковки лекарств либо препаратов.

Места незаконного сбыта рассматриваемых веществ вне предпринимательской деятельности преступниками зачастую оборудуются техническими устройствами, которые предназначены для контрнаблюдения и противодействия сотрудникам правоохранительных органов, осуществляющим борьбу с рассматриваемой группой уголовно-наказуемых деяний.

В качестве мест постоянного незаконного хранения сильнодействующих и ядовитых веществ используются в основном занимаемые, а также снимаемые жилые помещения, подвалы, гаражи и т.п. Места хранения указанных веществ могут также располагаться в местах концентрации лиц, употребляющих наркотики (например, на рынках, возле метро, аптек, а в спальных районах).

Способы совершения уголовно-наказуемых деяний рассматриваемой группы условно можно разделить на простые и сложные.

Сложный способ предполагает определенную последовательность действий, которые должен выполнить преступник с целью реализации задуманного. Один из наиболее популярных, хотя и сложных способов совершения рассматриваемого преступления, например, состоит в том, что конечный потребитель веществ этой группы, осознавая преступность всех осуществляемых им действий, вступает в незаконный сговор с владельцами или фармацевтами аптечного либо лечебного учреждения. Основная цель такого лица состоит в получении незаконного рецепта на так называемые «лекарственные средства». Вследствие этого такой «покупатель» оплачивает как само такое лекарственное средство, так и оказанные ему «услуги» в виде изготовления рецепта, обращения в лечебное учреждение и т.п.[1]

Второй сложный способ подразумевает применение бесконтактного сбыта соответствующих веществ конечному потребителю и может выглядеть следующим образом. Поставщики веществ, указанных в данном исследовании, организовав их отправку и переправку по территории Российской Федерации, используют для этого организованную сеть диспетчеров, которые оповещают доверенных лиц о наличии такого «товара». Параллельно с отправкой они сообщают телефоны, а также номера счетов, зачастую web-кошельков, используемых для получения на них денежных средств. Потребители указанных веществ осуществляют перевод денег за «товар» на указанный счет, после чего членами группировки оборудуется тайник, в который помещаются указанные вещества. Место нахождения такого тайника диспетчером указывается заинтересованному лицу сообщением СМС, либо же сообщается через доверенных лиц. Такая структура незаконной группировки имеет четко отлаженную структуру и схему деятельности, действующую по принципу, который непосредственный контакт всех заинтересованных в данном процессе лиц исключает. При этом номера телефонов, денежные счета, счета web-кошельков с определенной периодичностью меняются. Сами диспетчерские пункты располагаются в другом регионе, который служит отправной точкой сбыта сильнодействующих и/либо ядовитых веществ.

Особенность уголовно-наказуемых деяний указанной группы состоит в том, что они не затрагивают напрямую права, а также законные интересы человека и гражданина, хотя в виде исключения можно указать на корыстно-

[1] Чистова Л.Е. Особенности криминалистической характеристики преступлений, связанных с незаконным оборотом наркотиков, совершаемых организованными преступными формированиями // Теоретико-методологические и прикладные аспекты социальных институтов права, экономики, управления и образования Материалы Всероссийской научной конференции с международным участием. Гуманитарно-социальный институт. 2016. С. 436.

насильственные преступления с использованием соответствующих веществ в качестве орудия их совершения.

Резюмируя изложенное, можно сделать следующие выводы:

1. Преступления совершаются с применением разного рода конспирации, а иными словами – маскировки.

2. Сбыт осуществляется только отдельным лицам, в соответствующих кругах именуемым «проверенными» покупателями.

3. Местами постоянного незаконного хранения сильнодействующих, а также ядовитых веществ зачастую служат занимаемые, а также снимаемые жилые помещения, подвалы, гаражи и т.п. Основная цель преступников –определить места постоянной концентрации «постоянных клиентов» – наркоманов.

4. В качестве способа совершения рассматриваемого преступления служит использование простой и сложной схемы сбыта сильнодействующих и ядовитых веществ. Простой способ состоит в непосредственной передаче указанных веществ прямому потребителю, а в сложном способе зачастую задействуется целая группа лиц, осуществляющих такую незаконную деятельность – фармацевты, владельцы аптек и т.п.

Довольно популярным стал также дистанционный способ распространения сильнодействующих и ядовитых веществ, в котором задействована преступная иерархия «производитель/сбытчик – диспетчер – конечный потребитель». Состав участников этой схемы может меняться в зависимости от масштабов деятельности такого рода.

Литература

1. Чистова Л.Е. Особенности криминалистической характеристики преступлений, связанных с незаконным оборотом наркотиков, совершаемых организованными преступными формированиями // Теоретико-методологические и прикладные аспекты социальных институтов права, экономики, управления и образования Материалы Всероссийской научной конференции с международным участием. Гуманитарно-социальный институт. 2016.

В.А. Агаян

Использование искусственного интеллекта в целях совершения преступления

Аннотация. Статья посвящена актуальной угрозе информационной безопасности, связанной с широким распространением компьютерных технологий. Автором рассматривается один из аспектов киберпреступности, а именно преступности с использованием искусственного интеллекта.

Ключевые слова: искусственный интеллект, преступление, информационная безопасность, киберпреступность, информация.

В последнее время мы практически ежедневно узнаем, как искусственный интеллект научился новым навыкам. Компьютерные алгоритмы уже умеют копировать стили рисования известных художников, имитировать чужие голоса, создавать поддельные видеоролики с публичными личностями и многое другое. Многие эксперты в сфере обеспечения информационно безопасности обеспокоены тем, что разрабатываемые технологии могут использоваться злоумышленниками для совершения преступлений.

Искусственный интеллект (ИИ) — свойство искусственных систем выполнять творческие функции, которые традиционно считаются прерогативой человека.

Некоторые формы ИИ являются или будут являться опасными по своей природе. К ним относятся случаи, когда системы с ИИ разрабатываются в военных целях, пусть даже и оборонительных. Если вы выгуливаете собаку без поводка, существует риск, что собака сбежит от вас, игнорируя ваши команды, и кого-нибудь покусает. С учетом этого риска, не принято выгуливать собаку в общественных местах без поводка. Однако не все люди придерживаются этого правила. Риск того, что собака может не послушаться команды хозяина и ранить других животных или людей, потенциально выше, чем в том случае, когда она на поводке. Системе с ИИ необходимы границы, которые бы исполняли роль собачьего поводка. Это не снимет все существующие риски выхода системы с ИИ из-под контроля, но значительно их снизит. Решающее значение для оценки рисков причинения вреда имеет вид ограничения, применяемый к ИИ.

Если производитель четко указывает, для чего предназначен ИИ и какие ограничения он имеет, то тогда стоит рассматривать риск, который может причинить система при использовании ее за границами тех условий, для которых она создавалась. Например, использование автономного автомобиля в снежную погоду, тогда как производитель заявил, что автомобиль не предназначен для эксплуатации в условиях снегопада, может рассматриваться как серьезный риск причинения вреда. Несчастные случаи более вероятны в условиях, для которых автомобиль не построен. Полагаем, что в таком случае, ответственность за причинение вреда ложиться на то лицо, которое, зная о существующих ограничениях, тем не менее, использовало систему с искусственным интеллектом за рамками разрешенных границ.[1]

Другой аспект, который необходимо рассмотреть, заключается в том, какой эффект вызывает машинное обучение и подобные методы. Большинство систем с ИИ предназначено для изучения своего окружения посредством обработки большого количества данных, так называемая технология bigdata. С помощью этой технологии ИИ принимает решения на основе того, что он смог изучить ранее. Это делает развитие ИИ непредсказуемым, то есть система может придумывать стратегии или принимать решения, которые являются непредвиденными для ее разработчиков и пользователей. Почти наверняка будут ситуации, когда в цепочке от производства до использования ИИ люди все

[1] Ерахина Е.А., Тирранен В.А. Преступления, совершаемые с использованием искусственного интеллекта: проблема квалификации и расследования // Вестник Сибирского юридического института МВД России. 2019. № 2 (35). С. 36-41.

сделали «правильно», но ИИ учится, тем не менее «не тому».[1]

В настоящее время существует множество возможностей ИИ, которые так или иначе отрицательно сказываются на жизни современного общества и в реальной жизни, и в сети.

Одним из способов использования искусственного интеллекта в целях совершения преступления является фишинг.

Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Фишинг - это тип киберпреступления, при котором преступники выдают себя за надежный источник в Интернете, чтобы вынудить жертву передать им личную информацию (например, имя пользователя, пароль, номер банковской карты).

Эволюция современных технологий привела к появлению различных инноваций, и одна из них, в частности, уже всколыхнула медиа-ландшафт - речь идет про дипфейки. Дипфейк - это видео изображение или аудиозапись, которые были обработаны с помощью технологии искусственного интеллекта. Например, на видео с дипфейком можно сделать так, чтобы человек говорил или делал что-то, чего на самом деле в реальной жизни не было.

Дипфейки выглядят очень убедительно, и продолжающееся развитие технологий только усложнило различие между реальным и поддельным контентом. Хотя технология deepfake все еще относительно нова, мы регулярно наблюдаем ее значимую роль в пугающих тенденциях в сфере мошенничества и киберпреступности. Дипфейки стали серьезной проблемой для домашних и корпоративных пользователей, поскольку они используются преступниками для проведения мошеннических афер и атак с методами социальной инженерии, а также для распространения дезинформации.

В настоящее время боты стали еще одной формой взаимодействия машин с людьми, и в такой же степени это инструмент совершения различных преступлений. Бот - это специальная программа, созданная для выполнения простых задач. С помощью нейросетей боты уже научились имитировать поведение людей - и это открыло как новые возможности, так и создало новые проблемы.[2]

С каждым годом становятся все популярнее каналы коммуникации с банками - чат-боты. Это напрямую связано с тем, что клиенты ожидают от чат-ботов максимально быстрого ответа на свои вопросы. Самые популярные сценарии преступлений с использованием банковских чат-ботов - сбор информации о пользователе, рассылка вредоносных программ и подмена робота на мошенника.[3] Специалисты по безопасности обнаружили в банковских ботах уязвимости, которые дают доступ к персональным данным клиентов и переписке

---

[1] Сокова А.А. Искусственный интеллект: возможности и необходимость его уголовно-правовой охраны // Молодой ученый. 2019. № 16. С. 122-125.

[2] Смирнов Е.В. Проблема искусственного интеллекта: автореф. дисс. … канд. юридич. наук. Магнитогорск, 2012. С. 25.

[3] Антонова Е.Ю. Технологии искусственного интеллекта - субъект преступления или орудие / средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 1. С. 31-39.

в чате. Преступники могут: узнать номер и срок действия банковской карты; получить доступ к балансу счета и номеру телефона; подтвердить перевод денег на другой счет, если код подтверждения приходит в чат. При этом доступ к банковскому чат-боту не даст преступникам полного доступа к лицевому счету жертвы. Боты используются в банковских приложениях, мессенджерах, соцсетях и контакт-центрах. Наиболее безопасным считается общение через официальное приложение или личный кабинет на сайте банка, если пользователь прошел в них аутентификацию.[1]

Известны случаи, когда на промышленных предприятиях происходят трагические ситуации, связанные с роботами, вышедшими из строя, а иногда и с абсолютно исправными роботами, имеющими недостатки в разработанной для их работы системе.[2]

В результате исследования искусственного интеллекта можно сделать следующие выводы. Наука не будет стоять на месте, ведь благодаря усилиям ученых среди людей появился искусственный интеллект. Люди думают, что это хорошо, потому что ИИ поможет людям за счет разработчиков. Но есть одно «но» - ИИ может принести не только пользу, но и вред. В конце концов, злоумышленник может создать искусственный интеллект и запрограммировать его на совершение преступлений в своих интересах. Искусственный интеллект не может быть признан независимым субъектом (ни физическим, ни юридическим лицом), потому что это всего лишь программа, разработанная программистом, и он не может быть осведомлен о совершении преступных деяний, потому что лицо, создавшее его, является программой, разработанной для выполнения воли создателя. ИИ может быть использован в качестве инструмента и средства совершения преступлений, поскольку он может непосредственно воздействовать на объект преступления или способствовать влиянию со стороны власти преступника. Признание искусственного интеллекта потерпевшим в настоящее время является несвоевременно, поскольку развитие самообучающихся компьютерных программ еще не достигло такого уровня, чтобы их сравнивали с людьми в контексте социальной значимости.

Литература

1. Агаян В.А., Пичугина И.Ю. Цифровые средства совершения преступлений или искусственный интеллект, виртуальная реальность, darknet в преступной деятельности // Актуальные вопросы обеспечения прав и свобод человека и гражданина: региональный вектор. материалы IV Всероссийской научно-практической конференции. Хабаровск, 2022. С. 106-109.
2. Антонова Е.Ю. Технологии искусственного интеллекта - субъект преступления или орудие / средство совершения преступления? //

[1] Грачева Ю.В. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15. № 6(115). С. 169-178.

[2] Williams v. Litton Systems, Inc. https://law.justia.com/cases/michigan/supreme-court/1989/81951-5.html

Юридический вестник Кубанского государственного университета. 2022. № 1. С. 31-39.
3. Грачева Ю.В. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15. № 6(115). С. 169-178.
4. Ерахина Е.А., Тирранен В.А. Преступления, совершаемые с использованием искусственного интеллекта: проблема квалификации и расследования // Вестник Сибирского юридического института МВД России. 2019. № 2 (35). С. 36-41.
5. Лапунин М.М. Обстоятельства, исключающие преступность деяния, и научно-технический прогресс // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 6 (62). С. 81–87.
6. Смирнов Е.В. Проблема искусственного интеллекта: автореф. дисс. … канд. юридич. наук. Магнитогорск, 2012. С. 25.
7. Сокова А.А. Искусственный интеллект: возможности и необходимость его уголовно-правовой охраны // Молодой ученый. 2019. № 16. С. 122-125.

П.Б. Афанасьев

Отдельные направления противодействия киберпреступности

Аннотация. Несмотря на реализуемые меры по противодействию киберпреступности, существует потребность в определении основных направлений противодействия киберпреступности. В статье автор еще раз пытается определить основные направления и, соответствующую совокупность мер, которые необходимо реализовать в целях повышения эффективности противодействия киберпреступности.

Ключевые слова: киберпреступность, предупреждение, меры противодействия, борьба, компьютерная грамотность.

Противодействие киберпреступности предполагает реализацию совокупности мер, направленных на снижение или устранение тех или иных факторов, оказывающих негативное влияние на состояние киберпреступности[1].

В числе направлений противодействия киберпреступности называется повышение кадрового потенциала правоохранительных органов.

В этих целях в Следственном комитете России был создан отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий[2], а в системе МВД России было создано Управление «К»,

[1]См.: Антонян Ю.М., Афанасьева О.Р., Гончарова М.В. Преступность в России: монография. – М., 2023; Афанасьева О.Р. Состояние киберпреступности в Германии// В сб.: Правоохранительная и правозащитная деятельность: вчера, сегодня, завтра. Сборник статей Международной научно-практической конференции. М., 2022. С. 10-14.

[2]SLEDCOM.RU // Электронный ресурс. URL: https://sledcom.ru/press/interview/item/1529946/ (дата обращения: 21.04.2023); Шиян В.И.

непосредственно специализирующееся на противодействие компьютерным преступлениям. Однако создание специализированных подразделений не может решить проблемы противодействия киберпреступности, которая демонстрирует интенсивное развитие. В этой связи в литературе отмечается необходимость создания «кибердружин», которые состояли бы из людей, добровольно помогающих правоохранительным органам в борьбе с данными преступлениями, а также постоянное повышение квалификации сотрудников.

В целях повышения профессиональной подготовки сотрудников МВД РФ в 2018 году Group-IB и Академия управления МВД России заявили о сотрудничестве в области повышения профессионального уровня преподавателей Академии и о проведении вместе научных исследований[1].

На конференции Cyber Crime Con 2018[2] также заявили о старте работы CyberSchool – центра повышения навыков и компетенции по кибербезопасности, образовательные программы которого позволяют легко адаптироваться абсолютно любому участнику, так как можно начать изучать программу, находясь на любом уровне подготовки.

Генеральная прокуратура Российской Федерации отмечает, что, несмотря на наличие специальных подразделений по борьбе с киберпреступностью в правоохранительных органах, «важно, чтобы работа на данном направлении осуществлялась качественно и целенаправленно всеми ведомствами, входящими в правоохранительную систему, с возможностью присоединения соответствующих подразделений иных компетентных органов, прежде всего Росфинмониторинга, Роскомнадзора и Банка России»[3], что обусловлено необходимостью создания единой системы борьбы с киберпреступлениями. Одним из возможных путей создания такой системы было бы заключение соглашения об электронном обмене информацией между органами государственной власти и службами при взаимодействии с банками, операторами связи и т.д. Центром, координирующим борьбу с киберпреступностью, мог бы стать созданный при ФСБ Национальный координационный центр по компьютерным преступлениям или же созданный межведомственный орган по координации деятельности в круглосуточном режиме.

Криминологические аспекты противодействия преступлениям, совершаемым с использованием информационно- телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 168-171.

[1] Group-IB и Академия Управления МВД заключили соглашение о партнерстве в сфере подготовки кадров [Электронный ресурс] URL: https://www.facct.ru/media-center/press-releases/gib-amvd/?ysclid=ljcdkyc3ts196602402 (дата обращения: 24.04.2023).

[2] GROUP-IB // Электронный ресурс. URL: https://www.group-ib.ru/media-center/press-releases/cybercrimecon-2018-summary/ (дата обращения: 24.04.2023).

[3] TASS.RU // Электронный ресурс. URL: https://tass.ru/obschestvo/9032391 (дата обращения: 24.04.20223); Саркисян А.Ж., Иоффе М.И. Особенности обеспечения кибербезопасности при проведении важных общественно-политических, спортивных и иных мероприятий международного уровня в рамках противодействия экстремизму // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. № 1. С. 48-52.

Специализированные подразделения создаются не только в правоохранительных органах, но и иных организациях. Так, «в 2015 г. Центральным банком РФ по поручению Совета Безопасности РФ был организован Центр борьбы с киберугрозами финансового характера»[1], направлениями деятельности которого является сбор данных о кибератаках на банки и клиентов банков, о возможных кибератаках, а также передача этих данных учреждениям в сфере финансов. Банки обмениваются телефонами и номерами карт злоумышленников — на федеральном, региональном и отраслевом уровнях.

В следующего направления противодействия киберпреступности называется – повышение компьютерной грамотности населения[2]. В рамках данного направления предлагается обучать пользователей ПК тем тактикам, которые используются киберпреступниками для достижения своих преступных целей. Обучение предлагается проводить путем периодических практических занятий и лекций. Однако у этого метода есть и свой минус: затратность, особенно принимая во внимание факт того, что тактики фишинга изо дня в день видоизменяются.

В связи с этим представляет интерес идея распространения учебного материала по телевидению, радиовещанию и в «Интернет»-пространстве. «В ряды познавательных передач еженедельно можно включать программы, которые на примере обманутых граждан продемонстрируют способы и лазейки мошеннических комбинаций, которыми пользуются злоумышленники»[3].

В работе С.С. Симоновой «Противодействие киберпреступности в России и зарубежных странах: криминологический и виктимологический аспекты»[4] предлагается использование технологии интеллектуального машинного обучения. Суть этой технологии заключается в следующем: в браузер внедряется особая программа классификации, которая способна обнаружить фишинговые атаки и мгновенно передать об этом информацию пользователю. Кроме того, в научном труде отмечается наибольшая важность в проведении семинаров, позволяющих предупредить киберпреступность, среди лиц несовершеннолетнего и пожилого возраста, так как именно эти категории лиц наиболее часто становятся жертвами киберпреступников. Причем среди лиц преклонного возраста больше всего жертв, подвергшихся мошенническим

[1] Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник Воронежского института МВД России. — 2020. — № 3. — С. 258.

[2] Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — № 2. — С.273.

[3] Орлова М.С. Преступления, совершаемые посредством информационно-телекоммуникационных технологий: основные криминологические показатели и особенности предупреждения // Астерион. – 2021. – С. 188.

[4] Симонова С.С. Противодействие киберпреступности в России и зарубежных странах: криминологический и виктимологический аспекты // Вестник Российского нового университета. – 2022. - № 3. – С. 60-61.

действиям, а среди подростков – кибербуллингу, фишингу и насилию как психического, так и сексуального характера.

Ряд исследователей в качестве действенной меры отмечают факт внесения в трудовой договор при приеме на работу новых сотрудников пункта об ответственности за разглашение конфиденциальных сведений о системе обеспечения безопасности служебной информации юридического лица. Кроме того, предлагается осуществлять постоянный контроль за тем, чтобы своевременно устанавливались и обновлялись программы-антивирусы на технических устройствах сотрудников[1].

Необходимо понимать, что меры по пресечению киберпреступности должна реализовываться не только государственными органами, отдельными юридическими лицами, но и гражданами, поскольку только комплексный подход позволит повысить эффективность противодействия преступности.

Кроме того, существует необходимость в проведении криминологических исследований, которые помогли бы сформировать новую концепцию борьбы с киберпреступностью и поспособствовали бы формированию правоприменительной практики, основанной на рекомендациях, выработанных научными специалистами в данной сфере[2].

Таким образом, изучив совокупность мер, реализуемых в настоящий момент в сфере предупреждения и устранения последствий киберпреступности, можно сделать вывод о том, что в России наличествует множество недостатков не только в сфере правового регулирования, но и в системе противодействия киберпреступности. Можно заметить, что, несмотря на создание подразделений по борьбе с киберпреступностью в правоохранительных органах, их взаимодействие с общественными организациями, до сих существует ряд проблем, требующих разрешения. Ощущается потребность в объединении сил абсолютно всех участников, задействованных в информационной сфере и напрямую заинтересованных в борьбе с киберпреступностью: органов государственной власти, предпринимателей, общественных организаций и граждан.

Литература

1. Антонян Ю.М., Афанасьева О.Р., Гончарова М.В. Преступность в России: монография. – М., 2023. 272 с.
2. Афанасьева О.Р. Состояние киберпреступности в Германии// В сб.: Правоохранительная и правозащитная деятельность: вчера, сегодня, завтра. Сборник статей Международной научно-практической конференции. Москва, 2022. С. 10-14.

[1] Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — № 2. — С.273.

[2] Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. – 2012. – С. 16.

3. Орлова М.С. Преступления, совершаемые посредством информационно-телекоммуникационных технологий: основные криминологические показатели и особенности предупреждения // Астерион. – 2021. – С. 186-188.
4. Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. – 2012. – С. 10-16.
5. Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — № 2. — С.265-276.
6. Саркисян А.Ж., Иоффе М.И. Особенности обеспечения кибербезопасности при проведении важных общественно-политических, спортивных и иных мероприятий международного уровня в рамках противодействия экстремизму // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. № 1. С. 48-52.
7. Симонова С.С. Противодействие киберпреступности в России и зарубежных странах: криминологический и виктимологический аспекты // Вестник Российского нового университета. – 2022. - № 3. – С. 58-62.
8. Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник Воронежского института МВД России. — 2020. — № 3. — С. 256-262.
9. Шиян В.И. Криминологические аспекты противодействия преступлениям, совершаемым с использованием информационно- телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 168-171.

О.Р. Афанасьева

Детерминанты киберпреступности

Аннотация. Современное состояние киберпреступности предопределяет интерес к причинам, ее порождающим. В статье автор определяет перечень детерминант преступности и уделяет внимание характеристике некоторых из них.

Ключевые слова: киберпреступность, предупреждение, причина преступности, детерминанта, условие преступности.

Для анализа киберпреступности и определения способов борьбы с ней, необходимо понимать причины и условия, способствующие ее развитию.

Определение причин и условий преступности считается одной из главных тем в криминологической науке[1].

Причины киберпреступности можно разделить на следующие виды: социальные, экономические, правовые, организационные и политические, в их числе можно отметить следующие.

1. Повсеместный доступ к сети «Интернет».

Креативное агентство We Are Social и сервис для SMM Hootsuite опубликовали свое ежегодное исследование сети Интернет (Digital 2022 Global Overview Report[2]). В соответствии с представленным отчетом население мира составляет 7,91 млрд человек. Число пользователей сети «Интернет» во всем мире к началу 2022 года выросло до 4,95 миллиарда, а это 62,5% от общей численности населения мира. Данные показывают, что за последний год число пользователей «Интернета» выросло на 192 миллиона (+ 4%). Опираясь на эти данные, становится очевидным факт вовлечения чуть ли ни всей планеты в сеть, и становится очевидным рост киберпреступности. Такой прирост числа пользователей, развитие различных операций, проводимых через «Интернет» (электронная торговля, банковские счета), факт того, что в настоящее время отсутствует легальное определение «киберпреступность», разрозненность противодействия киберпреступности негативно отражается на состоянии преступности.

2. Негативное влияние «Интернета» на личность киберпреступника и иллюзии, создаваемые сетью.

Относительно психологического аспекта киберпреступлений нужно обратить внимание на ее анонимность, которая позволяет преступнику, как он считает, повысить свой социальный статус, особенно если в жизни он совершенно не состоялся как личность. Погружаясь в виртуальный мир, человек уходит от реальности, воображая себя героем, меняет привычный социальный статус. Интернет дает ему иллюзию самодостаточности. Кроме того, такой «герой» не чувствует опасности, ведь в ответ на его противоправные действия не последует негативной реакции со стороны общества, он как бы прячется в сети, отгораживая себя от психологического воздействия других людей. У него есть группа единомышленников, которая с ним заодно, а большего ему и не надо.

3. Организованный и транснациональный характер киберпреступности.

Так как основной проблемой выявления и расследования компьютерных преступлений является их транснациональный и трансграничный характер, который затрудняет процесс их расследования и раскрытия, то требуется

---

[1] Гончарова М.В., Шиян В.И. Состояние и тенденции современной киберпреступности// Вестник Академии Следственного комитета Российской Федерации. 2021. № 1 (27). С. 53-56; Афанасьев П.Б. Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 10-14.

[2] We are social [Электронный ресурс]. URL: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ (дата обращения: 16.04.2023).

объединение сил всего мирового сообщества, направленных на борьбу с компьютерной преступностью.

Важно понимать, что характерной чертой киберпреступности также является ее латентность, значительная часть преступлений скрыта от правоохранительных органов, поэтому нельзя с точностью оценить ее реальные показатели, они существенно отличаются от официальной статистики. Одной из причин латентности является то, что «убыток от киберпреступления часто кажется жертве незначительным по сравнению с процедурой расследования»[1], из-за чего многие преступления в этой сфере остаются нераскрытыми.

4. Несовершенство законодательства.

В отечественном уголовном законодательстве отсутствует ответственность за такие деяния как «троллинг», «сталкинг», кибербуллинг; кроме того, отсутствует понятие «киберпреступности»; в нормативно-правовой базе не регламентируется вопрос оценки ущерба, возникшего из-за компьютерного преступления и т.д.

5. Отсутствие единых стандартов безопасности для компьютерных программ.

6. Низкая грамотность населения в сфере информационно-телекоммуникационных технологий.

В криминологической науке наличествует мнение о том, что возрастанию уровня киберпреступности способствует низкий уровень информационного развития общества в России. Граждане, порой, не знают самых основ обращения с техникой, не считают нужным проверять достоверность сайтов, которые они посещают. Некоторые не считают нужным устанавливать антивирусные программы. Из-за недостатка знаний в рассматриваемой области злоумышленникам открывается простор для совершения все новых преступлений.

Так, С. Шебзухов по результатам исследования обращает внимание, что из числа опрошенных им 98,6 % - пользуются Интернет-банками, у 94,4 % граждан есть аккаунты в социальных сетях «Вконтакте» и «Instagram». При этом у 67,6 % опрошенных один и тот же пароль для нескольких соцсетей, у 57,7 % пароль включает в себя только цифры и буквы, что считается ненадежным. 46,5 % респондентов не проверяют адресную строку, когда вводят пароль, что создает реальную угрозу фишинг-атаки в отношении этих граждан[2].

7. Недостаточный профессиональный уровень сотрудников органов, деятельность которых направлена на борьбу с киберпреступностью.

Несмотря на создание специализированных подразделений правоохранительных органов отмечается проблема профессиональной

[1] Кучерков И.А. О понятии киберпреступление в законодательстве и научной доктрине // Юридическая наука. — 2019. — С. 80.

[2] Шебзухов С. Киберпреступность в современной России: причины и условия // Право и жизнь. — 2021.

подготовки кандидатов на должности в данные подразделения[1]. Данные подразделения комплектуются сотрудниками, у которых есть опыт работы по борьбе с преступностью в сфере экономики или же теми, у которых есть опыт в раскрытии правонарушений в сфере нарушения авторских и смежных прав и изъятия контрафактной продукции, но все еще они не обладают знаниями и навыками, необходимыми для проведения расследования киберпреступлений.

8. Отставание мер безопасности, реализуемых государством, от уровня возможностей злоумышленников.

9. Недостаточный уровень информационной безопасности в большинстве организаций.

10. Отсутствие должного уровня взаимодействия между всеми субъектами противодействия киберпреступности, то есть «отсутствие скоординированности в работе государственных и общественных структур в сфере обеспечения информационной безопасности»[2].

11. Высокая стоимость лицензионного программного обеспечения, монополизм разработчиков программ для компьютеров, недобросовестная конкуренция между производителями программного обеспечения и антивирусных программ.

Монополизм позволяет разработчикам повышать цены на компьютерные продукты, в связи с чем многие пользователи задумываются о приобретении более дешевых версий программ, и в результате оказываются жертвами преступлений.

Таким образом, представленный перечень детерминант киберпреступности свидетельствует о наличии комплекса причин и условий детерминант преступности, требующих, соответственно, реализации комплекса мер, направленных на противодействие киберпреступности.

Литература

1. Афанасьев П.Б. Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 10-14.
2. Гончарова М.В., Шиян В.И. Состояние и тенденции современной киберпреступности// Вестник Академии Следственного комитета

[1] Тутуков А.Ю. Основные детерминанты компьютерной преступности в Российской Федерации // Пробелы в российском законодательстве. — Юридический журнал. — 2018; Лагутин П. Д., Миханова Т. А. Киберпреступность как актуальная угроза обществу // Молодой ученый. — 2018. — № 42 (228). — С. 108-109.

[2] Попов А. Н. Преступления в сфере компьютерной информации: учебное пособие. – СПб. 2018. — С. 16; Саркисян А.Ж., Иоффе М.И. Особенности обеспечения кибербезопасности при проведении важных общественно-политических, спортивных и иных мероприятий международного уровня в рамках противодействия экстремизму // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. № 1. С. 48-52.

Российской Федерации. 2021. № 1 (27). С. 53-56.
3. Кучерков И.А. О понятии киберпреступление в законодательстве и научной доктрине // Юридическая наука. — 2019. — С. 78-81.
4. Лагутин П. Д., Миханова Т. А. Киберпреступность как актуальная угроза обществу // Молодой ученый. — 2018. — № 42 (228). — С. 108-109.
5. Попов А. Н. Преступления в сфере компьютерной информации: учебное пособие. – СПб. 2018.
6. Саркисян А.Ж., Иоффе М.И. Особенности обеспечения кибербезопасности при проведении важных общественно-политических, спортивных и иных мероприятий международного уровня в рамках противодействия экстремизму // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. № 1. С. 48-52.
7. Тутуков А.Ю. Основные детерминанты компьютерной преступности в Российской Федерации // Пробелы в российском законодательстве. — Юридический журнал. — 2018.
8. Шебзухов С. Киберпреступность в современной России: причины и условия // Право и жизнь. — 2021.

З.М. Бешукова

Киберпреступность в пандемийный и постпандемийный периоды: динамика и основные тренды

Аннотация. В статье анализируются официальные статистические данные о числе преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, за период с 2018 по 2022 гг. Сделан вывод, что в Российской Федерации допандемийный уровень таких преступлений характеризуется негативной тенденцией к стабильному повышению. Однако все же пик роста таких преступлений приходится на первый год пандемии. На основе анализа отчета Интерпола «Киберпреступность: воздействие COVID-19» приводятся основные тренды киберпреступности в период пандемии коронавирусной инфекции. В постпандемийный период уровень киберпреступлений не снизился, однако и скачка вверх уровня таких преступлений также не произошло.

Ключевые слова: киберпреступления, кибербезопасность, COVID-19, фишинг, мошенничество, компьютерные преступления, блокчейн-технологии, вредоносное программное обеспечение, Интерпол.

Пандемия коронавирусной инфекции нанесла серьезный ущерб мировой экономике, экономическому развитию значительного числа отдельно взятых государств, масштабным потрясениям подверглись также социальная сфера и культура многих стран. Не осталась в стороне от влияния пандемии и преступность. Введение ограничительных мер, связанных с предотвращением распространения новой коронавирусной инфекции, привело к снижению количества преступлений в ряде стран мира, вместе с тем серьезные изменения

произошли в структуре преступности. Впрочем, это вполне логично и было вполне прогнозируемо. Так, например, ограничение свободного передвижения закономерно привело к снижению уличной преступности, количеству краж из жилых помещений, а также преступлений, совершаемых лицами без гражданства и иностранными гражданами, и др.[1]

В контексте сказанного необходимо отметить также и то, что пандемия коронавирусной инфекции вызвала социальную напряженность, что явилось одной из причин роста числа преступлений, являющихся проявлениями экстремистской и террористической деятельности. Существенный рост числа преступлений, совершаемых в киберпространстве, в условиях ограничительных мер был также неизбежен. В период пандемии COVID-19 во всем мире наблюдается резкий рост киберпреступности. Если говорить о состоянии преступности в обозначенный период в Российской Федерации, то убедительно сказанное доказывают официальные статистические данные[2], представленные для наглядности в таблице 1.

Таблица 1 – Зарегистрировано преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий

Годы	2018	2019	2020	2021	2022
Количество преступлений	174 674	294 409	510 396	517 722	522 065

Как видим, в РФ допандемийный уровень преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, характеризуется негативной тенденцией к стабильному повышению. Однако все же пик роста таких преступлений приходится на первый год пандемии – 2020 г. (+ 215 987 преступлений или на 73,4% больше, чем за аналогичный период прошлого года). По данным Министерства внутренних дел РФ в 2020 г. больше половины таких преступлений (52,4%) относится к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5%); больше половины (58,8%) совершается с использованием сети «Интернет»: 300,3 тыс. (+91,3%), почти половина (42,9%) – средств мобильной связи: 218,7 тыс. (+88,3%). Четыре таких преступления (80,4%) из пяти совершаются путем кражи или мошенничества: 410,5 тыс. (+74,3%), почти каждое одиннадцатое (9,2%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 47,1 тыс. (+90,7%)[3].

Если говорить о влиянии пандемии на киберпреступность в глобальном (общемировом) масштабе, то по данным Интерпола уровень киберпреступности повысился во всех странах. Однако при этом данной организацией сделан вывод,

[1] Трахов А.И., Бешукова З.М. Бланкетность антиэкстремистских норм уголовного закона: как решить уравнение с неизвестным количеством переменных (на примере статьи 280 УК РФ)? // Гуманитарные, социально-экономические и общественные науки. 2022. № 4. С. 168.

[2] Данные о состоянии преступности в России // Официальный сайт МВД России. URL: https://мвд.рф/folder/101762 (дата обращения: 15.05.2023)

[3] Там же.

что, несмотря на то, что физические лица столкнулись с угрозами, связанными с хакерскими атаками, фишингом, мошенничеством и другими видами киберпреступности, целью киберпреступников в обозначенный период все чаще становились крупные корпорации и объекты критической инфраструктуры.

В контексте данного исследования важно отметить, что Интерполом был подготовлен на основе данных, полученных из 48 стран-членов и от 4 частных партнеров, аналитический отчет «Киберпреступность: воздействие COVID-19» (далее по тексту – Отчет)[1]. В Отчет кроме этих данных также были включены материалы, подготовленные подразделением Интерпола по реагированию на киберпреступления (CTR) и его Центром кибербезопасности (CFC).

Приведем основные выводы о влиянии пандемии на киберпреступность, содержащиеся в Отчете:

1. Интернет-мошенничество и фишинг. Воспользовавшись пандемией, киберпреступники пересмотрели свои обычные схемы онлайн-мошенничества и фишинга. Так, они рассылали электронные письма или сообщения на тему COVID-19 со ссылками на вредоносные сайты или копии страниц, чтобы получить доступ к данным пользователей. При этом злоумышленники выдавали себя в большинстве своем за органы здравоохранения.

2. Подрывное вредоносное программное обеспечение (программы-вымогатели и DDos). Киберпреступники все чаще использовали вредоносное программное обеспечение против объектов критической инфраструктуры и системы здравоохранения, которое приводило к сбоям или полной остановке бизнес-процессов, а также к временной или постоянной утере важных данных.

Одной из главных тенденций также стало увеличение количества атак на технологические решения, используемые для удаленной работы. Киберпреступники активно атаковали слабо защищенные системы VPN, электронную почту и видеоконференции, используемые для связи на удаленной работе. Полученная информация продавалась на черном рынке или использовалась для шантажа.

3. Вредоносное программное обеспечение для сбора данных. Киберпреступники, используя информацию, связанную с COVID-19, в качестве приманки, проникали в системы для компрометации сетей, кражи данных, перевода денег и создания ботнет сетей.

4. Атаки на веб-платформы и злонамеренное использование блокчейн-технологий. Из-за увеличения количества онлайн-транзакций и банковских операций киберпреступники также начали усиленно атаковать финансовые учреждения. Они стали использовать новые методы, такие как атаки на веб-платформы и злонамеренное использование блокчейн-технологий, чтобы украсть деньги.

5. Вредоносные домены. Значительно увеличилось число киберпреступников, регистрирующих доменные имена с содержанием таких ключевых слов как

[1] COVID-19 Cybercrime Analysis Report - August 2020. URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (дата обращения: 15.05.2023).

«коронавирус» или «COVID». К слову, в период с января по 5 марта 2020 г. в мире было зарегистрировано около 4 000 доменов, имена которых имели смысловую привязку к COVID-19. На конец марта этого же года счет уже шел на тысячи регистрирующихся ежедневно доменных имен с этой тематикой. В России в период с 1 января по 27 марта 2020 г. в домене .RU было зарегистрировано 1310, а в домене .РФ 324 доменных имени, в которых встречались слова corona, covid, virus, корона, ковид, вирус[1].

Созданные веб-сайты, выглядевшие как официальные источники информации о пандемии, лежали в основе широкого спектра вредоносных действий.

6. Распространение ложной информации. Неопределенность социально-экономической ситуации в мире, неадекватно понятые угрозы, а также теории заговора способствовали росту беспокойства среди населения, а в некоторых случаях способствовали совершению кибератак.

Подводя итог, можно сделать вывод, что киберпреступность очень быстро адаптировалась к ситуации сложившейся во всем мире из-за пандемии коронавирусной инфекции. Она стала более агрессивной и организованной. В постпандемийный год (2022 г.) уровень киберпреступлений не снизился, однако и резкого скачка вверх уровня таких преступлений также не произошло.

Литература

1. Трахов А.И., Бешукова З.М. Бланкетность антиэкстремистских норм уголовного закона: как решить уравнение с неизвестным количеством переменных (на примере статьи 280 УК РФ)? // Гуманитарные, социально-экономические и общественные науки. – 2022. – № 4. – С. 168–173.

В.В. Бычков

К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей

Аннотация. В статье приводятся высказывания Президента России В.В. Путина, Секретаря Совета безопасности России Н.П. Патрушева, Председателя Следственного комитета Российской Федерации А.И. Бастрыкина о необходимости противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационные сети. Доводятся статистические данные, относящиеся к преступлениям данного вида. Раскрывается проблематика противодействия киберэкстремизму. Формулируется необходимость разработки научно

[1] В доменах .RU и .РФ зарегистрировано 1638 «коронавирусных» доменов. URL: https://www.tssonline.ru/news/v-domenah-tu-i-rf-zaregestrirovano-bolee-1638-koronavirusnih-domenov (дата обращения: 15.05.2023).

обоснованных способов их разрешения и выполнение установок высшего руководства страны на формирование государственной программы борьбы с современным экстремизмом.

Ключевые слова: экстремизм, преступления экстремистской направленности, киберэкстремизм, информационно-телекоммуникационные сети, Интернет, мобильная телефония, противодействие, раскрытие, расследование, Специальная военная операция.

За последнее десятилетие, с 2013 г. по 2022 г., в Российской Федерации фиксируется рост экстремистской деятельности. Если в 2013 г. было отмечено 896[1] преступлений экстремистской направленности, то в 2022 г. уже 1566. Следует отметить, что с 2017 г. по 2019 г. снижение их количества с 1521 до 585 объясняется их частичной декриминализацией. Однако за последующие четыре года их количество увеличилось более чем в 2,5 раза.

При этом отмечается и резкий рост информатизации и компьютеризации российского общества. В 2022 г. в России было зафиксировано 106 млн. пользователей социальных сетей, что на 7 млн больше, чем в 2021 г., и более 227 млн сотовых мобильных подключений, с 2021 г. их количество увеличилось на более 4 млн. На начало 2022 г. Интернетом в стране пользовалось 89% населения[2].

В этих условиях отмечается быстрый рост «высокотехнологичной» преступности с широким использованием современных компьютеризованных устройств и информационных технологий. Если в 2019 г. с использованием Интернета было совершено 157 тыс. 36 преступлений[3], то в 2020 г. – уже 300 тыс. 337, в 2021 г. – 351 тыс. 463, в 2022 г. – 381 тыс. 112. То есть за четыре года произошел рост преступности данного вида почти в 2,5 раза.

Возрастающая общественная опасность экстремистских проявлений многократно отмечалась в выступлениях высшего руководства страны, поручениях Президента России В.В. Путина о необходимости оперативного пресечения распространения экстремистской идеологии. В частности, выступая в феврале 2023 г. на заседании коллегии ФСБ России, он акцентировал: «… должна быть продолжена работа по выявлению и пресечению действий тех, кто использует Интернет и социальные сети для пропаганды идеологии терроризма и экстремизма, кто пытается вовлечь в террористические группировки наших граждан, конечно, мы с вами хорошо знаем, наиболее уязвимая категория здесь – это молодёжь. Столь же активно надо противодействовать экстремизму»[4].

---

[1] Здесь и далее: Официальный сайт МВД России. Состояние преступности. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics.

[2] Интернет в России в 2022 году: самые важные цифры и статистика. URL: https://www.web-canape.ru/business/internet-v-rossii-v-2022-godu-samye-vazhnye-cifry-i-statistika.

[3] Здесь и далее: Официальный сайт МВД России. Состояние преступности. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics.

[4] Заседание коллегии ФСБ России. Владимир Путин принял участие в расширенном заседании коллегии Федеральной службы безопасности. URL: http://kremlin.ru/events/president/news/70597.

В связи с особой опасностью экстремизма для общества и государства противодействие ему является прерогативой правоохранительных органов.

Секретарь Совета безопасности России Н.П. Патрушев в марте 2023 г. на совещании по национальной безопасности обратил внимание, что экстремистские организации проявляют высокую активность в информационном пространстве. При этом растет количество преступлений экстремистской направленности, совершаемых с использованием Интернета[1].

Так, Председатель Следственного комитета Российской Федерации А.И. Бастрыкин в одном из интервью средствам массовой информации заявил, что «совместно с другими правоохранительными органами мы противодействуем терроризму и экстремизму»[2].

В ряде нормативных правовых актов, принятых в последние годы в Российской Федерации, констатировано возникновение новых проблем борьбы с преступностью, возникающих из-за сложных процессов социально-экономического развития в условиях перехода к информационному обществу[3]. Многие из них связаны со всеобщей компьютеризацией, использованием глобальных информационно-телекоммуникационных сетей и повсеместным распространением мобильной телефонии с ее новыми возможностями доступа к Интернету.

С использованием средств мобильной связи в 2019 г. было совершено 116 тыс. 154 преступления, в 2020 г. – их количество увеличилось почти в два раза – до 218 тыс. 739, и последующие года этот показатель фактически стабилен: в 2021 г. – 217 тыс. 552, в 2022 г. – 212 тыс. 963.

Интернет и мобильная телефония все шире используется при совершении преступлений экстремистской направленности. Так, если в 2019 г. было зафиксировано 257 публичных призывов к осуществлению экстремистской деятельности (ст. 280 УК РФ) с использованием компьютерных и телекоммуникационных технологий, то в 2020 г. уже 340, в 2021 г. – 455, в 2022 г. – 493. То есть за четыре года произошел рост преступности данного вида почти в два раза

При этом усиливающийся мониторинг правоохранителями Интернета в части экстремистской деятельности заставляет экстремистов переходить в закодированные («закрытые») сети Интернета, так называемые, «ДаркНет»

---

[1] Патрушев предупредил о попытках экстремистов снизить уровень поддержки СВО. URL: https://tass.ru/politika/17325733.

[2] Следование западным ценностям не лучшим образом сказывается на развитии общества. Александр Бастрыкин в интервью «РГ» раскрыл секреты обучения следователей // Российская газета. 2022. 6 сентября.

[3] Указы Президента РФ: от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»; от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»; от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»; от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года»; от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»; от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» и др.

(«Скрытая сеть», «Темный интернет», «Тёмная сеть», «Теневая сеть», «Тёмный веб») и «Глубинный Интернет» («Глубокая сеть», «Невидимая сеть», «Глубокая паутина», «Глубокий интернет»), где осуществляется вербовка, связь с кураторами, оплата экстремистской деятельности, распространяются методические рекомендации по совершению указанных преступлений[1].При этом отмечаются проявления множественности преступлений данного вида с различными формами соучастия, в том числе «перекрестного». В них вовлекаются лица разного возраста, обладающие компетенциями в использовании современных информационных технологий, что активно используется членами экстремистских сообществ и организаций.

Результаты анализа важнейших особенностей преступлений в сфере киберэкстремизма, так называемого киберэкстремизма, по имеющимся сведениям о практике их расследования, показывают, что во многих случаях речь идет не об одном, а об определенной совокупности преступлений. При этом фиксируются весьма разветвленные и «совмещенные» формы соучастия в сложных формах проявлений множественности киберэкстремизма. Более того, во многих случаях в рамках киберэкстремизма выделяются несколько этапов, связанных с организацией группы исполнителей определенных видов таких преступлений, в том числе, иностранными агентами, когда приготовления к их совершению и сокрытию на каждом этапе могут представлять собой самостоятельное преступление.

При расследовании преступлений данного вида возникает ряд проблем, связанных с их адекватной уголовно-правовой характеристикой, отделением признаков каждого из преступлений, анализом особенностей проявления их множественности, включая идеальные и реальные совокупности преступлений различного вида, установлением конкретных форм соучастия вовлеченных в них субъектов.

Более того, во многих случаях в рамках киберэкстремизма выделяются несколько этапов, связанных с организацией группы исполнителей таких преступлений, приготовления к их совершению и сокрытию, каждый из которых может представлять самостоятельное преступление. То есть при раскрытии и расследования преступлений данного вида возникает ряд проблем, связанных с отделением признаков каждого из преступлений, анализом особенностей из возможных совокупностей, а также установления конкретных форм соучастия вовлеченных в них субъектов. Аналогичные выводы можно сделать и в отношении проблем, связанных с идентификацией личностных качеств субъектов данных преступлений, их мотивации и связей с современными социально-политическими процессами.

Рассматривая проблемы борьбы с «высокотехнологичными» проявлениями подготовки и сопровождения экстремизма в его «традиционном» понимании с криминалистических позиций, нельзя не отметить следующие тенденции. С

[1] За посещение каких сайтов Даркнета вас могут посадить? URL: https://deadlylaugh.ru/wall?i=111111116_56; Путешествие по Даркнету. Обходим самые злачные места .onion. URL: https://xakep.ru/2018/12/29/darknet-russia.

одной стороны – совершенствование способов приготовления к преступлениям рассматриваемого вида и их информационному сопровождению, а также маскировки данной части киберэкстремизма происходит с использованием все более изощренных схем и современного инструментария. В преступную деятельность данного вида вовлекается большое количество лиц, обладающих высоким уровнем специальных знаний и профессиональных компетенций в различных сферах информационных технологий, включая применение искусственного интеллекта. Но с другой стороны, многие ученые отмечают явное отставание в разработке криминалистической техники, тактики и методики применительно к сфере борьбы с киберэкстремизмом.

Вместе с тем, в последние годы был выпущен ряд публикаций, раскрывающих особенности подобных разработок в рамках соответствующих разделов компьютерной криминалистики применительно к различным видам преступных проявлений в ряде сфер традиционной и цифровой экономики и финансов. При этом речь идет о проблемно-ориентированном применении в борьбе с современной высокотехнологичной преступностью и определенных элементов искусственного интеллекта в составе интерактивных экспертных систем, сориентированных на надлежащее информационное обеспечение широкого спектра следственных действий.

С позиций криминалистической науки можно сделать ряд выводов о том, что по результатам обобщения уже накопленного опыта в разработке современного инструментария компьютерной криминалистики, сориентированного на раскрытие и расследование преступлений в сфере экономики, необходимо развернуть соответствующие разработки и применительно к другим видам высокотехнологичных преступлений. А отмеченные выше нарастающие негативные тенденции развития современного экстремизма, и прежде всего, киберэкстремизма, требуют принятия безотлагательных мер для обеспечения сотрудников правоохранительных органов современным, научно обоснованным и выверенным с правовых позиций криминалистическим инструментарием, позволяющим существенно повысить эффективность выявления, раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием Интернета.

Кроме того, с началом Специальной военной операции по денацификации и демилитаризации неонацистского режима в Украине информационные атаки на российских граждан с использованием Интернета не только резко возросли по объему, но и стали откровенно русофобскими. При этом не скрывается их системно организованный характер, а также попытки связать в единый комплекс нескольких видов киберэкстремизма с террористическими актами. Для стимулирования этой деятельности используются различные схемы их финансирования, а также совершения «маскирующих» преступлений в рамках единой совокупности с «основным» преступлением, учитывая особенности сложившейся реальной практики выявления, раскрытия и расследования преступлений данного вида.

В повестку дня встает ряд вопросов о применении в борьбе с киберэкстремизмом всего комплекса тех возможностей, которые развиты в рамках наук уголовно-правового блока, обогатив их новым инструментарием

наук информационного блока, выверенным с правовой точки зрения. Такой подход полностью отвечает установкам государственной политики по созданию новой научной специальности 5.1.4 «Уголовно-правовые науки». При этом интегрирующую роль в создания нового инструментария в борьбе с киберэкстремизмом может взять на себя криминалистика.

Таким образом, вышесказанное определяет не только актуальность исследования проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, но и его целевую установку на разработку научно обоснованных способов их разрешения и выполнение установок высшего руководства страны на формирование государственной программы борьбы с современным экстремизмом, тесно связанным с терроризмом, и его общественно опасными последствиями.

С.В. Валов

Результаты аналитических исследований субъектов кибербезопасности и реагирования на инциденты в системе информации о киберпреступности

Аннотация. Получение максимально полной информации о киберпреступности позволит всесторонне оценивать исходящие от неё угрозы и комплексно подходить к разработке мер противодействия и наступательной борьбы с различными её проявлениями в социальном пространстве в реальном и виртуальном измерениях. Дана оценка в недостаточной степени востребованной в криминологических исследованиях информации, полученной профессиональными субъектами обеспечения кибербезопасности.

Ключевые слова: киберпреступность, кибербезопасность, аналитические данные, криминологическая характеристика, показатели преступности.

На технологической основе достижений четвертой промышленной революции, предоставившей человечеству оригинальные сочетания физических, биологических и социальных систем[1], произошли качественные изменения, характеризуемые переходом от единичных случаев противоправного использования программно-аппаратных средств до не знающей государственных границ киберпреступности[2].

Масштабы противоправного воздействия киберпреступлений на различные сферы социальной жизни привели к тому, что сформировался автономный от правоохранительных органов сегмент, в котором действуют субъекты, профессионально осуществляющие функции обеспечения кибербезопасности и защиты определённых интересов, прав и свобод индивидуальных и

[1] Шваб, К. Четвертая промышленная революция. М.: «Эксмо», 2016.

[2] Герке, М. Понимание киберпреступности: Явление, задачи и законодательный ответ // Электронный ресурс. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf <дата обращения: 26.04.2023>.

коллективных пользователей современных информационно-коммуникационных и иных цифровых технологий. Если правоохранительные органы действуют в киберпространстве во исполнение возложенных на них публичных функций, то субъекты, оказывающие услуги комплексной защиты и оперативного реагирования на инциденты в сфере обеспечения кибербезопасности, преследуют коммерческие интересы, поскольку предлагаемые ими решения и продукты востребованы на рынке. По экспертным оценкам, в настоящее время на российском рынке действует 230 отечественных компаний-разработчиков продуктов и поставщиков услуг в сфере информационной безопасности в следующих сегментах: «Защита инфраструктуры», «Мониторинг, исследование и анализ», «Защита данных» и «Услуги и сервисы»[1]. В каждом сегменте выделены специализированные направления оказания услуг. Отдельные игроки представлены во всех сегментах.

Из субъектов, которые предоставляют для публичного обозрения результаты проведённых ими аналитических исследований состояния и изменений противоправных посягательств, мотивации и технологической оснащённости киберпреступности, реальной и виртуальной географии направленности атак и расположения очагов активности, выделим аналитические исследования Kaspersky[2], «Ростелеком-Солар»[3]; Positive Technology[4], IB-Group[5] (в 2023 г. в России ребрендинг в F.A.C.C.T.[6]). Учитывая трансграничный характер глобального информационного поля, в контексте рассматриваемой проблемы обратим внимание на иностранные аналитические исследования тенденций и трендов трансформации киберпреступности[7].

Все доступные для публичного доступа аналитические материалы подразделены по степени охвата объекта исследования на *глобальные*[8] и *тематические*. В основу тематических обзоров положены различные критерии.

---

[1] Карта российского рынка информационной безопасности 2023 года // Электронный ресурс. URL: https://www.tadviser.ru/index.php/Статья:Карта_российского_рынка_. информационной_безопасности_2023 <дата обращения: 26.04.2023>.

[2] https://www.kaspersky.ru/blog/category/threats/ <дата обращения: 26.04.2023>.

[3] https://rt-solar.ru/analytics/reports/ <дата обращения: 26.04.2023>.

[4] https://www.ptsecurity.com/ru-ru/research/analytics/ <дата обращения: 26.04.2023>.

[5] https://www.group-ib.com/resources/research-hub/ <дата обращения: 26.04.2023>.

[6] https://www.facct.ru/resources/research-hub/ <дата обращения: 26.04.2023>.

[7] См., например: https://www.cyderes.com/blog/category/resources/ <дата обращения: 20.05.2023>.

[8] См.: Актуальные киберугрозы: итоги 2022 года / Positive Technology, 29 марта 2023 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ <дата обращения: 26.04.2023>; Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023 / Ежегодный флагманский отчёт Group-IB // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/hi-tech-crime-trends-2022/ <дата обращения: 26.04.2023>; 2022 cybersecurity conversations report // Электронный ресурс. URL: https://www.cyderes.com/wp-content/uploads/2022/07/2022-Cybersecurity-Conversations-Report_V1.0.pdf <дата обращения: 26.04.2023>.

К ним отнесены государства[1], сектора и сегменты мировой[2] или региональной экономик[3], государственного управления[4], оказания целевых услуг населению, виртуальные социальные пространства; технологии, используемые в противоправных целях, и модели их применения в отношении определённых групп объектов; имущественный и репутационный вред, причинённый кибератаками[5]; уязвимости операционного и прикладного обеспечения; стратегии создания и обеспечения целостности контура безопасности; алгоритмы действий специалистов в области кибербезопасности на прогнозируемые и состоявшиеся инциденты; возможности установления лиц, виновных в кибератаках на объекты посягательства[6].

По временным параметрам аналитические отчёты подразделены на *годовые* и *периодические*. Во второй группе выделим ежеквартальные отчёты об актуальных киберугрозах в отношении определённых объектов. Выстроенные в хронологическом порядке они позволяют с большей точностью отслеживать происходящие изменения и анализировать оперативность реагирования заинтересованных субъектов в публичном и частном секторе на причины проявления активности и наступившие негативные последствия.

По направленности фокуса внимания выделим *диагностические*, *прогностические*[7] и *комплексные* отчёты. В первых внимание уделяют причинам возникновения и процессу проявления конкретных угроз, во второй группе – предприняты попытки выстроить модель уязвимостей, направления, средства и методы атак на защищаемые ценности, выстроить стратегии и определить тактику противодействия, в третьей – события прошлого, настоящего и будущего рассмотрены во временной и логической последовательности.

В обзорах представлены следующие параметры, характеризующие современное состояние девиантных проявлений в киберпространстве: 1) общее число зарегистрированных инцидентов; 2) соотношение успешных и отражённых атак; 3) выбор объекта атак (индивиды или организации,

---

[1] Cyber crime in India – statistics & facts // Электронный ресурс. URL: https://www.statista.com/topics/5054/cyber-crime-in-india/ <дата обращения: 20.05.2023>.

[2] Healthcare Cybersecurity Report 2021-2022 // Электронный ресурс. URL: https://www.cyderes.com/blog/cybersecurity-healthcare-report-2021-2022/ <дата обращения: 20.05.2023>.

[3] Как атаковали российский бизнес в 2022 году // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/incident-response-2022/ <дата обращения: 26.04.2023>.

[4] Отчет об исследовании серии кибератак на органы государственной власти РФ // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/2203/?ysclid=lhwbznchkq326878276 <дата обращения: 26.04.2023>.

[5] Техники и тактики киберпреступников // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/3416/ <дата обращения: 26.04.2023>.

[6] Возможности мобильной криминалистики: как извлекать и исследовать данные мобильных устройств и раскрывать преступления // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/mobile-forensics/ <дата обращения: 26.04.2023>.

[7] URL: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf <дата обращения: 26.04.2023>.

государственный сектор, IT-компании, отдельные сектора экономики); 4) используемые технологии и тактика действий злоумышленников (фишинг, бреши в операционных системах, уязвимости в компонентах программ, средства аутентификации клиента); 5) предмет интереса злоумышленников (персональные данные, данные платёжных карт, вэб-сайты для коммуникации с клиентами, электронные деньги, нарушение логистики товаров и информации, устойчивость систем защиты, оперативность реагирования на проникновение и др.). По оценкам экспертов Positive Technology в 2022 году чаще всего конфиденциальная информация была похищена в медучреждениях (в 82% инцидентов), в научных и образовательных организациях (в 67%), в ритейл-сегменте (в 65%)[1] для последующего использования с учётом достижений социальной инженерии и оказания влияния на объект воздействия.

Резонно возникает вопрос об обоснованности представленных результатов. В пользу говорят использованные методы, которые авторы не скрывают. К ним отнесены обобщение сведений о расследованных инцидентах, сопоставление результатов с данными конкурентов, опросы лиц, ответственных за кибербезопасность в различных организациях. К факторам, требующим критической оценки, отнесём охват вниманием любых инцидентов без использования норм уголовного законодательства, коммерциализацию оказываемых услуг, решение задач роста их востребованности на фоне представленной картины досягаемости и уязвимости от атак. В целях противодействия в получении информации противной стороной отдельные субъекты предоставляют сведения только персонифицированным потребителям, действия в сети и аутентичность которых могут быть перепроверены.

Изложенная в обзорах информация даёт возможность при её всесторонней обработке и многократной проверке получить достаточно полное представление о ландшафте современных угроз, оценить степень их общественной опасности, скорректировать нормативные модели деяний, преследуемых государством в различных правовых режимах, актуализировать методики расследования преступлений, разработать новые тактические приёмы. Интерес вызывают методика и приёмы изложения представляемых сведений. Одновременно аналитические отчёты позволяют задуматься о пересмотре устоявшейся системы абсолютных и относительных криминологических показателей преступности с учётом социальных процессов, присущих исключительно киберпреступлениям.

Литература

1. Актуальные киберугрозы: итоги 2022 года / Positive Technology, 29 марта 2023 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ <дата обращения: 26.04.2023>.
2. Возможности мобильной криминалистики: как извлекать и исследовать данные мобильных устройств и раскрывать преступления // Электронный

[1] Актуальные киберугрозы: итоги 2022 года.

ресурс. URL: https://www.facct.ru/resources/research-hub/mobile-forensics/ <дата обращения: 26.04.2023>.
3. Герке, М. Понимание киберпреступности: Явление, задачи и законодательный ответ // Электронный ресурс. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf <дата обращения: 26.04.2023>.
4. Как атаковали российский бизнес в 2022 году // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/incident-response-2022/ <дата обращения: 26.04.2023>.
5. Карта российского рынка информационной безопасности 2023 года // Электронный ресурс. URL: https://www.tadviser.ru/index.php/Статья: Карта_российского_рынка_информационной_безопасности_2023 <дата обращения: 26.04.2023>.
6. Отчёт об исследовании серии кибератак на органы государственной власти Российской Федерации // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/2203/?ysclid=lhwbznchkq326878276 <дата обращения: 26.04.2023>.
7. Техники и тактики киберпреступников // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/3416/ <дата обращения: 26.04.2023>.
8. Шваб, К. Четвертая промышленная революция. М.: «Эксмо», 2016.
9. Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023 // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/hi-tech-crime-trends-2022/ <дата обращения: 26.04.2023>.
10. Cyber crime in India – statistics & facts // Электронный ресурс. URL: https://www.statista.com/topics/5054/cyber-crime-in-india/ <дата обращения: 20.05.2023>.
11. Healthcare Cybersecurity Report 2021-2022 // Электронный ресурс. URL: https://www.cyderes.com/blog/cybersecurity-healthcare-report-2021-2022/ <дата обращения: 20.05.2023>.

А.А. Вихляев

О некоторых мерах по мониторингу информационно-телекоммуникационных сетей при реализации комплексных мероприятий, направленных на выявление и раскрытие преступлений, связанных с распространением религиозных материалов экстремистской направленности

Аннотация. В рамках исследования обозначенной проблематики, автором проведен анализ современной системы противодействия религиозному экстремизму в информационно-телекоммуникационных сетях. На основе полученных данных обозначены наиболее актуальные меры, позволяющие обеспечить действенный мониторинг религиозно-экстремистского контента в сети «Интернет» через призму текущей криминологической и общественно-политической ситуации. Также в статье дана фактическая оценка реализации

современных мер профилактики в области противодействия экстремизму на религиозной почве.

Ключевые слова: религиозный экстремизм, религиозное объединение, профилактика, мониторинг, информационно-телекоммуникационная сеть «Интернет».

Действующая Стратегия противодействия экстремизму[1] определяет экстремистскую деятельность как одну из наиболее сложных проблем современного общества. По данным официальной статистики[2], в 2022 году на территории Российской Федерации было зарегистрировано более 1,5 тыс. преступлений экстремистской направленности, что на 50% больше показателей предыдущего года.

Под экстремизмом понимаются общественно-опасные деяния, которые могут быть совершены по мотивам политической, идеологической, расовой, национальной и (или) религиозной ненависти, или вражды, а также по мотивам ненависти или вражды в отношении какой-либо социальной группы. Религиозный экстремизм – одна из наиболее опасных его форм. Это обусловлено и тем, что религиозные мотивы активно применяются в иных формах противоправного поведения – например, при пропаганде националистической идеологии или при распространении ксенофобии или разжигания межэтнических конфликтов.

В условиях развития современных цифровых технологий информационно-телекоммуникационные сети являются основным способом коммуникации между религиозными объединениями и их последователями.

Нередко религиозные объединения получают финансирование от иностранных религиозных организаций, а также иностранных государств, отдельных граждан и лиц, получающих иностранную поддержку или находящихся под иностранным влиянием, что дает возможность использовать идеологию, распространяемую посредством таких религиозных объединений для ведения информационной войны, вербовки посредством сети «Интернет» лиц для осуществления актов экстремизма и терроризма или дестабилизации общественно-политической ситуации в Российской Федерации.

Так, 22 октября 2022 года в ходе проведения специальной военной операции на территории Запорожья[3] были выявлены центры вербовки лиц в целях осуществления экстремистской деятельности на территории Российской Федерации, действовавшие на базе штаб-квартир запрещенной в России религиозно-экстремистской организации «Свидетели Иеговы», спонсирование которых осуществлялось со стороны недружественных стран. Информация о

[1]Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28.11.2014 № Пр-2753).

[2] Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс] URL: https://epp.genproc.gov.ru/web/gprf (дата обращения: 10.04.2023).

[3] Официальный сайт канала «Россия 1». Платформа «Смотрим». [Электронный ресурс] URL: https://smotrim.ru/video/2502564 (дата обращения: 10.04.2023).

деятельности секты также распространялась посредством сети «Интернет», что дополнительно повышало его доступность для потенциальных последователей.

Если для религиозных объединений, осуществляющих свою деятельность легально, современные технологии представляют важный элемент информационного обмена со своими последователями и размещения информации, имеющей социально-значимый характер, то для религиозных организаций и групп, прямо осуществляющих религиозно-экстремистскую деятельность – действенный способ вовлечения в противоправную деятельность новых адептов, распространения информации деструктивного содержания или совершения преступлений экстремистской направленности (например, общественно-опасных деяний, предусмотренных ст.ст.280, 282 или 148 УК РФ).

Кроме того, посредством использования некоторых браузеров (например, Google Chrome) пользователи информационно-телекоммуникационных сетей могут свободно получать информацию о функционировании и деятельности ряда запрещенных в Российской Федерации религиозных объединений и сект. Дополнительным элементом обхода сложившейся системы противодействия распространения социально-деструктивного контента в сети «Интернет», стали возможности VPN-соединений или иных средств анонимизации.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ на территории России введен реестр социальных сетей, ведение которого поручено Роскомнадзору, а также переданы полномочия по самостоятельной блокировке подобных информационных ресурсов провайдерам хостингов, на которых размещается деструктивный контент. В целях нивелирования возможностей негативного влияния религиозных объединений, в информационно-телекоммуникационных сетях Роскомнадзор вправе осуществить блокировку запрещенного контента, в т.ч. и принять меры по привлечению владельцев аудиовизуального сервиса, разместивших информацию, содержащую публичные призывы к терроризму, или оправдывающую экстремистскую деятельность, по ст.13.37 КоАП РФ.

Следует отметить, что при распространении аудио- и видеоматериалов, в т.ч. посредством информационно-телекоммуникационных сетей, российские религиозные объединения и миссии, осуществляющие непосредственные коммуникации с отечественными религиозными организациями и группами, обязаны обеспечить маркировку в информационно-телекоммуникационных сетях распространяемого ими контента и аудио-, видеопродукции в соответствии с полным наименованием представляемой религиозной организации.

Кроме того, в случае получения денежных пожертвований от международных религиозных, иностранных организаций или иностранных частных лиц, религиозные объединения обязаны отчитываться перед федеральными органами государственной власти об указанных средствах, в том числе и размещая соответствую информацию на своих официальных ресурсах в сети «Интернет».

В случае сокрытия информации в части, касающейся получения имущества или денежных пожертвований от международных организаций, иностранных религиозных организаций или частных лиц, в т.ч. и лиц, имеющих статус

иностранного агента на территории Российской Федерации, а равно не размещение маркировки соответствующей иностранной организации или религиозной миссии в информационно-телекоммуникационных сетях, религиозные объединения несут юридическую ответственность в соответствии с ч.3 ст.5.26 КоАП РФ.

При реализации мер по обеспечению национальной безопасности в 2016 году был принят пакет законов, направленных на совершенствование системы противодействия распространению экстремизма и терроризма в Российской Федерации (Федеральные законы №№374-ФЗ и 375-ФЗ от 06.07.2016), внесших изменения в нормативные правовые акты, предусматривающие оборот информации на территории России и ответственность за нарушение порядка распространения информации.

Благодаря указанным законодательным инициативам была проработана система защиты информационно-телекоммуникационных ресурсов от распространения информации социально-деструктивного, экстремистского и террористического характера, а также обозначены меры по мониторингу и противодействию его свободному распространению на территории Российской Федерации.

На основании Постановления Правительства Российской Федерации от 12.04.2018 №445 были установлены порядок и сроки хранения пользовательских сообщений, а также требования к оборудованию, которое операторы связи должны использовать для хранения сообщений. Указанное постановление было принято во исполнение требований подп. 2 п. 1 ст. 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи». Постановление предписывает операторам связи, осуществляющим передачу как текстовой, так и голосовой информации, обеспечить накопление и хранение информации на принадлежащим им технических средствах, расположенных на территории Российской Федерации, в течение 6 месяцев с даты окончания ее приема, передачи, доставки и (или) обработки.

Кроме того, Постановлением Правительства РФ от 26.02.2022 № 256 были утверждены Правила хранения организатором распространения информации в информационно-телекоммуникационной сети «Интернет» текстовых сообщений пользователей информационно-телекоммуникационной сети «Интернет», голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет», которыми установлены схожие требования к хранению пользовательской информации организаторами распространения информации – в течение 6 месяцев.

Материалы о противоправной деятельности, полученные от организаторов хранения информации в рамках изучения обстоятельств противоправной деятельности религиозных объединений в сети «Интернет» при проведении комплексных оперативно-розыскных мероприятий, могут быть использованы в последствии в качестве доказательств по уголовным делам.

За несоблюдение требований к хранению и распространению информации предусмотрена ответственность в соответствии со ст.13.31 КоАП РФ, а в

случаях, когда нарушаются правила распространения информации в средствах массовой информации со стороны лиц, имеющих статус иностранного агента, - по части 2.1 статьи 13.15 КоАП РФ.

Проведенное исследование показало, что действующие правовые механизмы в текущих общественно-политических условиях позволяют обеспечить многофакторный контроль за деятельностью религиозных объединений на территории Российской Федерации и осуществлять всесторонние мониторинг и профилактику размещения информации, распространяемой религиозными объединениями, или отдельными лицами, занимающимися миссионерской деятельностью от лица иностранных религиозных организаций, в информационно-телекоммуникационных сетях, в т.ч. в сети «Интернет».

Рассмотренные в настоящей статье меры не являются исчерпывающими, однако, наравне с действующей системой мониторинга и противодействия терроризму и экстремизму в Российской Федерации, способны обеспечить надлежащий уровень информационной безопасности, своевременную блокировку экстремистского, террористического и социально-деструктивного контента и снизить вероятность совершения преступлений религиозно-экстремистского характера посредством использования информационно-телекоммуникационных сетей.

М.Ф. Гарафутдинова

«Цифровой сыск» в расследовании киберпреступлений

Аннотация. Активное развитие информационных технологий и цифровая трансформация в обществе характеризуется появлением новых возможностей в деятельности оперативных подразделений. В статье рассматриваются возможности биометрические технологии, электронные банки данных, интернет-технологии при проведении отдельных оперативно-розыскных мероприятий.

Ключевые слова: киберпреступление, оперативно-розыскное мероприятие, интернет-технологии, цифровой сыск.

Как известно, киберпреступлением (КП) считается деятельность, направленная на незаконное применение компьютера, глобальных сетей либо сетевых устройств. Учитывая опасность преступлений в сфере компьютерной информации, законодатель включил их в главу 28 «Преступления в сфере компьютерной информации» к разделу IX УК «Преступления против общественной безопасности и общественного порядка». Значение термина «компьютерная информация» сформулировано в примечании к ст. 272 УК РФ.

Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их

хранения, обработки и передачи.[1] Компьютерная информация относительно просто пересылается, преобразуется и дублируется. С учетом этих особенностей и изъятие информации как вещественного доказательств отличается от изъятия вещей. К источнику компьютерной информации могут иметь доступ одновременно практически неограниченное количество пользователей.

Среди совершаемых киберпреступлений можно выделить следующие основные типы:

- Интернет-мошенничество;
- Взлом e-mail;
- Незаконные операции с применением личных данных;
- Незаконные операции с применением корпоративных данных;
- Воровство сведений банковских карт, финансовой информации;
- Воровство, продажа корпоративной информации;
- Кибершантаж;
- Атаки вредоносных программ-вымогателей;
- Криптоджекинг (майнинг на посторонних ресурсах без разрешения владельца);
- Кибершпионаж (незаконное получение доступа касательно закрытой информации государственных/коммерческих структур);
- Кибератаки (атаки вирусов-вредителей).

Практические все совершаемые КП можно разделить на незаконную деятельность, чьей основной целью выступают непосредственно ПК пользователей, а также преступления в области инфотехнологий, где ПК применяются с целью совершения иных неправомерных действий.

Не секрет, что эффективность выявления, предупреждения, пресечения и раскрытия любых преступлений находится в прямой зависимости от уровня владения оперативной и иной информацией.

На сегодняшний день, важнейшим источником такой информации, являются сведения, находящиеся в свободном доступе (независимая от действий сотрудников правоохранительных органов), которые могут стать содержанием доказательств, при соблюдении порядка (правил) ее закрепления (фиксации), хранения и трансформации. Многое зависит от осведомленности следователя или иного лица, уполномоченного на осуществление указанных действий, о технических характеристиках носителя электронной информации, способах ее формирования, а также вариантах сокрытия и осуществления иных форм противодействия расследованию. В связи с этим, необходимо обучать сотрудников органов расследования преступлений, методам и приемам работы с открытыми данными при раскрытии и расследовании преступлений с применением компьютерных технологий.

Оперативными сотрудниками при проведении ОРМ активно используется

[1] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет".

публичное пространство Интернета, которое выступает, во-первых, как ресурс, позволяющий получить (добыть) необходимую информацию о различных объектах и, во-вторых, как средство (инструмент) отождествления личности.

Для выявления преступлений, ряд оперативно-розыскных мероприятий и следственных действий приходится выполнять с учётом особенностей получения значимой для следствия информации из виртуального пространства по мере выявления и фиксации закодированных информационных следов. Согласно ст. 6 ФЗ об ОРД к ключевым из них относятся: опрос, наблюдение, исследование предметов и документов, прослушивание телефонных переговоров, снятие информации в технических каналов связи, получение компьютерной информации. С точки зрения своей значимости для последующей трансформации в электронные доказательства цифровая информация, полученная оперативным путем, может быть условно разделена на две группы.[1]

Первичная электронная оперативная информация. Такая информация может привлечь внимание сотрудника оперативного подразделения при изучении интернет-пространства (сайтов, порталов, страниц пользователей социальных сетей); сообщений электронной почты; контактов мобильной телефонной связи и т. д. Для сотрудников органа, осуществляющего оперативно-розыскную деятельность повседневным стал мониторинг социальных групп в сети Интернет, интерактивных многопользовательских веб-сайтов, в рамках которых пользователи имеют возможность создавать связи с другими пользователями (социальные связи). Интернет позволяет войти с кем-то в переписку, и в результате обнаружить информацию, представляющую оперативный интерес, эта информация может к нему поступать и по электронным каналам от анонимных источников. Она подлежит документированию и тщательной проверке, которые регламентированы действующим законодательством об оперативно-розыскной деятельности.

Для поиска оперативной информации осуществляется организованное наблюдение за сетевыми ресурсами в Интернете: мониторинг аукционов; мониторинг администраторов сетевых городских барахолок; мониторинг даркнет-площадок (торговая площадка по купле-продаже запрещенных к обороту и ограниченных в обороте в Российской Федерации предметов, а также краденого имущества или реализации имущества, приобретенного за счет похищенных денежных средств для придания легального вида денежным средствам, добытым преступным путем). Указанные мероприятия позволяют оперативным сотрудникам выявлять и задерживать лиц, причастных к подготовке или совершению преступлений.

Технологически, на первоначальном этапе осуществления оперативно-розыскной деятельности по выявлению преступлений с использованием информационно-телекоммуникационных систем, осуществляются следующие операции: устанавливаются регистраторы доменных имен (юридическое лицо, аккредитованное координатором для оказания услуг регистрации доменных

[1] Электронные доказательства в уголовном судопроизводстве : учеб, пособие для вузов / отв. ред. С. В. Зуев., 2020. С. 163-164.

имен), устанавливается провайдер хостинга (т.е. лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет), а также интернет-провайдер, который в конечном счете и может сообщить IP-адрес конкретного пользователя, точнее, точки доступа в сеть Интернет. В результате появляется возможность установить фактическое местонахождение компьютера, мобильного устройства, точки доступа в Интернет, с неограниченным числом пользователей. Но при этом, нужно отметить, что достоверное установление лица, разместившего информацию в сети Интернет затрудняется тем, что при регистрации доменного имени, сайта или регистрационного аккаунта на ресурсе в качестве пользователя проверка подлинности представленных данных не проводится.

Вторая группа цифровой информации – это информация, закрепленная на цифровом носителе, как результат проведения ОРМ. При проведении таких ОРМ участие IT- специалиста направлено на поиск цифровых источников и в настоящее время является обязательным. Таковым может быть сотрудник экспертных подразделений, имеющий допуск к проведению компьютерно-технических исследований или соответствующее образование. Также могут привлекаться системные администраторы, консультанты специализированных магазинов, преподаватели вузов, технические аналитики и т. д. — т. е. любое лицо, обладающее познаниями в области обслуживания электронно-технических устройств.

Перед проведением необходимых действий следует убедиться в соответствии квалификации специалиста поставленным задачам. Например, исследование сетей и сетевого сервера существенно отличается от проверки комплектности электронно-вычислительной машины, поэтому требует разных специалистов. Разумеется, требуется детальный инструктаж специалиста относительно его функций, прав и обязанностей и общего порядка проведения действия. Важно отметить, что результаты оперативно-розыскной деятельности до их перепроверки следственным путем имеют исключительно поисково-ориентирующее значение.

Основными познавательными приемами обращения с цифровой информацией после ее обнаружения и фиксации в ходе производства следственных и иных процессуальных действий являются изъятие ее носителей и (или) копирование самой информации. В случае значительной угрозы интересам общества или государства при согласии на это специалиста следует изымать носитель цифровой информации, в остальных случаях сотрудники правоохранительных органов, как правило, при наличии соответствующего специалиста и технической возможности производят копирование. Копирование цифровой информации и изъятие ее носителя могут применяться как в принудительном, так и добровольном порядке в отношении субъекта, распоряжающегося носителем.[1]

[1] Зуев С. В., Овсянников Д. В. Копирование электронной информации в теории и практике уголовного процесса // Вестник СамГУ. 2014. № 11/2. С. 171.

В настоящее время, можно утверждать о существовании такого термина, как «цифровой сыск» (OSINT), который является эффективным аналогом существующих оперативно-розыскных мероприятий или отлично их дополняют. Перечислим возможности «цифрового сыска»:

- идентификация пользователей анонимных номеров телефонов, адресов электронной почты, владельцев защищенных мессенджеров, криптовалютных кошельков;
- отслеживание перемещения пользователей электронных устройств по всему миру с применением рекламных модулей (технологии ADINT);
- деанонимизаци посетителя любого интернет-ресурса по идентификаторам, оставленным его электронным устройством.[1]

Специалисты в области IT указывают, что идентификаторы электронных устройств пользователей, которые остаются при посещении ими любого интернет-ресурса (модель устройства, версия операционной системы и браузера, языковые и экранные параметры, ip-адрес и иные параметры соединения, авторизованные аккаунты электронной почты и социальных сетей,рекламные идентификаторы и иные), позволяют установить и выделить уникальное устройство из миллионов подобных.

Очевидно, что условием получения оперативной цифровой информации с использованием публичного пространства сети Интернет является наличие современной компьютерной техники с доступом в Интернет. Также, невозможно осуществлять поисковые и идентификационные действия без специфического программного обеспечения и сервисов. Однако, сотрудники оперативных подразделений ОВД зачастую не имеют ни служебного компьютера с доступом в Интернет, ни возможности использования вышеуказанных программных средств и сервисов. Отметим, что позволяющие идентифицировать граждан по их изображениям в социальных сетях сервисы, наиболее часто используемые оперативными сотрудниками в служебной деятельности, как правило является общедоступной условно бесплатной программой. Однако, использование таких демоверсий имеет существенные ограничения по числу возможных поисков лиц по их изображениям. Кроме того, не гарантирована постоянная работа подобных публичных сервисов, в любой момент они могут оказаться недоступными.

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 09.03.2022).
2. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 "О некоторых вопросах судебной практики по уголовным делам о

[1] И.С. Бедеров Проблемы и тенденции в расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Противодействие киберпреступлениям и преступлениям в сфере вы соких технологий: материалы Всероссийской научно-практической конференции (Москва, 10 декабря 2020 года) / Под общ. ред. Д.Н. Кожухарика. М.: Московская академия Следственного комитета Российской Федерации, 2021.

преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». –
3. Электронные доказательства в уголовном судопроизводстве : учеб, пособие для вузов / отв. ред. С. В. Зуев., 2020. С. 163-164.
4. Зуев С. В., Овсянников Д. В. Копирование электронной информации в теории и практике уголовного процесса // Вестник СамГУ. 2014. № 11/2. С. 171.
5. Бедеров И.С.Проблемы и тенденции в расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий**.** Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: материалы Всероссийской научно-практической конференции (Москва, 10 декабря 2020 года) / Под общ. ред. Д.Н. Кожухарика. М.: Московская академия Следственного комитета Российской Федерации, 2021

Д.К. Гончаров

Особенности тактики осмотра места происшествия при расследовании незаконных организации и проведения азартных игр с использованием информационно-телекоммуникационной сети «Интернет»

Аннотация. В данной статье рассмотрены проблемные вопросы расследования незаконных организации и проведения азартных игр, связанные со сложностью получения следов преступлений. Автором осуществлена попытка установления взаимосвязи между количеством лиц, осужденных за незаконные организацию и проведение азартных игр, и качеством проведенных оперативно-розыскных мероприятий и следственных действий. В качестве одного из основных следственных действий при расследовании незаконных организации и проведения азартных игр выделен осмотр места происшествия. Рассмотрена тактика проведения осмотра места происшествия. Автором предложены меры по совершенствованию тактических комбинаций, применяемых при проведении осмотра места происшествия при расследовании незаконных организации и проведения азартных игр с использованием информационно-телекоммуникационной сети «Интернет».

Ключевые слова: азартные игры, организатор, осмотр, электронно-цифровые следы, информационно-телекоммуникационные технологии, расследование, тактика.

В настоящее время наблюдается динамичный рост незаконных игорных заведений в различных регионах Российской Федерации. Как известно, азартные игры приносят колоссальные доходы их организаторам и, зачастую, приводят к разорению лиц, вовлеченных в азарт и жаждущих выиграть «легкие деньги».

Незаконные игорные заведения, помимо прочего, оказывают негативное влияние на здоровые экономические отношения государства.

Принятие Федерального закона от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» обусловило ограничения организации и проведения азартных игр на территории Российской Федерации, выразившиеся в установлении специально отведенных разрешенных игорных зон, расположенных в Республике Крым, Алтайском крае, Краснодарском крае, Приморском крае и Калининградской области[1]. За пределами таких зон на территории указанных субъектов Российской Федерации, а также на территории остальных субъектов Российской Федерации деятельность игорных заведений запрещена.

Статьей 171.2 УК РФ предусмотрена уголовная ответственность за незаконные организацию и (или) проведение азартных игр, а равно систематическое предоставление помещений для незаконных организации и (или) проведения азартных игр с использованием игрового оборудования с максимальным сроком наказания в виде лишения свободы до шести лет[2].

Однако, существующие достаточно жесткие санкции не пугают организаторов незаконных азартных игр, которые, используя меры конспирации, продолжают открывать новые игорные заведения. Сотрудниками правоохранительных органов на постоянной основе проводятся мероприятия, направленные на пресечение, выявление, раскрытие и расследование фактов незаконных организации и проведения азартных игр.

В соответствии с официальными данными Судебного Департамента при Верховном Суде Российской Федерации, за незаконные организацию и проведение азартных игр на территории Российской Федерации по ст. 171.2 УК РФ осуждено в 2017 году 1378 лиц, в 2018 году – 1093, в 2019 году – 1067, в 2020 году – 762, в 2021 году – 946, в 2022 году – 1164[3].

Проведя сравнительный анализ обвинительных заключений, материалов следственно-судебной практики и приговоров по ст. 171.2 УК РФ, вступивших в законную силу, в различных регионах Российской Федерации, можем заключить, что не все лица, причастные к совершению преступлений в сфере незаконной игорной деятельности, привлекаются к уголовной ответственности.

---

[1] Федеральный закон от 29.12.2006 № 244-ФЗ (в редакции от 02.07.2021) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации». [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64924/ (дата обращения 27.04.2023).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 09.03.2022). [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». – URL: http://www.consultant.ru/ document/ cons_doc_LAW_10699/ b20820739fab5a2c2645f2c2dba2d73e9025f6e4/ (дата обращения 28.04.2023).

[3] Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. [Электронный ресурс] // Судебная статистика РФ: URL: http://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения 09.05.2022).

По нашему мнению, основными причинами тому могут служить высокая латентность таких преступлений, используемые злоумышленниками методы конспирации, отсутствие необходимого опыта сотрудников правоохранительных органов, качество получения и фиксации доказательств совершенных противоправных деяний в данной сфере.

Как показывает практика расследования незаконных организации и проведения азартных игр, основой доказательной базы являются вовремя полученные и зафиксированные надлежащим образом электронно-цифровые следы совершенных преступлений. Качество и полнота сбора таких следов зависит от грамотно подобранной криминалистической тактики.

В криминалистической науке существует рад трудов В.М. Алиева, Р.С. Белкина, В.А. Волынского, Б.В. Волженкина, А.Э. Жалинского, Э.А. Ивановой, Н.В. Машинской, И.Н. Мосечкина, А.А. Лихолетова, В.А. Никулиной, Г.А. Тосуняна, А.А. Шебуновой, которые были посвящены основам выявления и раскрытия преступлений в сфере игорной деятельности.

При этом, вопросы криминалистической тактики при расследовании незаконных организации и проведения азартных игр изучены недостаточно.

В связи со стремительным развитием информационно-телекоммуникационных технологий, преступники переводят свой нелегальный бизнес, связанный с азартными играми, в мировую сеть «Интернет», что значительно усложняет процесс фиксации следов преступной деятельности и установления лиц, причастных к совершению преступлений. В последнее время в науке все чаще стали выделять специфические следы, возникающие в искусственно созданной на основе компьютерных систем среде электронно-цифрового отображения[1]. Получение таких следов, зачастую, имеет решающее значение для доказывания вины организаторов незаконных азартных игр и лиц, которые их проводят.

Наряду с проведением оперативно-розыскных мероприятий, направленных на установление лиц, причастных к незаконным организации и проведению азартных игр, фиксации процесса проведения азартных игр, а также доказательств причастности установленных лиц к указанной противоправной деятельности, немаловажное значение при расследовании незаконных организации и проведения азартных игр имеет проведение следственных действий, основным из которых является проведение осмотра места происшествия.

Как известно, осмотр места происшествия, как самостоятельное следственное действие, занимает определенный временной промежуток, и разделяется на этапы и стадии. Классически осмотр разделяется на 3 этапа: подготовительный,

[1] Мещеряков В.А. Электронно-цифровое отображение как методическая основа цифровой криминалистики / В.А. Мещеряков, О.Ю. Цурлуй // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации : Сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / Под редакцией Ю.В. Гаврилина, Ю.В. Шпагиной. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2021. – С. 232-238.

рабочий и заключительный[1]. По мнению Н.П. Яблокова, необходимо выделять следующие этапы (стадии) осмотра места происшествия: «подготовительную, ориентирующую (обзорную), детального исследования, заключительную»[2]. Е.П. Ищенко, А.А. Топоркова считают, что осмотр места происшествия также делится на две стадии: начальную (общий осмотр) и детальный осмотр[3].

Применительно к проведению осмотра места происшествия в местах незаконного проведения азартных игр как предназначенных для проведения азартных игр, так и вне этих мест, на стадии подготовительного этапа, до выезда на место происшествия необходимо определить круг участников, их задачи, примерное местонахождение во время проведения следственного действия, целесообразность привлечения подразделений силовой поддержки и их количество.

Перед проведением осмотра помещения, в котором осуществляется проведение азартных игр, необходимо рассчитать количество участвующих лиц, их роли и обязанности непосредственно во время проведения следственного действия. Обязательным является привлечение специалиста в области компьютерных технологий[4]. Как показывает практика, кроме сотрудников Следственного комитета, органов внутренних дел, специалистов в области компьютерных технологий, понятых[5], эффективным является привлечение сотрудников специальных подразделений силовой поддержки, которые, кроме эффекта внезапности, могут в считанные секунды обездвижить преступников и иных лиц, находящихся в игорном заведении. Данная мера необходима для того, чтобы исключить возможность аварийного отключения питания игрового оборудования от электрической сети, с целью фиксации электронно-цифровых следов. Преимущественное большинство таких следов, которые подтверждают выход в сеть «Интернет» и работу игровых приложений с удаленными серверами, может быть зафиксировано только во время проведения азартных игр. Поэтому осмотр игорного оборудования перед изъятием рекомендуется проводить непосредственно в месте проведения азартных игр, когда это оборудование подключено к сети и используется во время игры.

Для этого, на подготовительном этапе, перед проведением осмотра, во время планирования тактической комбинации, направленной на получение доказательств по расследуемому уголовному делу, следователю необходимо ознакомиться с техническим паспортом помещения, в котором проводятся

---

[1] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. М.: Норма, 2000. С. 571.

[2] Яблоков Н.П. Криминалистика: классический университетский учебник. М.: Юристь, 2005. С. 437.

[3] Ищенко Е.П., Топорков А.А. Криминалистика: учебник. М.: ИНФРА-М, 2010. С. 354–355.

[4] Гусев А.В. Концепция формирования специального криминалистического познания и механизма его реализации в уголовном судопроизводстве вне судебно-экспертной деятельности: автореф. дис. ... д-ра юрид. наук. Краснодар, 2015. – 46 с.

[5] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/a3c8328be5f6240b55ac1c22ce81975ece4ff2c1/(дата обращения 26.04.2023).

азартные игры, подготовить схему, на которой указать расположение игорного оборудования, точки подключения к сети электропитания, примерное местоположение сотрудников игрового зала, а также игроков.

Также, на подготовительном этапе по приезду на место происшествия, целесообразно отправить в игровой зал нескольких сотрудников полиции в гражданской форме одежды, которые под видом игроков смогут контролировать местоположение сотрудников игорного заведения и при поступлении команды путем смс-информирования, смогут в считанные секунды задержать оператора, администратора, охранника и иных членов преступной группы, не давая им возможности помешать проведению следственных действий и смогут таким образом обеспечить беспрепятственный вход в помещение игрового зала.

Рабочий этап осмотра места происшествия в обязательном порядке необходимо проводить с участием специалиста в сфере компьютерных технологий, с целью установления и фиксации следовой цифровой информации, установленных компьютерных программ и игровых приложений, фиксации сведений о выходе в сеть «Интернет» и подключении к игровым серверам, а также получения статистических данных, позволяющих впоследствии путем проведения судебной экономической экспертизы определить размер извлеченного дохода.

На заключительном этапе необходимо обеспечить составление протокола с приложениями, проконтролировать их подписание всеми участниками осмотра, указав имеющиеся у них замечания, упаковать изымаемые предметы, обеспечив невозможность их вскрытия посторонними лицами, зачитать протокол осмотра присутствующим, после чего обеспечить доставку изъятых предметов в следственное подразделение, для их последующего признания вещественными доказательствами.

Подводя итоги, можем сделать вывод о том, что при расследовании незаконных организации и проведения азартных игр с использованием информационно-телекоммуникационной сети «Интернет» существует ряд трудностей получения электронно-цифровых следов, необходимых для доказывания причастности организаторов и иных лиц, незаконно проводящих азартные игры, к совершению данного рода преступлений. При слаженной работе правоохранительных органов и правильно подобранной криминалистической тактике, используемой при проведении оперативно-розыскных мероприятий и следственных действий, в преимущественном большинстве случаев удается достичь конечного результата расследования – установления истины по делу. Ключевым следственным действием, позволяющим получить и зафиксировать необходимые для доказывания вины участников преступной деятельности следы, является осмотр места происшествия, который необходимо проводить в местах проведения азартных игр во время непосредственного функционирования игорного оборудования, с привлечением специалиста в области компьютерных технологий, при поддержке оперативных сотрудников. При этом, все действия следователя и иных участников следственных действий должны быть тщательно спланированы и заранее продуманы.

Литература

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. М.: Норма, 2000. С. 571.
2. Гусев А.В. Концепция формирования специального криминалистического познания и механизма его реализации в уголовном судопроизводстве вне судебно-экспертной деятельности: автореф. дис. ... д-ра юрид. наук. Краснодар, 2015. – 46 с.
3. Ищенко Е.П., Топорков А.А. Криминалистика: учебник. М.: ИНФРА-М, 2010. С. 354–355.
4. Мещеряков В.А. Электронно-цифровое отображение как методическая основа цифровой криминалистики / В.А. Мещеряков, О.Ю. Цурлуй // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации : Сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / Под редакцией Ю.В. Гаврилина, Ю.В. Шпагиной. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2021. – С. 232-238.
5. Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. [Электронный ресурс] // Судебная статистика РФ: URL: http://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения 09.05.2022).
6. Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/a3c8328be5f6240b55ac1c22ce81975ece4ff2c1/(дата обращения 26.04.2023).
7. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 09.03.2022). [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». – URL: http://www.consultant.ru/ document/ cons_doc_LAW_10699/ b20820739fab5a2c2645f2c2dba2d73e9025f6e4/ (дата обращения 28.04.2023).
8. Федеральный закон от 29.12.2006 № 244-ФЗ (в редакции от 02.07.2021) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации». [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64924/ (дата обращения 27.04.2023).
9. Яблоков Н.П. Криминалистика: классический университетский учебник. М.: Юристь, 2005. С. 437.

В.Ю. Голубовский

Проблемы противодействия киберпреступлениям против собственности

Аннотация. Развитие общества в настоящий период связано с повсеместной цифровизацией всех сфер жизнедеятельности. Информационные и телекоммуникационные сети стали незаменимыми при решении многих вопросов. Интерес ученых к проблемам преступлений против собственности всегда является высоким, что связано и с распространенностью данной группы преступлений, и проблемами предупреждения киберпреступности.

Ключевые слова: киберпреступность, предупреждение, преступелние, сотрудничество, цифровизация

Развитие информационных технологий позволило по-новому взглянуть на предмет хищений: в науке уголовного права все более становится популярной позиция о вещно-правовой природе безналичных денег; на момент окончания преступлений, отличающийся от традиционного понимания момента окончания хищений, что связано с особенностями преступлений против собственности, где предметом выступают безналичные, в том числе электронные денежные средства; на проблемы квалификации. Не только названные составы преступлений могут быть совершены посредством использования информационно-телекоммуникационных технологий.

Всемирный Экономический Форум 2020 г., который проходил в Давосе, стал местом, где активно обсуждали рост значения кибербезопасности, которая, имеет огромное значение при совместных действиях государств по предупреждению киберпреступлений[1].

Стремительно рост числа киберпреступлений прослеживается с 2020 года, с распространением COVID-19. По данным замглавы Совбеза Дмитрия Медведева, за пять месяцев 2020 года количество преступлений с использованием интернета и мобильной связи составило более 180 тысяч. Это приблизительно на 85% больше, чем за аналогичный период прошлого года[2].

Больше половины зарегистрированных киберпреступлений (52,1 %) относится к категориям тяжких и особо тяжких (272 233; -5,6 %). В структуре киберпреступлений преобладают мошенничества (47,88 %; всего - 249 984), кражи (21,75 %; всего - 113 565) и преступления в сфере незаконного оборота наркотиков (11,92 %; всего - 62 209)[3].

За 2022 год в 7 субъектах Российской Федерации зафиксирован рост числа киберпреступлений. Наибольшие значения зафиксированы в Республике

[1]Почему мировое сообщество так боится киберпреступников России? URL:https://zen.yandex.ru/media/sharespro/pochemu-mirovoe-soobscestvo-tak-boitsia-kiberprestupnikov-rossii-5e36730069772e0fcc737d34(дата обращения: 10.05.2023).

[2] Мошенники атаковали россиян на удаленке. Число киберпреступлений выросло в десятки раз. URL:https://ura.news/news/1052439348?ysclid=lhhlrm5yi0488145805(08.05.2023).

[3] Состояние преступности в России за январь – декабрь 2022 года. Москва. URL: file:///C:/Users/User/Downloads/Sbornik_22_12-5.pdf(дата обращения: 10.05.2023).

Северная Осетия - Алания, Тверской области, Чукотском АО, Рязанской области, Республике Крым, Московской области, г. Севастополь. В 17 субъектах Российской Федерации зарегистрировано более половины всех киберпреступлений, совершенных на территории Российской Федерации. Следует также отметить значительный рост числа вымогательств, фактов неправомерного оборота средств платежей, публичных призывов к осуществлению террористической деятельности, публичных оправданий терроризма или пропаганды терроризма, изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних и неправомерного доступа к компьютерной информации[1].

С учетом актуальности проблем киберпреступности, помимо профилактики и разъяснительной работы среди граждан, важное значение имеет качественная коммуникация между всеми участниками процесса расследования таких преступлений. Главные причины этой ситуации, это доверчивость граждан и низкий уровень технической грамотности. Большинство злоумышленников представляются сотрудниками банков и под разными предлогами убеждают передать им информацию с банковских карт, CVC-коды и смс-пароли. Подключая программы удаленного доступа к онлайн банку, обманщики переводят средства на свои счета.

Кроме того, растет многообразие видов преступлений. С целью повышения цифровой грамотности в сфере информационной безопасности органы государственной власти разработали памятку для населения по безопасному поведению в Интернете.

Негативной тенденцией является рост числа кибератак на промышленные предприятия, например, Свердловской области. Если вести речь о Российской Федерации, то общий ущерб за 2022 год составил порядка 170 млрд. рублей. Региональный ущерб, это десятки, сотни миллионов рублей. При этом ситуация улучшается, и компании, которые занимаются предотвращением киберпреступлений, и различные органы власти идентифицируют большое количество фишинговых сайтов. Чаще всего киберпреступники атаковали предприятия финансового сектора и те, которые занимаются кадровыми вопросами[2].

Таким образом, как показывает практика, кибератак фиксируется больше, но и реагирование на них становится лучше, эффективнее.

Литература

1. Мошенники атаковали россиян на удаленке. Число киберпреступлений выросло в десятки раз. URL:https://ura.news/news/1052439348?ysclid=lhhlrm5yi0488145805.

[1] Там же.

[2] Ущерб свердловских предприятий от кибератак составил сотни миллионов. URL: https://ura.news/news/1052648216?ysclid=lhhloxcf3x474262008(дата обращения: 10.05.2023).

2. Почему мировое сообщество так боится киберпреступников России? URL:https://zen.yandex.ru/media/sharespro/pochemu-mirovoe-soobscestvo-tak-boitsia-kiberprestupnikov-rossii-5e36730069772e0fcc737d34(дата обращения: 10.05.2023).
3. Состояние преступности в России за январь – декабрь 2022 года. Москва. URL: file:///C:/Users/User/Downloads/Sbornik_22_12-5.pdf(дата обращения: 10.05.2023).
4. Ущерб свердловских предприятий от кибератак составил сотни миллионов. URL: https://ura.news/news/1052648216?ysclid=lhhloxcf3x474262008(дата обращения: 08.05.2023).

М.Е. Гущев

Перспективы использования искусственного интеллекта в расследовании преступлений

Аннотация. В статье рассматриваются перспективные возможности использования искусственного интеллекта в расследовании преступлений. Определяются основные направления потенциального применения данной компьютерной технологии. Особое внимание уделяется использованию искусственного интеллекта в расследовании киберпреступлений.

Ключевые слова: искусственный интеллект, расследование преступлений, машинное обучение, алгоритмы.

Искусственный интеллект (далее - ИИ) - это имитация человеческого интеллекта в машинах, которые запрограммированы думать и действовать как люди. Он включает в себя использование алгоритмов машинного обучения, обработки естественного языка (NLP) и других технологий, позволяющих машинам обучаться и адаптироваться к новым ситуациям. В последние годы ИИ приобрел огромную популярность, его применение варьируется от голосовых помощников до автономных транспортных средств.

При этом нельзя не отменить интерес научного сообщества к проблеме использования ИИ в деятельности следователя. Количество и качество публикаций по данной тематике свидетельствует о востребованности этого нового механизма, разработке общих и частных криминалистических методик, поиске путей интеграции ИИ в следственную деятельность. Результаты

исследований отражаются в работах А.А. Бессонова[1,2], В.В. Бычкова и В.А. Прорвича[3], О.В. Овчинниковой[4] и многих других.

Использование ИИ становится все более важным инструментом в борьбе с преступностью. ИИ - это тип компьютерной технологии, которая имитирует человеческий интеллект в форме обучения, рассуждений и решения проблем. В контексте расследования преступлений ИИ может использоваться для анализа больших объемов сложных данных и выявления закономерностей и взаимосвязей, которые трудно или невозможно было бы обнаружить аналитику-человеку.

Одно из возможных применений ИИ в расследовании преступлений - анализ больших данных (big data). Правоохранительные органы могут использовать ИИ для просеивания огромных объемов данных, собранных из различных источников, таких как социальные сети, камеры наблюдения и вышки сотовой связи. Анализируя эти данные с помощью алгоритмов машинного обучения, следователи могут извлечь ценную информацию, которая поможет им выявить преступников и раскрыть преступления.

Технология ИИ также может быть использована для прогнозирования преступной деятельности. Предиктивная правоохранительная деятельность - пример того, как ИИ может использоваться для предотвращения преступлений до их совершения. Алгоритмы предиктивной правоохранительная деятельности используют исторические данные о преступности для выявления районов, которые более подвержены преступной деятельности. Затем правоохранительные органы могут сконцентрировать свои ресурсы в районах, где вероятность преступлений выше, что снижает потенциал преступной активности в этих районах.

Еще одно применение ИИ в расследовании преступлений - это анализ доказательств. Такие криминалистические методы, как профилирование ДНК, анализ отпечатков пальцев и баллистическая экспертиза, уже несколько десятилетий используются для идентификации подозреваемых и установления их связи с преступлениями. ИИ может повысить точность и эффективность этих методов. Например, Компанией Папилон возможности нейросетей реализованы в продукте Папилон-Нейро.[5] Кроме этого, технология распознавания изображений на базе ИИ может анализировать записи камер наблюдения для определения черт лица и других характеристик подозреваемого, которые затем

---

[1] Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. – Москва: Проспект, 2021. -816 с.
[2] Бессонов А.А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. №1 (35).
[3] Бычков В. В., Прорвич В. А. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета // Правопорядок: история, теория, практика. 2021. №2 (29).
[4] Овчинникова О. В. Перспективы применения искусственного интеллекта в досудебном производстве // Правопорядок: история, теория, практика. 2022. №1 (32).
[5] https://www.papillon.ru/wp-content/uploads/Info_103.pdf (дата обращения 25.04.2023).

могут быть сопоставлены с имеющимися в распоряжении правоохранительных органов изображениями.

Существенный вклад ИИ может внести в одну из актуальнейших проблем современности – противодействие киберпреступности. Рост киберпреступности стал серьезной проблемой для правоохранительных органов во всем мире. Преступники становятся все более изощренными в своей тактике, что затрудняет для следователей их выявление и преследование.

ИИ обладает огромным потенциалом, когда речь идет о расследовании киберпреступлений. Он может быть использован различными способами, включая:

1. Прогнозирующий анализ: Алгоритмы ИИ могут использоваться для анализа огромных объемов данных с целью выявления закономерностей и прогнозирования будущих кибератак. Этого можно достичь путем анализа исторических данных, выявления известных вредоносных программ и обнаружения аномалий.

2. Обнаружение мошенничества: ИИ может использоваться для обнаружения мошеннических действий, например, мошенничества с кредитными картами, путем анализа моделей транзакций и выявления любых аномалий.

3. Поведенческий анализ: Алгоритмы ИИ могут использоваться для анализа поведения пользователей и выявления любой подозрительной активности, которая может указывать на кибератаку.

4. Автоматизированное обнаружение и реагирование на угрозы: Инструменты на базе ИИ могут быть развернуты для мониторинга систем и сетей с целью обнаружения любых потенциальных угроз. Эти инструменты также могут быть настроены на автоматическое реагирование на любые выявленные угрозы путем их блокирования или изоляции.

Преимущества использования ИИ в расследовании киберпреступлений:

1. Скорость: Инструменты на базе ИИ могут анализировать огромные объемы данных в сети в режиме реального времени, помогая следователям быстро выявлять кибератаки и реагировать на них.

2. Точность: Алгоритмы ИИ могут выявлять закономерности и аномалии, которые могут быть неочевидны для человека, проводящего расследование, тем самым обеспечивая более точную оценку рисков киберпреступлений.

3. Масштабируемость: Инструменты на базе ИИ могут быть увеличены или уменьшены в зависимости от размера сети, за которой ведется наблюдение. Это облегчает правоохранительным органам работу с расследованиями разного масштаба.

Недостатки использования ИИ в расследовании киберпреступлений:

1. Ограниченное понимание: Алгоритмы ИИ опираются на исторические данные для выявления закономерностей и аномалий. Однако киберпреступники постоянно развивают свою тактику, что затрудняет алгоритмам ИИ обнаружение новых типов кибератак.

2. Стоимость: Разработка и развертывание инструментов на базе ИИ может быть дорогостоящей, причем затраты включают как их приобретение, так и техническое обслуживание, а также затраты на электроэнергию.

3. Конфиденциальность данных: Использование ИИ в расследовании киберпреступлений предполагает сбор огромного количества данных, что вызывает обеспокоенность по поводу конфиденциальности и защиты данных.

ИИ способен произвести революцию в расследовании киберпреступлений, выявляя закономерности и аномалии в больших массивах данных. Однако его эффективность зависит от качества анализируемых данных и точности алгоритмов ИИ. Правоохранительным органам необходимо будет инвестировать в разработку и внедрение решений ИИ для расширения возможностей расследования киберпреступлений.

Использование ИИ в расследовании преступлений вызывает озабоченность по поводу неприкосновенности частной жизни и гражданских свобод. Использование алгоритмов ИИ и прогнозных моделей должно быть прозрачным и подотчетным, чтобы гарантировать, что они не дискриминируют определенные группы населения и не закрепляют существующие предубеждения. Согласимся с мнением И.Б. Воробьевой[1] о том, что использование ИИ в расследовании преступлений должно подчиняться этическим и правовым рамкам, регулирующим его использование, включая законы о защите данных и частной жизни.

Также заслуживают внимания выводы В.В. Бирюкова и Т.П. Бирюковой о том, что «важнейшим условием внедрения искусственного интеллекта является алгоритмизация расследования, а для того, чтобы научить машину, надо изначально научить человека, который ее будет обучать, любая ошибка или некомпетентность на этапе обучения машины (формирования базы знаний) или введения данных в базы данных недостоверной, непроверенной информации чревата ошибками в предлагаемых следователю рекомендациях и алгоритмах расследования»[2].

В заключение отметим, что ИИ является мощным инструментом для правоохранительных органов, позволяя им анализировать сложные данные, прогнозировать преступную деятельность и совершенствовать криминалистические методы. Однако его использование должно быть прозрачным и подотчетным, а его применение должно руководствоваться этическими и правовыми принципами. Ответственное использование ИИ в расследовании преступлений имеет огромный потенциал повышения уровня общественной безопасности и снижения уровня преступности.

Литература

1. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. – Москва: Проспект, 2021. -816 с.

[1] Воробьёва И.Б. Этические аспекты использования систем искусственного интеллекта при расследовании преступлений // Вестник СГЮА. 2022. №4 (147).

[2] Бирюков В.В., Бирюкова Т.П. Современные возможности использования потенциала компьютерных технологий в расследовании преступлений // Вестник юридического факультета Южного федерального университета. 2022. №3.

2. Бессонов А.А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. №1 (35).
3. Бирюков В.В., Бирюкова Т.П. Современные возможности использования потенциала компьютерных технологий в расследовании преступлений // Вестник юридического факультета Южного федерального университета. 2022. №3.
4. Бычков В. В., Прорвич В. А. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета // Правопорядок: история, теория, практика. 2021. №2 (29).
5. Воробьёва И.Б. Этические аспекты использования систем искусственного интеллекта при расследовании преступлений // Вестник СГЮА. 2022. №4 (147).
6. Овчинникова О. В. Перспективы применения искусственного интеллекта в досудебном производстве // Правопорядок: история, теория, практика. 2022. №1 (32).

Е.А. Зайцева

Внедрение дистанционных технологий в отечественном досудебном и судебном производстве по уголовным делам

Аннотация. В статье дается обзор порядка внедрения дистанционных технологий в уголовном судопроизводстве. Делается вывод о приоритетном оснащении средствами видео-конференц-связи и нормативном регулировании работы этих средств в судебном производстве. Анализируются причины «отставания» досудебного производства в части внедрения дистанционных технологий.

Ключевые слова: цифровизация уголовного судопроизводства, дистанционные технологии, дистанционный допрос, видео-конференц-связь.

Успешно противостоять в современных условиях киберпреступности, использующей достижения технического прогресса в сфере информационно-телекоммуникационных технологий и компьютерных сетей, весьма сложно. Решение этой задачи требует адекватного реагирования со стороны правоохранительных органов, которые также должны активно внедрять в правоприменительную практику возможности компьютерных и дистанционных технологий, что диктует потребность в создании четких нормативных основ функционирования в уголовном процессе соответствующего оборудования и закрепления в процессуальных документах результатов его применения.

Законодатель, реагируя на эти тенденции, постепенно вводит в текст УПК РФ новеллы, направленные на урегулирование отношений, возникающих по поводу использования в уголовном судопроизводстве дистанционных технологий. Так, в ч. 6 ст. 35 УПК РФ, введенной Федеральным законом от 27.12.2009 № 346-ФЗ,

упоминается возможность участия обвиняемого посредством видео-конференц-связи (ВКС) в заседании суда при решении вопроса об изменении территориальной подсудности уголовного дела для обеспечения безопасности участников процесса. При этом первоначальная редакция проекта данного Федерального закона (№ 250826-5) не содержала новелл о применении дистанционных технологий – они появились в тексте законопроекта, подготовленном ко второму чтению[1].

В ходе реформирования системы проверочных судебных производств Федеральным законом от 29.12.2010 № 433-ФЗ было предусмотрено участие осужденного, содержащегося под стражей, в апелляционном суде с помощью систем видеоконференц-связи (ст. 389.12 УПК РФ); закреплено право апелляционной инстанции дистанционно исследовать доказательства (ст. 389.13 УПК РФ); установлена возможность участия осужденного посредством ВКС в заседании кассационного суда (ст. 401.13 УПК РФ).

В 2011 г. ст. 240 УПК РФ была дополнена новой частью 4, предусматривающей использование систем ВКС при допросе судом потерпевших и свидетелей (Федеральный закон от 20.03.2011 № 39-ФЗ). Данный закон также ввел в УПК РФ новую статью 278.1. «Особенности допроса свидетеля путем использования систем видеоконференц-связи», фактически регламентировав алгоритм дистанционного допроса свидетеля в суде.

В тот же день, 20 марта 2011 г. был принят Федеральный закон № 40-ФЗ, который дополнил ч. 2 ст. 399 УПК РФ, регламентирующую процедуры рассмотрения процессуальных вопросов в стадии исполнения приговора, положением о возможности участия осужденного в заседании суда с помощью ВКС. Аналогичные возможности в стадии исполнения приговора для потерпевшего и его законного представителя (представителя) были предусмотрены Федеральным законом от 23.07.2013 № 221-ФЗ, которым в ст. 399 УПК РФ была введена новая часть 2.1.

Федеральным законом от 21.07.2014 № 251-ФЗ ст. 241 УПК РФ была дополнена новой частью 6.1, закрепляющей основание участия в судебном заседании подсудимого, содержащегося под стражей, посредством ВКС. Этим же законом была скорректирована ст. 293 УПК РФ, предусматривающая порядок реализации права подсудимого на последнее слово, который теперь получил возможность обращаться с таковым к суду посредством систем видео-конференц-связи.

В числе последних дополнений УПК РФ, нацеленных на расширение использования дистанционных технологий в уголовном судопроизводстве, - ст. 473.4 УПК РФ, закрепившая право присутствовать в судебном заседании посредством ВКС содержащемуся под стражей лицу, чье имущество по решению суда иностранного государства подлежит конфискации (Федеральный закон от 05.12.2017 № 387-ФЗ). Также Федеральным законом от 29.12.2022 № 610-ФЗ был

[1] См.: Законопроект № 250826-5. Система обеспечения законодательной деятельности Государственной Думы Федерального Собрания Российской Федерации. URL: https://sozd.duma.gov.ru/bill/250826-5 (дата обращения: 20.03.2023).

заново прописан общий алгоритм использования судом систем ВКС в новой ст. 241.1 УПК РФ, тем самым в главе 35 УПК РФ было *закреплено еще одно общее условие судебного разбирательства.*

Таким образом, мы видим массированное проникновение дистанционных технологий в судебную деятельность при отправлении правосудия по уголовным делам судами первой инстанции, при проверке не вступивших и вступивших в законную силу судебных решений, а также при разрешении вопросов, связанных с исполнением приговора (в том числе – приговора иностранного государства в рамках международного сотрудничества).

При этом законодатель упорно (вплоть до декабря 2021 г.) обходил молчанием не менее востребованный (с точки зрения дистанционного режима) сегмент процессуальной деятельности – досудебное производство по уголовным делам[1]. Чем это было обусловлено? Полагаем, тому несколько причин.

Во-первых, *причины институционального свойства*. Ввиду того, что российский уголовный процесс тяготеет к смешанному типу, судебное производство в нем организовано в состязательном формате, что предусматривает особый режим судоговорения, исследования доказательств судом с участием сторон. В досудебном производстве, построенном на розыскных началах, реализуется иная модель формирования и исследования доказательств, что требует дополнительных гарантий достоверности получаемой информации.

Во-вторых, *причины процессуально-технологического характера*, обусловленные особенностями процессуальной формы доказательственной деятельности в суде и на предварительном расследовании. В случае недоступности для следователя (дознавателя) свидетеля или потерпевшего, уехавшего в другой регион, применялся институт поручения (ч. 1 ст. 152 УПК РФ), что позволяло субъекту расследования, не покидая место своей дислокации, получить протокол допроса или другого следственного действия в довольно сжатые сроки (в 10-суточный срок). Что касается судебного производства, то в силу принципа непосредственности (ст. 240 УПК РФ) суд должен сам заслушать все показания, лично обозреть вещественные доказательства и документы[2], чтобы обеспечить себе надежную доказательственную основу для разрешения уголовного дела по существу. Именно эта особенность диктует необходимость непосредственно получать информацию из первоисточника (путем допроса свидетелей, потерпевших, подсудимых, специалистов, экспертов), а не перелагать ответственность за извлечение и закрепление доказательственной информации на других субъектов доказывания. Чтобы заслушать допрашиваемых лиц, находящихся на удалении, суд должен иметь технологические возможности, вытекающие из специфики процессуальной формы. Эти возможности нашли нормативное воплощение в виде

[1] Исключение –Федеральный закон от 06.06 2019 № 120-ФЗ. Однако надо отдавать себе отчет в том, что этот акт распространяет свое регулятивное воздействие только на отношения, возникающие в связи с исполнением запросов о правовой помощи в рамках международного сотрудничества в уголовном судопроизводстве.

[2] Конечно же, при рассмотрении уголовного дела в общем порядке.

соответствующих новелл, анализ которых был дан нами выше. Ну и нужно учитывать то обстоятельство, что в случае неявки в суд одного из свидетелей, допросить которого необходимо для правильного разрешения уголовного дела, суду придется отложить дело слушанием – до получения возможности явки данного лица в судебное заседание. При этом прибывшие в суд участники со стороны защиты и обвинения оказываются в состоянии «вынужденного простоя», а заседание придется возобновить после обеспечения явки этого свидетеля в суд.

В-третьих, *причины технического свойства, которые тесно связаны с экономическими причинами*. Если сравнить тенденции, которые характеризуют ряд важных аспектов досудебного и судебного производства в этом ключе, можно заметить, что эти тенденции – «разновекторные». Так, в 2011 г. «основные» органы предварительного расследования подверглись реформированию, которое привело к существенному сокращению кадрового состава следственных подразделений и подразделений дознания ОВД. Финансирование не увеличивалось, экономические проблемы решались за счет «внутренних резервов» (за счет экономии на сокращении личного состава). А практически в это же время Правительство РФ выносит Распоряжение от 20.09.2012 г. № 1735-р «Об утверждении Концепции федеральной целевой программы «Развитие судебной системы России на 2013-2020 годы»»[1], где среди целевых показателей успешности реализации данной Программы обозначено достижение в 2017 г. 95% оснащенности комплектами ВКС федеральных судов общей юрисдикции (исходя из имеющихся в 2012 г. лишь 3%)[2].

Вышеуказанные причины в комплексе и создали ситуацию, когда дистанционные технологии прочно вошли в арсенал познавательных средств именно представителей судейского корпуса, получив законодательную «прописку» в УПК РФ. Реально к проблемам оснащения досудебного производства эффективными дистанционными средствами в нормативном аспекте законодатель обратился лишь в декабре 2021 г., когда Федеральным законом от 30.12.2021 № 501-ФЗ в УПК РФ была введена статья 189.1 «Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи». Позитивно оценивая этот шаг в контексте оптимизации ряда процедур предварительного расследования, тем не менее выскажем критические замечания относительно запрета, закрепленного в ч. 8 данной статьи, использовать системы ВКС при возможности разглашения государственной или иной охраняемой федеральным законом тайны либо данных о лице, в отношении которого приняты меры безопасности. Полагаем, указанные риски вполне «нейтрализуются» при использовании защищенных каналов связи («например сервиса видеоконференц-связи единой системы информационно-аналитического обеспечения деятельности МВД России», в том

[1] См: Об утверждении Концепции федеральной целевой программы «Развитие судебной системы России на 2013-2020 годы»: распоряжение Правительства РФ от 20 сентября 2012 г. № 1735-р // Собрание законодательства РФ. 2012. № 40. Ст. 5474.

[2] См.: Приложение № 1 к Концепции федеральной целевой программы «Развитие судебной системы России на 2013 - 2020 годы».

числе – с возможностью подключения мобильных устройств, о чем справедливо пишет О.А. Попова[1]). Для следователей (дознавателей) иных ведомств также доступны каналы ведомственной связи, что можно было бы учесть законодателям при конструировании норм данной статьи.

Литература

1. Законопроект № 250826-5 [Электронный ресурс]. Система обеспечения законодательной деятельности Государственной Думы Федерального Собрания Российской Федерации. URL: https://sozd.duma.gov.ru/bill/250826-5. (дата обращения: 20.03.2023).
2. Об утверждении Концепции федеральной целевой программы «Развитие судебной системы России на 2013-2020 годы»: распоряжение Правительства РФ от 20 сентября 2012 г. № 1735-р // СЗ РФ. 2012. № 40. Ст. 5474.
3. Федеральный закон от 27.12.2009 № 346-ФЗ «О внесении изменений в статьи 31 и 35 Уголовно-процессуального кодекса Российской Федерации» // СЗ РФ. 2009. № 52 (1 ч.). Ст. 6422.
4. Федеральный закон от 29.12.2010 № 433-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации» // СЗ РФ. 2011. № 1. Ст. 45.
5. Федеральный закон от 20.03.2011 № 40-ФЗ «О внесении изменений в статью 399 Уголовно-процессуального кодекса Российской Федерации» // СЗ РФ. 2011. № 13. Ст. 1687.
6. Федеральный закон от 23.07.2013 № 221-ФЗ «О внесении изменений в статью 83 Уголовного кодекса Российской Федерации и статью 399 Уголовно-процессуального кодекса Российской Федерации» // СЗ РФ. 2013. № 30 (Часть I). Ст. 4054.
7. Федеральный закон от 21.07.2014 № 251-ФЗ «О внесении изменений в статьи 241 и 293 Уголовно-процессуального кодекса Российской Федерации» // СЗ РФ. 2014. № 30 (Часть I). Ст. 4252.
8. Федеральный закон от 06.06.2019 № 120-ФЗ «О ратификации Второго дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам» // СЗ РФ. 2019. № 23. Ст. 2903.
9. Федеральный закон от 29.12.2022 № 610-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СЗ РФ. 2023. № 1 (часть I). Ст. 57.
10. Попова О.А. Организационные и процессуальные аспекты участия в уголовном судопроизводстве в режиме удаленного доступа // Вестник Волгоградской академии МВД России. 2020. № 3 (54). С. 111-117.

[1] Попова О.А. Организационные и процессуальные аспекты участия в уголовном судопроизводстве в режиме удаленного доступа // Вестник Волгоградской академии МВД России. 2020. № 3 (54). С. 115.

М. Н. Зиганшин

Технико-криминалистические особенности изъятия электронной информации

Аннотация. В статье рассматриваются особенности работы следственных органов с электронными носителями информации. Обозначены и проанализированы некоторые проблемы, возникающие при копировании, изъятии электронный информации. Изложены особенности исследования данного вида объектов в качестве вещественных доказательств.

Ключевые слова: цифровые следы; электронные носители информации; программное обеспечение; искусственный интеллект.

В практике предварительного следствия традиционно принято считать, что собирание доказательств представляет собой систему действий, направленных на восприятие объективно существующих следов происшедшего события и их процессуальную фиксацию[1].

В современных масштабах развития информационной обеспеченности общественности роль и значение доказательственной информации, содержащейся на электронных носителях, в уголовном судопроизводстве приобретает фактическую значимость, в связи с чем возникает необходимость регулирования порядка ее собирания нормативно-правового актами.

В ст. 86 УПК РФ законодатель не приводит определение процесса собирания доказательств, отмечая лишь, что он «осуществляется дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий».

Следует отметить, что в приведенной норме содержится также указание на процессуальные формы собирания доказательств для подозреваемого, обвиняемого, а также потерпевшего, гражданского истца, гражданского ответчика, их представителей, а также защитника.

Начальная и необходимая стадия собирания доказательств – это обнаружение доказательств означает их отыскание, выявление, установление тех или иных фактических данных, имеющих доказательственное значение[2].

Новые достижения науки и техники способны выполнять вспомогательные функции, а в перспективе и системы, в которых искусственный интеллект имеет возможность анализировать уголовные дела и безошибочно делать выводы о необходимости проведения того или иного следственного действия, строить следственные версии и судить о виновности лиц, что поможет научить машину анализировать человека, ведя с ним диалог[3].

---

[1] Чурилов С. Н. Криминалистическая методика расследования. М.: Юстицинформ, 2017. 204 с. 38.

[2] Тюнис И.О. Криминалистика. Учебное пособие. – М: Проспект, 2020. 220 с. 27.

[3] Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук / А.И. Зазулин.– Екатеринбург, 2018. 250 с. 143.

В таком случае перед разработчиками будет стоять задача создания алгоритма, который позволит роботизированному механизму составлять вопросы для допрашиваемого на основе имеющихся сведений в материалах уголовного дела, менять их в зависимости от ответов и, одновременно с этим, по мимике, жестикуляции и иным признакам определять степень правдивости показаний.

Ввод в действие таких разработок повлечет за собой возникновения нового ряда вопросов. В первую очередь предоставление искусственному интеллекту возможности самостоятельно проводить следственное действие подразумевает необходимость наделить робота процессуальным статусом, либо только лишь определить его как техническое средство, выполняющее вспомогательную функцию для должностного лица. В случае наделения процессуальным статусом искусственного интеллекта, возникает необходимость определения того, кто будет нести ответственность в случае допущения роботизированным механизмом технических или юридических ошибок.

В настоящее время представляется необходимостью оставить право последнего слова за следователем, ведь искусственный интеллект на данной стадии развития не обладает достаточными психическими, нравственными и мыслительными способностями, чтобы суметь оценить последствия неверных действий, понять свою вину, а главное понести ответственность.

Однако сами создатели таких систем при вводе их в эксплуатацию не могут спрогнозировать и предотвратить всех последствий использования роботизированных механизмов. Возможно, законодатель определит участниками уголовного процесса не только физических лиц, но и роботов, наделенных системами искусственного интеллекта, ведь установленный порядок сбора доказательств, в том числе и на электронных носителях информации, должен быть ускорен.

В первую очередь для этого будет необходимо расширить количество нормативно-правовых актов или отдельных норм права, связанных с регулированием сферы робототехники. До тех пор, пока искусственный интеллект по своему процессуальному статусу не будет приравнен к сотрудникам следственных органов, такая система будет считаться техническим средством, не способным составить конкуренцию экспертам-криминалистам, следователям и иным лицам, уполномоченным производить следственные действия.

В настоящее время законодателем сформулированы универсальные требования к порядку собирания доказательств на электронных носителях в специально введенной ст. 164.1 УПК РФ. Так, копирование информации определено в качестве приоритетного способа собирания доказательств на электронных носителях по уголовным делам о преступлениях экономической направленности, совершенных в сфере предпринимательской деятельности.

Определен исчерпывающий перечень исключений, позволяющих осуществлять изъятие электронных носителей информации. Существует рекомендация, что изъятие электронных носителей информации должно осуществляться с участием специалиста.

В реальной обстановке, когда, например, объем данных слишком велик или на самом носителе информации могут содержаться запрещенные к распространению сведения не могут быть оставлены пользователю, возникает необходимость производить изъятие. Изъятие электронных носителей допускается на основании судебного решения. Полномочия суда закреплены в ст. 29 УПК РФ, где предусмотрен перечень решений, принимаемых судом в ходе досудебного производства. При этом решения суда об изъятии электронных носителей информации в данном перечне не содержится.

Следует отметить, что применительно к п. 2 ч. 1 ст. 164.1 УПК РФ основаниями для изъятия электронных носителей информации выступают решения суда о производстве обыска и (или) выемки в жилище, в ходе которых происходит изъятие электронных носителей информации, а также о производстве выемки предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, а также предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, которые могут содержаться на электронных носителях информации, в связи с чем подлежат изъятию.

Помимо этого, особенностью изъятия носителя информации является право владельца на получение копии электронной информации. В таком случае он должен сам представить носитель, на который специалист производит копирование.

Существует программное обеспечение, в том числе, отечественное, способное зафиксировать факт совершения противоправного деяния, данные из которого могут стать доказательством в суде.

Исходя из изложенного, можно сделать вывод, что в настоящее время сбор электронной информации с электронных носителей зачастую происходит посредствам копирования информации. В других случаях приходится проводить изъятие электронных носителей информации, что требует получения судебного разрешения[1] и привлечения специалиста.

Однако с развитием технологий и появлением специального программного обеспечения появляется необходимость принимать во внимание наличие иных источников получения информации, которые потребуется использовать при расследовании уголовных дел.

Литература

1. Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дис. … канд. юрид. наук / А.И. Зазулин. [Текст] – Екатеринбург, 2018. 250 с. 143
2. Тюнис И.О. Криминалистика. Учебное пособие [Текст]. – М: Проспект, 2020. 220 с. 27.
3. Чурилов С. Н. Криминалистическая методика расследования [Текст]. М.: Юстицинформ, 2017. 204 с. 38.

[1] См. ч.4.1 ст.164 УПК РФ

В.С. Калашников

Территориальная подследственность уголовных дел о преступлениях, совершенных с использованием информационно-коммуникационных технологий

Аннотация. Статья посвящена вопросу установления места совершения компьютерного преступления. Рассмотрено соотношение информационного и физического пространства в целях определения места расследования преступления. Предложено на первоначальном этапе расследования территориальную подследственность определять по месту нахождения потерпевшего.

Ключевые слова: территориальная подследственность, киберпреступления, информационное пространство, информационно-коммуникационные технологии, место совершения преступления, потерпевший.

Одной из особенностей научно-технического прогресса является то, что открытие в той или иной сфере деятельности вызывает цепную реакцию, влекущую разработку научно-технических средств, количественно и качественно увеличивающихся в геометрической прогрессии. Еще пятьдесят лет назад персональный компьютер не являлся обязательным устройством, находящимся в каждой квартире и, фактически, нужен был только тем, кто выполнял на нем специфические задачи, например, вычислительные. В настоящее время громоздкая техника успешно заменяется компактным ноутбуком или ультрабуком, планшетом, смартфоном, в зависимости от целей использования.

Научно-технический прогресс, облегчив жизнь во многих сферах жизни, не обошел вниманием и преступную деятельность. Некоторые преступления стало проще совершать, другие перешли на более качественный уровень, появились новые противоправные деяния, в процессуальном законодательстве закрепились электронные носители информации. В юридической (и не только) литературе все чаще стали встречаться такие словосочетания, как информационная безопасность, кибератака, киберпреступления, информационно-коммуникационные технологии, и даже кибероружие. Большинство из указанных терминов связывают с так называемым информационным пространством, которое, в свою очередь, может быть как национальным, так и международным.

Само по себе пространство принято понимать как некоторую объективную реальность или часть ее, имеющую протяженность и объем, как место, где что-нибудь вмещается[1]. Уголовно-процессуальное законодательство предполагает совершение преступлений в этом самом физическом пространстве, имеющим

[1] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. М.: Азбуковник, 1999. С.622.

конкретные привязки к точкам на поверхности земного шара, с которыми и связано общее правило определения территориальной подследственности.

В настоящее время с использованием компьютера и компьютерных технологий можно совершить преступление почти из каждой главы Особенной части УК РФ. При этом, часть действий объективной стороны могут выполняться в так называемом информационном пространстве.

Как следует из Соглашения между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности", заключенного в г. Екатеринбурге 16.06.2009, "информационное пространство" - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[1].

Объективно, информационное пространство представляет собой набор данных в виде электрических сигналов. Оно существует одновременно везде, где находятся устройства, подключенные к указанной сети. В этом информационном пространстве могут совершаться противоправные деяния. Например, взлом электронного почтового ящика и копирование оттуда личной информации происходит, как правило, не на конкретных устройствах, принадлежащих пользователям. Почтовый ящик и его содержимое не находится на компьютере или ином устройстве потерпевшего, с которого он осуществляет доступ к своей почте. Равно как и злоумышленник на своем вычислительном устройстве лишь нажимает на клавиши, отправляя команды за пределы устройства и оказывая воздействие на объект, физическое расположение которого ему, скорее всего, не известно. Понятно, что следуя за электрическими сигналами, можно добраться до конкретного сервера на материальном носителе. Но определять территориальную подследственность такого преступления по месту нахождения сервера равносильно отмененной практике расследования дистанционных хищений с банковского счета по месту нахождения кредитной организации, в которой этот счет открыт.

А между тем, существующие правила определения территориальной подследственности немного не успевают за временем. Общее положение о расследовании уголовного дела по месту совершения преступления отсылает к особенностям окончания каждого отдельного состава преступного деяния.

При этом п.19 Постановления Пленума Верховного суда РФ от 15 декабря 2022 г. № 37 говорит, что при определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети "Интернет", и, соответственно, территориальной подсудности уголовного дела судам необходимо учитывать, что доступ к данной

[1] Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Заключено в г. Екатеринбурге 16.06.2009 // СПС «КонсультантПлюс». Дата обращения 25.04.2023.

сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных). Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления[1].

В свою очередь, Постановление Пленума Верховного Суда РФ от 27 декабря 2002 № 29[2] и Постановление Пленума Верховного Суда РФ от 30 ноября 2017 года № 48[3] уже не так категоричны. В частности, когда речь идет о хищении с банковского счета местом его совершения является, как правило, место совершения лицом действий, направленных на незаконное изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет).

Однако такой подход не совсем применим к преступлениям, предусмотренным ст.159 УК РФ. Даже в классическом мошенничестве потерпевший условно выполняет часть объективной стороны, а именно в том временном промежутке, когда злоумышленник осуществил, например, обман, и до момента получения им имущества, которым есть возможность распорядиться, потерпевшим производятся действия по передаче этого имущества.

Похожая схема реализуется и в отношении денежных средств, размещенных на банковском счете. Потерпевший самостоятельно осуществляет действия, направленные на списание средств со счета, и только после этого преступление считается оконченным. Возникает вопрос: в каком месте, в этом случае, выполняется объективная сторона?

Возникают проблемы с определением места преступления в случаях, когда используется социальная инженерия и преступники действуют группой лиц, находясь при этом в разных субъектах РФ. При этом каждый из злоумышленников вносит свою лепту в обман потерпевшего, а действия по переводу, как правило, совершаются не там, где находятся преступники.

Хищения криптовалют или иных цифровых финансовых активов ввиду особенностей использования и хранения тоже порождают проблемы правоприменения. Мошеннику достаточно один раз создать поддельный сайт по обмену валют, разместить его в сети «Интернет» и на протяжении неограниченного времени получать преступный доход, пассивно наблюдая, как

---

[1] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" // "Российская газета", № 294, 28.12.2022

[2] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) "О судебной практике по делам о краже, грабеже и разбое" // "Российская газета", № 9, 18.01.2003.

[3] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" //"Российская газета", № 280, 11.12.2017.

жертвы сами перечисляют ему деньги. Если следовать существующей практике, место преступления будет находиться по месту расположения компьютера, с которого этот сайт был впервые запущен.

При этом такие примеры можно найти в любом разделе Особенной части Уголовного кодекса РФ (склонение к самоубийству через сеть «Интернет», развратные действия в отношении малолетних через мессенджеры, распространение порнографии в социальных сетях и т.д.)

Дополнительной проблемой при определении территориальной подследственности, даже по общему правилу, является тот факт, что по большинству преступлений на момент возбуждения уголовного дела не известно, где была выполнена объективная сторона.

Можно использовать исключения из общего правила определения территориальной подследственности, установленные ст.152 УПК РФ. Но и в этих случаях приходится учитывать специфику преступления. Где будет считаться оконченным склонение к самоубийству, если для привлечения к ответственности не обязательно, чтобы потерпевший даже предпринял неудачную попытку суицида?

Место нахождения обвиняемого, особенно когда он неизвестен, не приближает правоприменителя к ответу на вопрос о территории расследования. Место нахождения большинства свидетелей тоже не всегда подходящий вариант. Во-первых, по таким преступлениям показания свидетелей далеко не главный вид доказательств, чаще выступают иные документы. Во-вторых, если день ото дня в разных регионах будет меняться количество свидетелей, указанное правило будет нарушено.

Еще одно исключение содержится в ч.4.1 ст.152 УПК РФ, согласно которой расследование может осуществляться по месту жительства потерпевшего. Учитывая специфику совершения преступлений с использованием информационно-коммуникационных технологий, целесообразно было бы на первоначальном этапе расследования распространить это правило на все подобные деяния, а уже потом, по мере собирания доказательственной базы, а также в случаях соединения уголовных дел, решать вопрос о подследственности по другим исключениям из общего правила определения места расследования.

Литература

1. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. М.: Азбуковник, 1999. 944 с.

М. В. Кардашевская

Понятие и виды цифровых следов

Аннотация. В статье обосновывается мнение, что цифровые следы по своему существу обнаруживают признаки документа. Автор дает понятие цифровых следов как документа и проводит их классификацию. На основании нормативных правовых актов раскрывается содержание отдельных видов цифровых следов.

Ключевые слова: цифровой след, документ, признаки, виды, документоведение.

При совершении правонарушений с использованием нынешних информационных технологий остаются следы, являющиеся значительной составной долей системы физически закрепленных следов. Данные следы в последние годы входят в доказательственную базу практически по каждому уголовному делу.

Цифровой след относится к сведениям (сообщениям, данным), представленным в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим. 1 к ст. 272 УК России).

Некоторые авторы относят данные следы к материальным невидимым следам[1]. Однако, это не совсем верная точка зрения. Да, этот след материален, поскольку он, как и любая иная информация, имеет свой носитель. Но поскольку эти сведения находятся на носителе, то их можно прочитать, просмотреть и иным способом изучить. То есть эти следы не являются невидимыми. С точки зрения криминалистики цифровой след – это документ, т. е. информация, хранящаяся на любом носителе, в том числе и электронном. Под ним надлежит понимать материальный носитель, который записывает, хранит и воспроизводит данные, обрабатываемые благодаря вычислительной технике[2]. Таким образом, документ - цифровой след отличается от бумажного документа только способом его выполнения и должен изучаться в криминалистическом документоведении по всем правилам изучения документа: содержание документа, авторство и способ изготовления документа.

Для всех цифровых следов характерно, что они: (1) представляют собой одну из конфигураций компьютерных сведений; (2) постоянно опосредованы через искусственно сформированный физический объект – электронный носитель данных, без которого эти следы невозможно воспринимать и изучать; (3) дистанционно доступны для неограниченного количества людей; (4) могут неоднократно копироваться; (5) пригодны для использования в уголовном

[1] Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. М., 2021. С. 104 – 106.

[2] п. 3.1.9. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения».

процессе только при использовании специальных технических средств или в случае их переноса на бумажный носитель[1].

Все документы, содержащие цифровой след, можно классифицировать на следующие виды:

1. В зависимости от степени распространенности:

а) доступные для большинства пользователей:

Файл – это запись на электронном носителе, имеющая свое название и хранящая в закодированном виде конкретные сведения с реквизитами, которые позволяют их идентифицировать.

Сетевой адрес – его определение указано в п. 16 ст. 2 Федерального закона от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации»[2].

Доменное имя – также определено в Федеральном законе № 149 от 27.07.2006 г.[3]

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

База данных – это упорядоченный набор структурированной информации или данных, которые обычно хранятся в электронном виде в компьютерной системе.

Программа для ЭВМ – ее определение содержится в ст. 1261 ГК России.

б) финансовые документы:

Электронные денежные средства – их определение содержится в п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»[4]. Там же содержится и указание, что к электронным денежным средствам не относится.

Цифровая валюта – ее определение содержится в ч. 3 ст. 1 Федерального закона от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и внесении изменений в отдельные законодательные акты Российской Федерации»[5].

Электронный журнал – это документ, определение которого содержится в п. 1.3. главы 1 Положения Банка России от 24.12.2004 № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» [6].

в) официальные документы:

---

[1] Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М., 2017. С. 127 – 128.

[2] П. 16 ст. 2 Федерального закона от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // СПС «КонсультантПлюс».

[3] П. 15 ст. 2 Федерального закона от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // СПС «КонсультантПлюс».

[4] П. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (ред. от 02.07.2021) // СПС «КонсультантПлюс».

[5] Ч. 3 ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». // СПС «КонсультантПлюс».

[6] П. 1.3. гл. 1 Положения Банка России от 24.12.2004 № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» (ред. от 28.09.2020) // СПС «КонсультантПлюс».

Электронная подпись – подпись лица: выполненная в электронном виде; прикрепленная к другим электронным сведениям; позволяющая установить лицо, ее выполнившую[1].

Электронный документ – его содержание раскрывается в п. 11.1 ст. 2 Федерального закона № 149[2].

2. В зависимости от использования в уголовном судопроизводстве:

- документы – письменные доказательства;
- документы – вещественные доказательства

3. В зависимости от формы фиксации информации: текстовые документы; графические; видео-, аудиозапись; в виде цифрового обозначения (компьютерные программы);

4. в зависимости от происхождения: частные (страница в соцсетях, переписка и т.п.); официальные;

5. в зависимости от подлинности содержания: подлинные; вируснозараженные; обработанные специальными программами для сокрытия истинной информации.

6. По степени доступности: строго привязанные к определенному носителю; документ, к которому можно получить доступ с любого электронного носителя (например, доступ к электронной почте);

7. По характеристики электронного носителя информации.

Представляется, что изучение цифровых следов как документа поможет избежать ошибки в научных исследованиях и на практике, а также позволит совершенствовать теоретические положения криминалистического документоведения и разработать соответствующие практические рекомендации.

Литература

1. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения»
2. Положение Банка России от 24.12.2004 № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» (ред. от 28.09.2020) // СПС «КонсультантПлюс»
3. Федеральный закон от 06.04.2011 «Об электронной подписи» (ред. от 02.07.2021) // СПС «КонсультантПлюс»
4. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (ред. от 02.07.2021) // СПС «КонсультантПлюс»
5. Федеральный закон от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // СПС «КонсультантПлюс»

[1] П. 1 ст. 2 Федерального закона от 06.04.2011 «Об электронной подписи» (ред. от 02.07.2021) // СПС «КонсультантПлюс»

[2] П. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // СПС «КонсультантПлюс»

6. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». // СПС «КонсультантПлюс»
7. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. М., 2021. С. 104 – 106.
8. Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М., 2017. С. 127 – 128.

Е.А. Киселёв

Особенности личности преступника, совершающего преступления с использованием современных информационных и телекоммуникационных технологий

Аннотация. В статье рассматривается основная характеристика признаков личности преступника зпт совершающего преступления с использованием современных информационных и телекоммуникационных технологий. Обращается особое внимание на то, что знания о специфических чертах личности преступника совершающего преступления в данной сфере имеют важное значение для процесса расследования. При этом делается акцент на выявленные характерные особенности личности подобного рода субъектов преступлений.

Ключевые слова: особенности личности преступника; преступления, совершаемые с использованием современных информационных и телекоммуникационных технологий; криминалистическая характеристика преступлений; элементы криминалистической характеристики; расследование преступлений; компьютерная информация; IT-преступления.

В течении последнего десятилетия по данным статистической отчетности МВД России, наблюдается устойчивый тренд роста удельного числа преступных деяний, совершаемых с использованием современных информационных и телекоммуникационных технологий (IT-преступления). И как отмечается в последнем квартальном статистическом отчете МВД России за 2023 год каждое третье преступление в России совершено с использованием информационно-телекоммуникационных технологий. При этом подавляющее большинство из них носит корыстных характер[1]. Это в свою очередь на первый план выводит такой из важнейших элементов криминалистической характеристики преступления, как сведения об особенностях личности преступника его совершающих[2].

[1] По данным ГИАЦ МВД России за 2013 – январь-март2023 // Официальный сайт МВД РФ. URL: https://xn--b1aew.xn--p1ai/reports/ (дата обращения: 15.04.2023).

[2] См.: Ким, Е. П. О криминалистической характеристике преступлений, совершаемых с использованием современных информационных и телекоммуникационных технологий / Е. П. Ким, Е. А. Киселев, О. Н. Каравянская // Научный компонент. – 2020. – № 3(7). – С. 201-207.

В свою очередь, анализ практики расследования IT-преступлений, показывает, что практически невозможно выделить единообразную характеристику субъекта указанных преступлений,[1].

Согласно данным статистики большая часть подобных преступлений, совершаются мужчинами. Возрастные характеристики субъектов преступных деяний данного вида, практически, по нашему мнению, не является существенными ввиду развития компьютерных технологий и повсеместного охвата всех слоев населения.

Наиболее существенным обстоятельством, подлежащим установлению в процессе расследования, является мотив совершения преступления.

В криминалистической методике в зависимости от мотива совершения преступления, субъектов данного вида преступных деяний, традиционно подразделяют на следующие группы:

Первая – хакеры, к которым относятся лица, совершающие IT-преступления с использованием современных информационных и телекоммуникационных технологий, воспринимающие защиту компьютерных систем и сетей как личный вызов и нарушающие ее для получения доступа к системе для собственного удовольствия;

Вторая – шпионы, к которым относятся лица, совершающие IT-преступления с использованием современных информационных и телекоммуникационных технологий для получения информации, используемой в политических, военных и экономических целях;

Третья – террористы, к которым относятся лица, совершающие IT-преступления с использованием современных информационных и телекоммуникационных технологий, взламывающие информационные системы для создания эффекта опасности, используемого в целях политического воздействия;

Четвертая – корыстные преступники, к которым относятся лица, совершающие IT-преступления с использованием современных информационных и телекоммуникационных технологий для получения имущественных или неимущественных выгод;

Пятая – вандалы, к которым относятся лица, совершающие IT-преступления с использованием современных информационных и телекоммуникационных технологий с целью нарушения нормальной работы и разрушения компьютерных систем и сетей, как правило действующие из хулиганских побуждений;

Шестая – лица, страдающие психическими болезнями – компьютерными фобиями;

Седьмая – лица, совершающие IT-преступления по личным мотивам (месть, неприязненные отношения);

Восьмая – лица, руководствующиеся иными мотивами.

---

[1] См.: Настольная книга следователя / А. И. Бастрыкин, Ю. А. Цветков, Ю. В. Голик [и др.]. Том 2. – Санкт-Петербург : Московская академия Следственного комитета Российской Федерации, 2021. – 340 с.

При совершении конкретного преступления возможно наличие нескольких мотивов.

Особое место в классификации субъектов занимают хакеры. Для этой категории характерны оригинальные способы совершения преступлений, которыми впоследствии пользуются другие. Они также создают свои объединения (группы), ведут активную деятельность в глобальной сети Интернет, создают специализированные сайты.

Литература

1. Ким, Е.П. О криминалистической характеристике преступлений, совершаемых с использованием современных информационных и телекоммуникационных технологий / Е.П. Ким, Е.А. Киселев, О.Н. Каравянская // Научный компонент. – 2020. – № 3(7). – С. 201-207.
2. Настольная книга следователя / А. И. Бастрыкин, Ю. А. Цветков, Ю. В. Голик [и др.]. Том 2. – Санкт-Петербург : Московская академия Следственного комитета Российской Федерации, 2021. – 340 с.
3. Технико-криминалистическое сопровождение расследования преступлений / А.М. Багмет, Е.А. Бартенев, С.Н. Волочай [и др.]. – Москва : Издательство "Юрлитинформ", 2016. – 256 с.

Ю.Г. Клещенко

Классификация способов совершения хищений денежных средств с использованием электронных средств платежа

Аннотация. В статье рассматривается классификация способов совершения преступных посягательств на денежные средства граждан, размещенных на счетах и картах. Дается анализ основных норм УК РФ, предусматривающих ответственность за данные деяния. Указаны способы получения сторонними лицами кодов доступа проведения операции по банковскому счету.

Ключевые слова: способы хищений, платежная информация, банковская карта, код доступа.

Современные тенденции увеличения количества денежных расчетов с использованием дистанционных банковских технологий одновременно обуславливают стремительный рост преступных посягательств на денежные средства граждан, размещенных на счетах и картах. Рост количества таких преступлений особенно ускорился в первые месяцы пандемии COVID-19.[1]

[1] Сухаренко А.Н., Савченко М.М., Трунцевский Ю.В., Криминальные вызовы пандемии COVID-19 в России: Научно-практическое пособие. Москва: Общество с ограниченной ответственностью «Проспект», 2021. – 336 с.

Для разработки мероприятий для предотвращения данных деяний, а также для разработки методик расследования преступлений, необходимо провести систематизацию способов их совершения.

Рассмотрим, данную М.М. Савченко, классификацию способов совершения преступлений указанной группы в зависимости от технологии обработки платежной информации:[1]

1. Неправомерное осуществление наличных расходных операций в кассе банка неуполномоченными лицами от имени клиента.
2. Постоянное или временное физическое завладение чужой банковской картой и ее неправомерное использование для осуществления операций.
3. Копирование информации с банковской карты, ее электронной полосы, а также ее реквизитов, достаточных для осуществления расходных операций.
4. Неправомерное завладение кодами (из смс-сообщений, таблиц разовых ключей и т.д.), являющимися аналогами электронной цифровой подписи, позволяющими совершить одну или несколько конкретных банковских операций.
5. Неправомерное завладение информацией, позволяющей использовать все возможности дистанционного банковского обслуживания от имени клиента.
6. Введение клиента банка в заблуждение с последующим побуждением к совершению безналичных расходных операций в пользу виновных лиц и их сообщников.

Следует отметить, что вышеуказанная классификация проведена в зависимости от путей завладения виновными лицами платежной информации, однако в рамках некоторых видов возможна уголовно-правовая квалификация деяний по различным статьям УК РФ. Основными нормами, предусматривающими ответственность за такие деяния, являются:

–статьи 158 УК РФ (пункт «г» части 3) – «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3)»;

– статья 159.3 УК РФ – «Мошенничество с использованием электронных средств платежа»;

– статья 159.6 УК РФ – «Мошенничество в сфере компьютерной информации».

Как указывает ряд авторов, разграничение данных составов между собой в некоторых случаях является достаточно сложной задачей.[2] В целях обеспечения единообразия судебной практики по рассматриваемой категории дел Верховным

---

[1] Савченко М.М. Проблемы уголовно-правовой защиты безопасности денежных средства физических лиц, размещенных на счетах в банках. // Юридическое образование и наука № 4, 2021, С. 34-40.

[2] Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. 2018. № 9. С. 43-47; Яни П. Мошенничество с использованием электронных средств платежа // Законность. 2019. № 5. С. 25-28; Савченко М.М. Правовая природа безналичных и электронных денег как предмета преступных посягательств // Бизнес. Образование. Право, 2021, май № 2(55), С. 118-124.

судом Российской Федерации было принято соответствующее Постановление № 48 от 30.11.2017 года, однако постоянное совершенствование информационных технологий банковского обслуживания обуславливает появление новых способов совершения хищений в данной сфере, что ставит все новые вопросы в правоприменительной практике.[1]

Так, пункт «г» части 3 статьи 158 УК РФ является квалифицированным составом преступления, предусмотренного частью 1 статьи 158 УК РФ «Кража – тайное хищение чужого имущества». Анализ диспозиции данной статьи позволяет сделать вывод, что под ее действия попадают исключительно случаи тайного хищения, что подтверждается практикой Верховного Суда РФ (пункт 2 Постановления Пленума ВС Российской Федерации от 27 декабря 2002 г № «О судебной практике по делам о краже, грабеже и разбое»).[2]

Как тайное хищение чужого имущества (кража) следует квалифицировать действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них.

Хищение, совершенное с физическим использованием банковских карт, может быть квалифицировано в зависимости от способа реализации преступного замысла либо по п. «Г» ч. 3 ст. 158, либо по ст. 159.3 УК РФ.

Преступник может завладеть картой различными способами: украсть карту, найти чужую карту, временно тайно завладеть чужой картой; получить карту путем удержания ее в фиктивном банкомате или специальном устройстве, устанавливаемом на настоящий банкомат.

В случае если лицо, завладевшее банковской картой, тайно осуществляет расходную операцию в банкомате, получая наличные денежные средства либо перечисляя их безналичным платежом на свой счет, данное деяние следует рассматривать как кражу по соответствующей части статьи 158 УК РФ. Состава мошенничества не образует также ситуация, при которой злоумышленник обманом выясняет пин-код карты. Данная позиция подтверждается пунктом 2 Постановления Пленума Верховного Суда Российской Федерации № 48: «если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа».

Деяния, связанные с копированием банковских карт, получением информации о секретных кодах (CVV/CVC) или с магнитной полосы подлежат юридической квалификации в зависимости от способа дальнейшего использования полученных данных. Квалификация осуществляется аналогично операциям с физической картой как кража или мошенничество по статье 159.3 либо части 3 статьи 159.6 УК РФ в зависимости от того, каким образом используется поддельная карта – для получения наличных денег или оплаты товаров и услуг.

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс.

[2] Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» // СПС «КонсультантПлюс».

«В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража».

В последнее время количество совершенных таким способом деяний сокращается, так карты без чипа (только с магнитной полосой) российскими банками почти не выдаются, а копирование карт с чипом технически невозможно. При использовании реквизитов карты, в том числе секретных кодов, при оплате товаров, банками почти повсеместно используется дополнительная технология защиты 3dSecurity, а при ее отсутствии у владельца счета имеется возможность отмены операции.

Квалификация деяний, связанных с завладениями информацией и/или кодами, являющимися аналогом простой неквалифицированной электронно-цифровой подписи, зависит от установления следующих обстоятельств:

– каким способом получена вышеуказанная информация/коды;

– каким образом использована эта информация/коды.

Коды для подтверждения операции могут быть получены следующими способами:

– при использовании вредоносных компьютерных программ;

– при использовании потерпевшим поддельных ссылок на страницы с формами оплаты товаров или услуг;

– при неправомерном завладении абонентским устройством потерпевшего, в том числе при незаконном перевыпуске сим-карты;

– простым подсматриванием кодов, в том числе с применением технических средств и приспособлений;

– при введении в заблуждение потерпевшего относительно назначения кода (например, потерпевший думает, что это код, необходимый для получения денег на счет, либо код для отмены операции).

Проведенная в данной работе классификация способов совершения хищений с банковских счетов физических лиц может стать основой для планирования первоначальных следственных действий и определения источников получения доказательств при расследовании уголовных дел.

Литература

1. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» // СПС «КонсультантПлюс».
2. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс».

3. Савченко М.М. Правовая природа безналичных и электронных денег как предмета преступных посягательств // Бизнес. Образование. Право, 2021, май № 2(55), С. 118-124.
4. Савченко М.М. Проблемы уголовно-правовой защиты безопасности денежных средства физических лиц, размещенных на счетах в банках. // Юридическое образование и наука № 4, 2021, С. 34-40.
5. Сухаренко А.Н., Савченко М.М., Трунцевский Ю.В., Криминальные вызовы пандемии COVID-19 в России: Научно-практическое пособие. Москва: Общество с ограниченной ответственностью «Проспект», 2021. – 336 с.
6. Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс».
7. Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. 2018. № 9. С. 43-47.
8. Яни П. Мошенничество с использованием электронных средств платежа // Законность. 2019. № 5. С. 25 – 28.

Ю.А. Кондратьев

Проблемы использования искусственного интеллекта в сфере противодействия криминальным угрозам обществу

Аннотация. В статье исследуются проблемы, связанные с использованием искусственного интеллекта в деятельности правоохранительных органов по противодействию криминальным угрозам обществу. С учетом того, что в настоящее время существенно расширяются сферы применения искусственного интеллекта, появление которого обусловлено развитием новых информационно-коммуникационных технологий, обосновывается потребность принятия решений по предупреждению возможных негативных проявлений его использования и государственному реагированию на них На основе анализа задач, которые решаются при помощи искусственного интеллекта, автор формулирует проблемы, возникающие в процессе внедрения искусственного интеллекта в деятельность правоохранительных органов и приходит к выводу о необходимости разработки комплекса мер, позволяющих обеспечивать участие искусственного интеллекта в процессах противодействия криминальным угрозам в рамках правового поля и под контролем общества.

Ключевые слова: криминальные угрозы, искусственный интеллект, информационно-коммуникационные технологии.

Использование информатизации и цифровых технологий в правоохранительной сфере способствует более эффективному применению

правовых норм и оптимизации профессиональной деятельности[1]. Целями внедрения и распространения информационно-коммуникационных технологий и информационных систем в правоохранительных органах является уменьшение в их деятельности ошибок, связанных с недостоверной информацией, упрощение системы делопроизводства, повышение оперативности в работе[2]. Для реализации этих целей процесс информатизации предполагает не только увеличение скорости получения и обработки информации, но и освобождение сотрудников от рукописного непроизводительного труда.

Общие тенденции информатизации общественной жизни обусловили формирование и принятие на базе Указа Президента Российской Федерации от 7 Мая 2018 №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[3] национальной программы «Цифровая экономика Российской Федерации»[4], которая должна была быть исполнена до конца 2024 г.

Одним из важнейших продуктов информатизации (цифровизации) является искусственный интеллект, без которого современный мир уже невозможно представить. В отечественной научной литературе проблемы цифровизации и внедрения искусственного интеллекта в исследованиях правового характера обсуждаются достаточно активно[5]. В то же время динамика распространения современных цифровых технологий настолько стремительна, что требует, как постоянного мониторинга, так и своевременного анализа происходящих изменений. При этом цифровая среда по-разному охватывает все сферы жизни общества, модифицирует механизм его развития, по-новому высвечивает интересы личности и их соотношение с функциями и задачами государства[6].

Официальное определение искусственного интеллекта дано в Указе Президента РФ от 10 октября 2019 г. № 490 «Национальная стратегия развития искусственного интеллекта на период до 2030 года», согласно которому искусственный интеллект представляет собой «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при

---

[1] Гайсинский И. Е., Никоненко Н. Д., Перова М. В. Исследование некоторых аспектов повышения эффективности Интернет-сайтов муниципальных образований// Государственное и муниципальное управление: ученые записки СКАГС, 2015, № 4. С. 76.

[2] Паламарчук С.А. Совершенствование конституционно-правового регулирования права на информацию в сети интернет // Северокавказский юридический вестник, 2015, №4. С.108–114.

[3] Указ Президента Российской Федерации от 07.05.2018 №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» (в редакции указов Президента Российской Федерации от 19.07.2018 №444 от 21.07.2020 № 474) //http://www.kremlin.ru/acts/bank/43027(дата обращения: 04.03.2023).

[4] Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru.

[5] См.: Искусственный интеллект в праве: научно-практическое пособие / под ред. Д. А. Пашенцева. М.: Инфотропик Медиа, 2021. — С. 13.

[6] Пороховский А. А. Цифровизация и искусственный интеллект: перспективы и вызовы. Экономика. Налоги. Право. 2020, №13(2). С. 85-86.

выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека»1. Из этого определения следует, что искусственный интеллект образует комплекс технологических решений, включающий в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений. Как отмечают С.А. Антипова О.М. Тляшев, в настоящее время предпринимаются все более настойчивые попытки создания искусственного интеллекта, превосходящего человеческий, на основе машинного обучения и «симбиоза знаний из различных фундаментальных наук с прикладными научными исследованиями и огромными массивами данных».[2]

В последние годы искусственный интеллект все активнее задействуется в сфере противодействия криминальным угрозам обществу, но именно здесь его использование становится не безопасным для человека. С одной стороны, внедрение искусственного интеллекта в систему безопасности страны, позволяет эффективно предотвращать преступления и иные правонарушения, позволяя осуществлять контроль за большим количеством людей одновременно в целях сохранения политической стабильности в государстве. С другой – искусственный интеллект, позволяющий осуществлять тотальный контроль за гражданским обществом, создает угрозу серьезного ущемления приватности, сокращает личное пространство граждан, в итоге, наряду с другими факторами, может привести к серьезным нарушениям прав и свобод человека и гражданина.

На наш взгляд, опасностью, угрожающей человеку, является именно «вездесущность» такой системы. Тотальный контроль за поведением граждан позволяет создать эффект так называемого «большого брата» или «бога», когда человек знает, что за ним наблюдают всегда. Создается ситуация, когда человек начинает вести себя по правилам даже тогда, когда за ним никто не наблюдает. Однако, в данном случае регулирование осуществляется на основе страха наказания, что пагубно влияет на человеческую психику. Возможно, что именно этот аспект подтверждает вывод о том, что внедрение искусственного интеллекта всегда будет иметь и отрицательные последствия.

Следует изначально иметь в виду, что искусственный интеллект не идеальная система. С его помощью не всегда можно точно определить реальную угрозу той сфере общественных отношений, контроль за которой ему доверяется, поэтому велика вероятность неточных прогнозов, а выстроенные на их основе оперативные и стратегические мероприятия могут оказаться вредоносными и причинить существенных вред обществу, как в рамках конкретной страны (или группы стран), так и в глобальном масштабе. Поэтому все программы, в совокупности образующие искусственный интеллект, реализуемые в данной

---

[1] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») — Указ президента // www.pravo.gov.ru. — 2019. — 10 октября.

[2] Антипова С.А., Тляшев О.М. Искусственный интеллект в сфере национальной безопасности: стратегическое противостояние КНР и США // Военная мысль, 2021. № 7. С. 130-140.

сфере, должны подвергаться серьезному общественному контролю и находиться в зоне особого внимания международных организаций.

В заключение можно с уверенностью сказать, что при использовании искусственного интеллекта в противодействии криминальным угрозам решается ряд важнейших задач:

1. Предупреждение преступлений и правонарушений. Например, в идеале определяя признаки того или иного вида криминального поведения, искусственный интеллект позволяет не только выявить преступника и пресечь его деятельность, но и оказать весьма ощутимое профилактическое воздействие.

2. Повышение уровня доверия населения к деятельности органов государственной власти по противодействию криминальным угрозам, существующей системе контроля, а также деятельности государственных органов в целом.

3. Автоматизация системы борьбы с преступностью, позволяющая обеспечить оперативный сбор интересующей информации и обеспечить ее незамедлительную реализацию в целях противодействия различным ее видам.

4. Создание прозрачного механизма в борьбе с криминальными угрозами, позволяющего эффективно противодействовать им, который будет минимально зависеть от человеческого фактора.

5. Интеграция имеющихся государственных ресурсов и возможностей гражданского общества в противодействии криминальным угрозам.

В процессе внедрения искусственного интеллекта в деятельность правоохранительных органов могут возникать серьезные правовые, этические, организационные проблемы, которые необходимо будет решать.

1. Проблема обеспечения безопасности информации при внедрении искусственного интеллекта в систему правоохранительных органов.

2. Проблема получения и конфиденциальной информации и сохранения ее в качестве таковой.

3. Проблема финансирования программ совершенствования искусственного интеллекта.

4. Проблема создания и развития нормативной платформы искусственного интеллекта.

5. Проблема обеспечения разумной, с точки зрения интересов общества, доступности и прозрачности системы.

6. Проблема правового обеспечения ответственности разработчиков искусственного интеллекта.

7. Проблема стандартизации оценки итогов работы искусственного интеллекта.

8. Проблемы технического (технологического) обеспечения внедрения и организации работы искусственного интеллекта.

Литература

1. Антипова С.А., Тляшев О.М. Искусственный интеллект в сфере национальной безопасности: стратегическое противостояние КНР и США // Военная мысль, 2021. №7. С. 130-140.
2. Гайсинский И. Е., Никоненко Н. Д., Перова М. В. Исследование некоторых аспектов повышения эффективности Интернет-сайтов муниципальных образований // Государственное и муниципальное управление: ученые записки СКАГС, 2015, № 4. - С. 75-81.
3. Джиоев С.Х. Правовые и организационные основы применения информационных технологий при осуществлении основных видов деятельности прокуратуры //Аграрное и земельное право, 2022. №% (209). - С.129-136.
4. Искусственный интеллект в праве: научно-практическое пособие / под ред. Д. А. Пашенцева. М.: Инфотропик Медиа, 2021. — 132 с;
5. Паламарчук С.А. Совершенствование конституционно-правового регулирования права на информацию в сети интернет // Северокавказский юридический вестник, 2015, №4. - С.108–114.
6. Пороховский А. А. Цифровизация и искусственный интеллект: перспективы и вызовы. Экономика. Налоги. Право. 2020, №13(2). С. 84-90.

Ю.В. Красненко

Использование специальных знаний как фактор повышения эффективности раскрытия и расследования преступлений, совершенных в киберпространстве

Аннотация. В статье рассмотрены вопросы применения специальных знаний специалистами и следователями-криминалистами при расследовании уголовных дел по преступлениям, связанным с использованием информационно-телекоммуникационных технологий в киберпространстве. Автором обозначены некоторые аспекты деятельности сведущих лиц при работе с компьютерной техникой и электронными доказательствами. Рассмотрены особенности криминалистической деятельности при обнаружении, фиксации и изъятии материальных следов преступлений. Предложены меры, способствующие повышению результативности и эффективности производства следственных действий.

Ключевые слова: специальные знания, криминалистическая деятельность, киберпреступность, специалист, следователь-криминалист.

Одним из приоритетных направлений внутренней политики Российской Федерации в настоящее время выступает развитие информационно-телекоммуникационных технологий, формирование автономного отечественного информационного пространства и создание соответствующей инфраструктуры. Это обусловлено тем, что за последние десятилетия различные

социальные сети, цифровые информационные системы, беспроводной доступ в сеть Интернет и возможность мгновенной передачи значительного массива данных на неограниченное расстояние в любую точку мира, стали повседневными для граждан нашей страны. При поддержке государства были созданы и успешно внедрены в деятельность органов законодательной, исполнительной и судебной власти системы предоставления различных услуг в электронном виде с возможностью дистанционной подготовки и получения необходимых документов.

В свою очередь, стремительная цифровизация различных общественных и государственных институтов, банковского и финансового секторов, в особенности связанная с направлением и использованием копий документов граждан с персональными данными, реквизитами счетов и банковских карт по незащищенным каналам связи, в значительной мере повлияла на изменение структуры экономических преступлений, которая перешла в киберпространство.

Так, согласно официальной статистике МВД России за несколько лет, количество преступлений, связанных с использованием информационно-телекоммуникационных технологий возросло со 174674 в 2018 году до 522065 в 2022 году (+298%)[1]. Данные показатели свидетельствуют о трехкратном увеличении обозначенного вида преступлений и, что характерно, тенденции возрастания их количества в настоящее время остаются неизменными.

Эффективность раскрытия преступлений и расследования уголовных дел, связанных с использованием информационно-телекоммуникационных технологий, обусловлена своевременным и полноценным применением специальных знаний как самими следователями, оперативными работниками, так и, в особенности, специалистами, следователями-криминалистами и судебными экспертами. Тесное взаимодействие сотрудников органов предварительного расследования с представленными участниками уголовного судопроизводства способствует не только надлежащим собиранию, проверке и оценке доказательств, но и более результативной постановке соответствующих задач для их последующего экспертного исследования.

Как верно отмечено Ю.В. Гаврилиным, «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»[2].

Между тем оптимальной формой использования специальных знаний для обнаружения и фиксации цифровых следов преступления в киберпространстве является деятельность специалистов в различных областях науки и техники. Для

[1] Краткая характеристика состояния преступности в Российской Федерации в 2018 г. и 2022 г. [Электронный ресурс]. URL: https://мвд.рф/reports/ (дата обращения: 18.04.2023).

[2] Гаврилин Ю.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [Ю.В. Гаврилин, А.В. Аносов и др.]. М. : Академия управления МВД России, 2019. Ч. 1. С. 133.

получения соответствующей информации целесообразно использовать возможности взаимодействия специалистов в сфере компьютерной техники с экономистами – по уголовным делам финансово-экономической направленности, с лингвистами – по противодействию экстремизму, химиками и биологами – при раскрытии преступлений в сфере незаконного оборота наркотиков и другими сведущими лицами.

Особую роль в противодействии современной высокотехнологичной преступности следует отвести осуществлению криминалистической, в особенности поисково-познавательной, деятельности специалистов, основанной на достижениях уголовно-правовых и естественно-технических наук. Преимущество данного вида деятельности перед производством судебной экспертизы заключается в том, что специалист действует в режиме реального времени вместе с другими субъектами раскрытия и расследования преступлений[1].

Отметим, что при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, достаточно часто требуется привлечение специалиста и следователя-криминалиста для обнаружения, фиксации и изъятия традиционных криминалистических следов, веществ и объектов.

К ним относятся следы пальцев на клавиатуре, компьютерной мыши, принтере и других аппаратных устройствах; микрочастицы биологического и искусственного происхождения (например, частицы крови, волос, одежды, которые попали в клавиатуру); следы обуви и орудия преступления, а также непосредственные электронные носители информации, как объекты материального мира.

Однако, несмотря на то, что данные действия являются одними из самых основных и необходимых, существует ряд проблем, связанных с собиранием рассматриваемых следов, что обусловлено использованием персональных компьютеров, средств сотовой связи, периферийных устройств множеством лиц, часто действующим в составе организованной преступной группы.

В данном случае для повышения результативности получения биологических следов, следов пальцев рук и ладоней, микрообъектов специалистам следует предпринимать следующие действия:

1) ограничить допуск и прикосновения иных участников следственного действия и лиц, находящихся в помещении, к техническим средствам, используемым преступниками, до их предварительного исследования;

2) исключить самостоятельные действия с персональными компьютерами и иными устройствами, в случае возникновения вероятности уничтожения или утраты имеющейся на них цифровой информации;

---

[1] Волынский А.Ф., Прорвич В.А. Актуальные проблемы создания инструментария компьютерной криминалистики по преступлениям в сфере цифровой экономики и финансов // В сборнике: Уголовный процесс и криминалистика: теория, практика, дидактика. Сборник материалов VI Всероссийской научно-практической конференции. Рязань, 2021. С. 71.

3) произвести тщательный осмотр предметов и документов, расположенных на рабочих местах или в непосредственной близости от компьютерной техники и устройств.

Реализация подобных мер позволит не только более подробно и качественно исследовать носители материальных и электронных следов, но и получить необходимую ориентирующую информацию, способствующую раскрытию преступления «по горячим следам».

Кроме того, использование специальных знаний при раскрытии преступлений, совершенных в киберпространстве может быть осуществлено при работе с систематизированными и алгоритмизированными криминалистическими и иными видами учетов.

В частности следует выделить функционирование федеральной базы данных геномной информации и централизованной интегрированной автоматизированной дактилоскопической информационной системы МВД России (ЦИАДИС-МВД), которые содержат существенные массивы цифровых данных криминалистически значимых объектов – ДНК и следов пальцев рук[1].

Таким образом, нами было рассмотрено одно из направлений деятельности правоохранительных органов по раскрытию и расследованию преступлений, совершенных в киберпространстве с использованием информационно-телекоммуникационных технологий. Результативность применения специальных знаний в данной области обусловлена особым характером исследуемых следов, способствующих получению как ориентирующей и разыскной информации, так и формированию доказательственной базы. Применение специальных знаний в данной ситуации связано с использованием достижений не только наук уголовно-правового блока, в особенности криминалистики, но и в сфере информационно-компьютерных технологий, экономики и других направлений научного знания.

Литература

1. Краткая характеристика состояния преступности в Российской Федерации в 2018 г. и 2022 г. [Электронный ресурс]. URL: https://мвд.рф/reports/ (дата обращения: 18.04.2023).
2. Гаврилин Ю.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [Ю.В. Гаврилин, А.В. Аносов и др.]. – М. : Академия управления МВД России, 2019. Ч. 1. 208 с.
3. Волынский А.Ф., Прорвич В.А. Актуальные проблемы создания инструментария компьютерной криминалистики по преступлениям в сфере

[1] Бессонов А.А. Перспективы использования технологии искусственного интеллекта в экспертно-криминалистической деятельности // Судебная экспертиза и исследования. 2022. № 1. С. 19.

цифровой экономики и финансов // В сборнике: Уголовный процесс и криминалистика: теория, практика, дидактика. Сборник материалов VI Всероссийской научно-практической конференции. Рязань, 2021. С. 67-74.
4. Бессонов А.А. Перспективы использования технологии искусственного интеллекта в экспертно-криминалистической деятельности // Судебная экспертиза и исследования. 2022. № 1. С. 16–21.

Е.В. Кунц

Роль ФСИН России в противодействие киберпреступлениям

Аннотация. Активная цифровизация всех сфер человеческой жизни не оставила без внимания и преступность, которая выражается в нарастающей криминализации киберпространства, пространства образованного компьютерными информационно-технологическим и устройствами при их работе. Учреждениям уголовно-исполнительной системы в общей системе противодействия киберпреступлениям отводится значимая роль. В настоящей статье раскрывается роль ФСИН России в противодействии указанному явлению.

Ключевые слова: киберпреступление, осужденный, противодейтвие, уголовно-исполнительная система, учреждение, федеральная служба исполнения наказаний

Содержание понятий «киберпреступлений» или преступлений, совершенных с использованием киберпространства, вышла за пределы главы 28 Уголовного кодекса Российской Федерации (Преступления в сфере компьютерной информации). Указом Президента Российской Федерации от 7 мая 2018 г № 204 определена национальная цель развития Российской Федерации - обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере[1]. Достижение поставленной цели невозможно без соответствующего нормативно-правового обеспечения развивающихся отношений.

Применительно к научному обеспечению противодействия киберпреступелниям, следует отметить, что нарастающий процесс криминализации киберпространства требует уже не изолированных действий и исследований, а разработки единой концепции противодействия данным негативным явлениям уголовно-правовыми, процессуальными, уголовно исполнительными, криминологическими и криминалистическими средствами.

В Генеральной прокуратуре Российской Федерации отдельно выделили проблему, когда к телефонным мошенничествам или кражам через интернет подключаются осужденные, отбывающие наказание в исправительных колониях

[1] Указ Президента Российской Федерации от 07.05.2018 г. № 204 « О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

и СИЗО[1]. Так, в Челябинской области, гражданин, отбывающий наказание в местах лишения свободы, знакомился с женщинами и продавал им несуществующие гаджеты. Потерпевшие перевели мужчине более 1,2 млн. рублей сами[2]/

В этой связи, Федеральная служба исполнения наказаний работает над соответствующей законодательной инициативой, чтобы обязать операторов сотовой связи использовать комплексы подавления сигнала в исправительных учреждениях[3].

В структуре киберпреступлений, совершаемых в местах лишения свободы, преобладают мошенничества (47,88 %; всего - 249 984), кражи (21,75 %; всего - 113 565) и в сфере незаконного оборота наркотиков (11,92 %; всего - 62 209). Прирост числа рассматриваемых преступлений в два и более раз зафиксирован по преступлениям, связанным с незаконным оборотом оружия (+196,0 %: всего - 74) и неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации (+226,4 %; всего - 519), а также фактам содействия террористической деятельности (всего - 251) и заведомо ложных сообщений об акте терроризма (всего - 21 424)[4].

Повлиять на противодействие киберпреступлениям способны такие факторы, как практика применения изменений, внесенных в Федеральный закон «О связи», направленных на пресечение хищений с использованием сокрытия или подмены номера абонента[5], а также разработка и внедрение механизмов противодействия противоправному поведению сотрудников банков при оформлении кредитов, связанному с ситуациями, когда полученные денежные средства незамедлительно переводятся третьей стороне и введение ответственности для лиц, открывающих банковские счета на свое имя за вознаграждение в пользу третьих лиц, выявление и наказание сотрудников УИС, позволяющих сотовую связь осужденным и заключенным в СИЗО.

Прогнозируется снижение числа зарегистрированных киберпреступлений в уголовно-исполнитеьной системе, что вполне обусловлено, созданием дополнительных законодательных барьеров для совершения киберпреступлений, повышением уровня взаимодействия компетентных органов, профессиональной подготовки и технического оснащения субъектов противодействия таким преступлениям.

---

[1] Генпрокуратура подготовила меры по борьбе с киберпреступностью в России. URL:https://tass.ru/obschestvo/9032391?ysclid=lhhhtan2a5199232743&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru(дата обращения: 15.04.2023).

[2] Магнитогорский заключенный продал женщинам несуществующие гаджеты на 1,2 млн. рублей. URL: https://ura.news/news/1052639967(дата обращения: 10.05.2023).

[3] В Волгоградской области снизилось число киберпреступлений. URL: https://rg.ru/2021/06/08/reg-ufo/v-volgogradskoj-oblasti-snizilos-chislo-kiberprestuplenij.html(дата обращения: 10.05.2023).

[4] Состояние преступности в России за январь – декабрь 2022 года. Москва. URL: file:///C:/Users/User/Downloads/Sbornik_22_12-5.pdf(дата обращения: 10.05.2023).

[5] Федеральный закон от 07.07. 2003 г. № 126-ФЗ (ред. от 14 июля 2022) // СЗ РФ. 2003. № 28. Ст. 2895.

Литература

1. В Волгоградской области снизилось число киберпреступлений. URL: https://rg.ru/2021/06/08/reg-ufo/v-volgogradskoj-oblasti-snizilos-chislo-kiberprestuplenij.html(дата обращения: 10.05.2023).
2. Генпрокуратура подготовила меры по борьбе с киберпреступностью в России. URL:https://tass.ru/obschestvo/9032391?ysclid=lhhhtan2a5199232743&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru(дата обращения: 15.04.2023).
3. Курганский осужденный сломал видеонаблюдение в камере. URL: https://ura.news/news/1052492847(дата обращения: 10.05.2023).
4. Магнитогорский заключенный продал женщинам несуществующие гаджеты на 1,2 млн. рублей. URL: https://ura.news/news/1052639967(дата обращения: 10.05.2023).
5. Состояние преступности в России за январь – декабрь 2022 года. Москва. URL: file:///C:/Users/User/Downloads/Sbornik_22_12-5.pdf(дата обращения: 10.05.2023).
6. Указ Президента Российской Федерации от 07.05.2018 г. № 204 « О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». URL: http://www.kremlin.ru/acts/bank/43027(дата обращения: 08.05.2023)
7. Федеральный закон от 07.07. 2003 г. № 126-ФЗ (ред. от 14 июля 2022) // СЗ РФ. 2003. № 28. Ст. 2895.
8. ФСИН собралась привлекать осужденных ИТ-шников к работе по специальности. URL: https://www.cnews.ru/news/top/2022-04-27_fsin_sobralas_privlekat(дата обращения: 18.04.2023).

А.А. Лебедева

OSINT– законность использования для целей расследования преступлений

Аннотация. Технологией ОСИНТа называют сбор публично доступной компьютерной информации для последующего анализа в целях противодействия противоправным деяниям. Поиск интересующей информации производится через общедоступные информационные ресурсы сети Интернет. В статье рассмотрены правовые основы применения ОСИНТа для целей расследования преступления.

Ключевые слова: инструменты ОСИНТа, расследование преступлений, поиск информации о событии преступления.

Технологией ОСИНТа называют сбор публично доступной информации для последующего анализа.[1] Инструменты ОСИНТа условно подразделяются на несколько категорий: поисковые машины, системы (самые главные — это Google, Yandex, Shodan и др., в меньшей степени, Rambler); алгоритмы поиска по словам/фразам; гиперссылки; открытые базы данных; онлайн-сервисы по типу баз данных; социальные сети; люди.

Источниками информации для OSINT могут служить открытые данные, которые можно найти в Интернете.

Сбор информации в рамках ОСИНТа подразумевает использование как пассивных , так и активных методов поиска. К пассивным относятся любые методы, которые не предполагают взаимодействия лица, осуществляющего поиск информации с целевыми системами и не подлежат автоматическому обнаружению. Так, при активном сборе данных аналитик (лицо, осуществляющее поиск информации) использует продвинутые техники и прочие методы, т.е. способы, предполагающие взаимодействие с целевыми системами (осуществляет регистрацию на ресурсе в сети Интернет с целью получения данных, доступных только зарегистрированным пользователям).

Направления использования ОСИНТ для целей расследования: сбор характеризующих данных о лице, организации; их локация; поиск информации, имеющей отношение к преступлению; поиск информации в теневом сегменте интернета с целью раскрытия преступлений и предотвращения новых и многие другие.

Принципы использования ОСИНТа для целей расследования преступления:

1. З*аконность*. Инструменты ОСИНТа в отличии от промышленного шпионажа и иной незаконной деятельности должны использоваться для обработки данных, размещенных в сети Интернет без нарушения закона.

1.1. Интернет ресурсы, использующие данные, полученные незаконным путем, не могут быть отнесены к инструментам ОСИНТ.

Так, 01.07 2021 года 1 июля в Таганском районном суде г. Москвы состоялось заседание по исковому заявлению Роскомнадзора в отношении владельца telegram-бота «Глаз Бога». Суд признал деятельность сервиса незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну. Распространение информации, полученной посредством Telegram-бота, признано незаконным.[2]

1.2. Для целей получения информации инструменты ОСИНТа не могут использовать закрытые (секретные базы данных).

Так, в апреле 2023 года сотрудниками ФСБ и ГУСБ МВД России произведены задержания лиц, подозреваемых в государственной измене. По версии следствия пятеро сотрудников органов внутренних дел за денежное вознаграждение, путем использования чужих паролей и доступа к закрытым базам данных,

[1] См.: Иванов В.Ю. Использование OSINT в раскрытии и расследовании преступлений// Вестник Уральского юридического института МВД России № 1 (37), 2023. С. 62.

[2] URL //https://rkn.gov.ru/news/rsoc/news73728.htm (дата обращения 26.04.2023).

предоставляли личные данные сотрудников правоохранительных органов, прокуроров, судей - заказчикам, среди которых были граждане Украины.[1]

2. *Этичность.* Этические вопросы использования инструментов ОСИНТа для целей расследования следует рассматривать не только с позиции уголовно-процессуального законодательства, но и Конституции РФ, Всеобщей декларации прав и свобод человека, других международных пактов о правах человека.

Рассмотрим, на сколько легитимно использовать функционал ОСИНТа для целей раскрытия и расследования преступлений.

1. Информация, полученная при помощи инструментов ОСИНТа должна обладать определенными свойствами – быть общедоступной, состоять и открытых данных.

1.1. На правомерность обработки информации из общедоступных источников прямо указывают ч. 4 ст. 29 Конституции Российской Федерации[2], п. 2 ст. 5 Федерального закона № 149-ФЗ (общедоступная информация)[3], иные федеральные законы. В ч. 1 ст. 7 Закона об информации[4] упоминается «*общедоступная информация*», под которой понимаются *«общеизвестные сведения и иная информация, доступ к которой не ограничен»*. [5]

Частным случаем изложенного правила является закрепленное в абз. 2 п. 1 ст. 152.2 ГК РФ положение, согласно которому в ситуации, когда информация о частной жизни гражданина ранее стала *общедоступной* либо была *раскрыта самим гражданином или по его воле*, не будет признаваться нарушением сбор, хранение, распространение и иное использование такой информации без согласия этого гражданина.[6] Таким образом, размещение информации в открытом доступе в сети Интернет *автоматически переводит ее в разряд общедоступной*. И как следствие: такая информация подпадает под соответствующие положения Закона об информации, а в части ее распространения – под специальное законодательство.

---

[1] ТАСС: в УВД по ЦАО Москвы проходят массовые проверки из-за утечки данных силовиков//URL https://www.bfm.ru/news/523630 (дата обращения 26.04.2023).

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС "КонсультантПлюс".

[3] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.03.2023).

[4] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.03.2023)

[5] Рожкова М.А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // Закон.ру. 2021. 13 января. URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye

[6] В данном случае федеральное законодательство закрепляет правило о допустимости распространения обозначенной общедоступной информации без согласия субъекта данных.

Так, применительно к персональным данным в контексте п. 2 ст. 7 Закона об информации можно говорить о том, что, как и любая иная информация, *ставшие общедоступными персональные данные допускают их свободное использование*, за исключением *распространения* – в отношении распространения продолжает действовать правило ст. 9 Закона о персональных данных об обязательности получения *согласия* субъекта персональных данных. Важно заметить, что такой вывод применим для ситуаций наличия *легального свободного доступа к персональным данным*, а не в случаях, например, утечек персональных данных в результате хакерских атак.

1.2. Информация, размещаемая ее обладателями в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.[1]

Открытые данные - информация, размещенная в сети Интернет в виде систематизированных данных, организованных в формате, обеспечивающем ее автоматическую обработку без предварительного изменения человеком, в целях неоднократного, свободного и бесплатного использования..."[2].

Набор открытых данных - систематизированная совокупность однотипных данных, представленных в форме открытых данных, состоящая из отдельных элементов, характеризующихся набором атрибутов, и позволяющая автоматизированным системам без участия человека идентифицировать, интерпретировать и обрабатывать такие элементы.."[3]

Таким образом «общедоступная информация, размещаемая в форме открытых данных», полученная путем использования ОСИНта, является разновидностью общедоступных данных, которую из прочих общедоступных данных выделяет то, что она размещена в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования (ч. 4 ст. 7 Закона об информации). Важно заметить, что на эти данные распространяется общий

[1] Рожкова М.А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // Закон.ру. 2021. 13 января. URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye

[2] "Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных. Версия 3.0"(утв. протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 № 4).

[3] Приказ Минпросвещения России от 12.09.2019 № 488 "Об организации работы с открытыми данными в Министерстве просвещения Российской Федерации" (вместе с "Регламентом организации работы с открытыми данными в Министерстве просвещения Российской Федерации", "Ведомственным планом Министерства просвещения Российской Федерации по реализации в 2019 - 2020 годах мероприятий в области открытых данных").

режим общедоступной информации (с некоторыми уточнениями, предусмотренными в ч. 5 и 6 ст. 7 Закона об информации)[1].

2.Следователь может использовать инструменты ОСИНТа в целях раскрытия и расследования преступления.

2.1. В соответствии со ст. 38 УПК РФ следователь - должностное лицом, уполномоченное в пределах компетенции самостоятельно направлять ход расследования, принимать решение о производстве следственных и иных процессуальных действий; давать органу дознания в случаях и порядке, установленных УПК РФ, обязательные для исполнения письменные поручения о проведении оперативно-розыскных мероприятий и др.

Согласно ст. 73 УПК РФ к обстоятельствам, подлежащим доказыванию по уголовному делу в числе прочих относят: событие преступления (время, место, способ и другие обстоятельства совершения преступления); обстоятельства, характеризующие личность обвиняемого.

На основании ч. 1 ст. 6. Федерального закона 27.07.2006 г. № 152-ФЗ «О персональных данных»[2] согласия субъекта персональных данных не требуется, когда обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, *уголовном судопроизводстве*, судопроизводстве в арбитражных судах.

Таким образом следователь лично, либо посредством направления письменного поручение правомочен использовать инструменты ОСИНТа для целей расследования преступления.

Следует отметить, что функционал судьи по применению инструментов ОСИНТа уже регламентирован.

Суд вправе самостоятельно получать необходимые для рассмотрения и разрешения административного дела сведения из открытых источников, в том числе из информационных систем, доступ к которым обеспечивается на официальных сайтах органов государственной власти, органов местного самоуправления в информационно-телекоммуникационной сети "Интернет".

О получении судом сведений данным способом судья (председательствующий в судебном заседании) объявляет сторонам. Полученные сведения приобщаются к материалам административного дела в зависимости от их формы в качестве письменных доказательств, аудио- или видеозаписей. При этом лица, участвующие в деле, вправе приводить свои доводы и представлять доказательства относительно достоверности таких сведений[3].

---

[1] Открытые данные: правовые основы. Мировые законодательные инициативы и ситуация в России // URL: https://data.gov.ru/otkrytye-dannye-pravovye-osnovy-mirovye-zakonodatelnye-iniciativy-i-situaciya-v-rossii).

[2] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) "О персональных данных" (с изм. и доп., вступ. в силу с 01.03.2023) // "Российская газета", № 165, 29.07.2006.

[3] Постановление Пленума Верховного Суда РФ от 15.11.2022 № 34 "О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта федерального закона "О внесении изменений в Кодекс административного судопроизводства Российской Федерации".

Вывод: ОСИНТ – это технологии сбора и анализа информации из открытых источников (сети Интернет), проводимый в рамках закона и с соблюдением этических норм, которая может быть использована органами предварительного следствия и дознания для целей раскрытия и расследования преступлений.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС "КонсультантПлюс".
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.03.2023).
3. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) "О персональных данных" (с изм. и доп., вступ. в силу с 01.03.2023)// "Российская газета", № 165, 29.07.2006.
4. Постановление Пленума Верховного Суда РФ от 15.11.2022 № 34 "О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта федерального закона "О внесении изменений в Кодекс административного судопроизводства Российской Федерации".
5. Приказ Минпросвещения России от 12.09.2019 № 488 "Об организации работы с открытыми данными в Министерстве просвещения Российской Федерации" (вместе с "Регламентом организации работы с открытыми данными в Министерстве просвещения Российской Федерации", "Ведомственным планом Министерства просвещения Российской Федерации по реализации в 2019 - 2020 годах мероприятий в области открытых данных").
6. Методические рекомендации по публикации открытых данных государственными органами и органами местного самоуправления, а также технические требования к публикации открытых данных. Версия 3.0(утв. протоколом заседания Правительственной комиссии по координации деятельности Открытого Правительства от 29.05.2014 № 4). URL //https://rkn.gov.ru/news/rsoc/news73728.htm(дата обращения 26.04.2023).
7. Иванов В.Ю. Использование OSINT в раскрытии и расследовании преступлений// Вестник Уральского юридического института МВД России № 1 (37), 2023. С. 62
8. Открытые данные: правовые основы. Мировые законодательные инициативы и ситуация в России // URL: https://data.gov.ru/otkrytye-dannye-pravovye-osnovy-mirovye-zakonodatelnye-iniciativy-i-situaciya-v-rossii).
9. Рожкова М.А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс]// Закон.ру. 2021. 13 января. URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye

10. ТАСС: в УВД по ЦАО Москвы проходят массовые проверки из-за утечки данных силовиков//URL https://www.bfm.ru/news/523630 (дата обращения 26.04.2023).

П.А. Литвишко

О российских инициативах по противодействию противоправному сбору доказательств в киберпространстве представителями иностранных государств и международных органов

Аннотация. В статье освещены международно-правовые аспекты и текущие отечественные инициативы по противодействию иностранной и международной нелегитимной деятельности правоохранительного и судебного характера в информационном пространстве: путем включения специальных норм в межправительственные соглашения о сотрудничестве в области обеспечения международной информационной безопасности и в разрабатываемый в рамках ООН проект всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях; введения в УК РФ статьи о незаконном осуществлении следственных, иных процессуальных действий и оперативно-розыскных мероприятий на территории Российской Федерации; имплементации в УПК РФ международно-правовых норм о консульской правовой помощи по уголовным делам посредством видеоконференции; урегулирования в законодательстве вопросов сохранения электронных доказательств свыше установленных законом сроков; совершенствования практики взаимодействия российских правоохранительных и судебных органов с «приземленными» иностранными провайдерами.

Ключевые слова: международная информационная безопасность, электронные доказательства, цифровой суверенитет, государственные акторы, видеоконференция, консульская правовая помощь.

Наряду с межгосударственным сотрудничеством в борьбе с киберпреступностью, одна из первостепенных составляющих международной и национальной информационной безопасности – противодействие как вредоносной активности против информационных систем, сетей и данных, исходящей от государственных акторов и спонсируемых (поддерживаемых) государствами киберпреступников, так и другим видам деятельности иностранных должностных лиц или действующих в их интересах частных лиц в киберпространстве, которые так или иначе связаны с вмешательством во внутренние дела государства, в том числе путем криминализации подобных действий и обеспечения эффективного уголовного преследования за их совершение.

Как известно, киберпространство включает в себя ряд уровней (слоев), центральный из которых составляет логический (виртуальный, цифровой) уровень, не имеющий материальных, географических границ. В то же время физический, технологический субстрат (носитель) киберпространства образует

ИКТ-инфраструктура (аппаратно-программное обеспечение), географически локализированная в пределах отдельных государств, включающая в себя в том числе оборудование пользователей (которые, в свою очередь, образуют социальный слой) и имеющих конкретную национальность провайдеров ИКТ-услуг и иных кастодианов данных.

Так, на глобальном международном уровне признается, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета (такие как невмешательство во внутренние дела других государств), применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях[1]. Поэтому страны, как правило, склонны расценивать дистанционные действия представителей иностранного государства, осуществляемые с его территории и физически достигающие лиц (объекты), заведомо находящихся (расположенные) в указанных странах, в качестве предпринимаемых в пределах их собственной территории; к таким действиям относятся трансграничные контакты по сетям любой связи с лицами, заведомо находящимися и использующими оконечное оборудование на территории соответствующей страны. (Тем самым применяется юридическая фикция «территориализации» киберпространства[2].) В случае таких действий без ведома ее властей они могут расцениваться как нарушающие международно-правовые принципы суверенного равенства государств, невмешательства во внутренние дела другого государства, образовывать преступление или иное правонарушение либо международно-противоправное деяние[3].

Из международных договоров, регулирующих следственные и судебные действия по трансграничному получению показаний посредством видеоконференции и телефонной конференции, заявлений и оговорок стран-участниц к ним, международно-правовых принципов суверенного равенства государств и невмешательства во внутренние дела другого государства следует

---

[1] Резолюция Генеральной ассамблеи ООН 73/27 от 05.12.2018 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»; Зиновьева Е., Шитьков С. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38–51.

[2] Терентьева Л.В. Разграничение экстратерриториальной и территориальной юрисдикции в киберпространстве // Право и цифровая экономика. 2022. № 1(15). С. 41–51.

[3] В соответствии с Основами государственной политики Российской Федерации в области международной информационной безопасности, утвержденными Указом Президента РФ от 12.04.2021 № 213 (п. 8), использование ИКТ для вмешательства во внутренние дела суверенных государств является одной из основных угроз международной информационной безопасности.

В соответствии с обновленной Концепцией внешней политики Российской Федерации, утвержденной Указом Президента РФ от 31.03.2023 № 229 (п. 15, 17, 18, 30), в целях обеспечения международной информационной безопасности, укрепления российского суверенитета в глобальном информационном пространстве Российская Федерация намерена уделять приоритетное внимание в том числе принятию мер, направленных на противодействие политике недружественных государств по использованию ИКТ для вмешательства во внутренние дела государств.

запрет на проведение данных действий, если страна, на чьей территории находится их участник (допрашиваемый, опознающий, опознаваемый и др.), не разрешает эти действия, даже в случаях наличия просьбы или согласия самого участника и отсутствия необходимости в услугах действующего в этой же стране «посредника» (ее должностного лица, консула представляемого государства, адвоката, нотариуса либо другого уполномоченного частного лица (commissioner)), традиционно выполняющего функции по удостоверению личности участника, факта добровольности его участия и иных условий.

Показательным с точки зрения различной оценки затронутыми государствами правомерности трансграничных обысков и выемок данных в информационных системах и сетях[1] является известное уголовное дело начала 2000-х годов США против российских хакеров А. Иванова и В. Горшкова, которых американские агенты путем проведения легендированного мероприятия в Интернете выманили из России в США, где в рамках оперативного эксперимента от них получили средства доступа к их российским информационным ресурсам; затем в отношении данных ресурсов в одностороннем порядке провели трансграничные обыск и выемку. Иванов и Горшков были осуждены в США, а российскими следственными органами в отношении американского агента, проводившего названные обыск и выемку, возбуждено уголовное дело о неправомерном доступе к компьютерной информации, совершенном лицом с использованием своего служебного положения[2].

По нашему мнению, подобные противоправные действия могут квалифицироваться как имеющие территориальный характер по ст. 11 УК РФ (по основанию физического местонахождения информационных ресурсов на территории РФ (на компьютере, сервере и т.д.)), так и экстратерриториальный характер по ст. 12 УК РФ (по основаниям гражданства потерпевшего, направленности деяния против интересов государства)[3].

Текущая геополитическая обстановка, системные недружественные действия правоохранительного и судебного характера в отношении нашего государства, предпринимаемые странами «коллективного Запада» и рядом международных органов и организаций, сокращение либо отсутствие возможностей взаимного

---

[1] Подробнее, в т.ч. об инструментах Совета Европы и проводимой в его рамках работе по данной тематике, см.: Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы: монография / под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2022. С. 63–85.

[2] Ст. 272 (неправомерный доступ к компьютерной информации, совершенный лицом с использованием своего служебного положения), 273 (использование вредоносных компьютерных программ, совершенное лицом с использованием своего служебного положения) УК РФ.

[3] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M.N. Schmitt, L. Vihul. Cambridge: Cambridge University Press, 2017. P. 11–29, 51–78.

Об определении американскими судами юрисдикции по месту возникновения вреда от совершенных за рубежом преступлений и экстратерриториального действия уголовного закона США в части соответствующих составов преступлений см.: Buresh D.L. The Computer Crimes of Vasiliy Gorshkov and Alexey Ivanov // Journal of Advanced Forensic Sciences. 2022. Vol. 1. Issue 2. P. 27–32.

антикриминального сотрудничества, привели к осознанию высокой актуальности и существенно ускорили выработку нормотворческих инициатив по защите Россией своего географического и информационного суверенного пространства от таких действий[1], в том числе с использованием опыта тех же западных стран[2].

1. Для предупреждения рассматриваемых ситуаций Российской Федерацией, начиная с 2022 г., в заключаемые двусторонние межправительственные соглашения о сотрудничестве в области обеспечения международной информационной безопасности вносится соответствующая норма. Так, в соответствии с Соглашением между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 24.06.2022 (ст. 2) «не допускается трансграничный доступ к компьютерной информации, хранящейся в информационной системе одного из государств Сторон, без официального взаимодействия с соответствующими компетентными органами государств Сторон; такое взаимодействие может осуществляться, в частности, в рамках двусторонних и многосторонних международных договоров, в том числе о правовой помощи по уголовным делам, а также в рамках международного сотрудничества правоохранительных органов».

2. В целях предотвращения односторонних трансграничных негласных оперативно-разыскных мероприятий в киберпространстве путем установления четких требований об обращении с международным запросом о правовой помощи или правоохранительном содействии для их проведения, а также к содержанию такого запроса по инициативе Генеральной прокуратуры РФ Российской Федерацией в разрабатываемый в рамках ООН проект всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях внесена соответствующая статья[3], призванная обеспечить детальное и самодостаточное

---

[1] Литвишко П.А. Процесс политизации деятельности международных судебных и следственных органов при рассмотрении ими дел в отношении Российской Федерации // Право в Вооруженных Силах – Военно-правовое обозрение. 2022. № 12(305). С. 137–143.

[2] Подробнее см.: Сборник материалов по международному сотрудничеству Следственного комитета Российской Федерации. М., 2015. С. 184–213.

[3] «Статья 78. Специальные методы расследования

1. В целях эффективной борьбы с преступлениями, охватываемыми настоящей Конвенцией, выявления и отслеживания средств и доходов от таких преступлений либо имущества, стоимость которого соответствует таким доходам, каждое Государство-участник, в пределах, допускаемых основополагающими принципами его внутренней правовой системы, и на условиях, установленных его внутренним законодательством, принимает необходимые меры, с тем чтобы разрешить использование негласных специальных методов расследования, таких как электронное или иные формы наблюдения, онлайн-операции под прикрытием или расширенный обыск его компетентными органами на его территории или на территории, находящейся под его юрисдикцией, а также обеспечивать, чтобы доказательства, полученные в результате применения таких мер, являлись допустимыми для целей судопроизводства.

2. При наличии разумных оснований полагать, что серьёзное преступление, охватываемое настоящей Конвенцией, совершено, совершается или с большой долей вероятности может быть совершено, Государство-участник, в пределах своих возможностей и на условиях,

регулирование применения негласных специальных методов расследования по сравнению с несамоисполнимым режимом, предусмотренным в Конвенциях ООН против транснациональной организованной преступности 2000 г. и против коррупции 2003 г. (ст. 20 и 50 соответственно). Российской Федерацией при этом указано на необходимость предотвращения – за счет положений этой статьи – односторонних трансграничных тайных кибероперациий государств-участников, нацеленных на обход двусторонней координации, создающих риск «дружественного огня» в отношении взаимной агентурной деятельности и противоречащих международному праву[1].

3. В целях противодействия принятию иностранными и международными органами односторонних мер по нелегитимному самостоятельному сбору доказательств, включая электронные, и иных сведений в Российской Федерации, в том числе посредством дистанционных трансграничных контактов из-за рубежа с физическими и юридическими лицами, находящимися на территории Российской Федерации, проведению мероприятий по выманиванию таким путем российских граждан за рубеж в целях их задержания Генеральной прокуратурой РФ с учетом зарубежного опыта разработан проект «блокирующего»

установленных его внутренним законодательством, по запросу другого Государства-участника о правовой помощи или правоохранительном содействии, а в случае необходимости – совместно с компетентными органами этого другого Государства-участника, использует негласные специальные методы расследования, такие как электронное или иные формы наблюдения, онлайн-операции под прикрытием или расширенный обыск, осуществляемые компетентными органами Государства-участника на его территории или на территории, находящейся под его юрисдикцией, и предоставляет доказательства, полученные в результате применения таких мер, запрашивающему Государству-участнику.

3. В запросе, направляемом в соответствии с пунктом 2 настоящей статьи, указываются:

(a) Данные о физических, юридических лицах, местонахождении или устройствах, средствах, доходах или имуществе, являющихся целью запрашиваемой меры;

(b) Данные об идентификаторах доступа в сеть, оборудования или сервиса, являющихся целью запрашиваемой меры;

(c) Где данное физическое, юридическое лицо (лица) или оборудование, средства, доходы или имущество находятся или предположительно находятся на территории запрашиваемого государства, или где находится либо учреждён, либо посредством осуществления деятельности по обработке данных иным образом действует с территории запрашиваемого государства любой соответствующий поставщик услуг;

(d) Вид негласного специального метода расследования, для осуществления которого запрашивается помощь, а также лица, поставщики услуг или организации, содействие которых может потребоваться для его осуществления;

(e) Срок, на который запрашивается помощь;

(f) Характер данных или информации, которые ожидается получить, и в особенности их связь с серьёзным преступлением, расследуемым в запрашивающем государстве, а также данные, подтверждающие обоснованность преследования».

[1] Заявление делегации Российской Федерации на пятой сессии Спецкомитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (Вена, 11–21 апреля 2023 года). URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (дата обращения: 14.04.2023).

федерального закона, который в апреле 2023 г. направлен ею в Государственную Думу Федерального Собрания РФ[1].

Объекты и предметы деяний, предусмотренных проектируемой ст. 294[1] и ст. 276 УК РФ, направленной в основном на противодействие разведывательной деятельности специальных служб иностранных государств, существенно различаются. Состав преступления, предусмотренный проектируемой ст. 294[1] УК РФ, образует общественно опасное нарушение порядка взаимодействия правоохранительных и судебных органов, конкретизированного в международном договоре и (или) законодательстве РФ (УПК РФ и Федеральном законе от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»), при проведении соответствующих действий и мероприятий на территории Российской Федерации в целях, противоречащих интересам Российской Федерации; цель причинения ущерба государственной безопасности при этом может не преследоваться. Объектами ст. 294[1] УК РФ являются общественные отношения по ограждению интересов Российской Федерации от вмешательства в ее внутренние дела в сфере осуществления правосудия и досудебного производства, нарушения порядка межгосударственного взаимодействия в данной сфере, территориального суверенитета как составляющей основ конституционного строя Российской Федерации. Субъектами преступления, предусмотренного проектом, являются соответствующие должностные лица независимо от их гражданства.

Названные в статье интересы Российской Федерации в основном отражены в документах стратегического планирования, таких как утвержденные указами Президента РФ Стратегия национальной безопасности РФ, Доктрина информационной безопасности РФ, Основы государственной политики РФ в области международной информационной безопасности, Концепция внешней политики РФ.

В то же время оказание гражданами РФ содействия в связи с осуществлением действий, названных в проектируемой ст. 294[1] УК РФ, такого как передача, в том числе с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), или собирание для передачи информации, охватывается ст. 275 и 275[1] УК РФ.

---

[1] «Статья 294[1]. Незаконное осуществление следственных, иных процессуальных действий и оперативно-розыскных мероприятий на территории Российской Федерации

Проведение иностранным должностным лицом либо должностным лицом публичной международной организации (международного органа), в которой не участвует Российская Федерация, следственного или иного процессуального действия, а равно оперативно-розыскного мероприятия на территории Российской Федерации в интересах иностранного государства, публичной международной организации (международного органа), в которой не участвует Российская Федерация, в том числе путем использования систем видео-конференц-связи или других средств связи с лицом, находящимся на территории Российской Федерации, в нарушение порядка взаимодействия с иностранными и международными правоохранительными и судебными органами, предусмотренного международным договором и (или) законодательством Российской Федерации, и в целях, противоречащих интересам Российской Федерации, –

наказывается лишением свободы на срок до пяти лет».

Законодательство зарубежных стран, использованное при формировании законопроекта, содержит раздельную криминализацию шпионажа и не связанной с ним несанкционированной деятельности представителей иностранных властей на территории данных стран.

Что касается ст. 286 (превышение должностных полномочий) УК РФ, то объем этих полномочий и факт их превышения иностранным должностным лицом по общему правилу определяются государством этого должностного лица, которое может также заявить об иммунитете своего должностного лица от иностранной уголовной юрисдикции[1].

Используемые в проектируемой ст. 294[1] УК РФ понятия «иностранное должностное лицо», «должностное лицо публичной международной организации (международного органа)» аналогичны по содержанию изложенным в примечании к ст. 290 УК РФ, в которое вносится соответствующее дополнение.

Производство предварительного следствия по уголовным делам о преступлении, предусмотренном проектом, предлагается отнести к компетенции Следственного комитета РФ, в связи с чем вносится дополнение в подп. «а» п. 1 ч. 2 ст. 151 УПК РФ.

В случае принятия закона он будет криминализировать в том числе неприемлемые для России действия, аналогичные предусмотренным п. «b» ст. 32 Будапештской конвенции о киберпреступности 2001 г. (Россия в ней из-за наличия данного положения не участвует).

Такие нормы служат также дополнительным средством оспаривания допустимости доказательств, полученных указанным в них способом. Вместе с тем вести речь об автоматическом подрыве допустимости доказательств, собранных подобным противоправным способом, пусть даже содержащим элементы международно-противоправного деяния, не приходится, поскольку допустимость определяет заинтересованный конечный пользователь этих доказательств, особенно если им задействуется институт так называемых защитных норм (Schutznorm), позволяющих сохранить допустимость доказательства в случае нарушения норм международного права при условии ненарушения основополагающих прав подозреваемого или обвиняемого (запрета пыток, прав на защиту, справедливое судебное разбирательство)[2].

4. В России сейчас совершенствуются и другие аспекты легитимизации сохранения и предоставления электронных доказательств как по иностранным, так и российским запросам, направленные на обеспечение своего и чужого суверенитета в информационном пространстве.

---

[1] Подробнее см.: Богуш Г. Подлежат ли иностранные должностные лица ответственности по УК РФ? // Уголовное право. 2010. № 4. С. 12–19; Литвишко П.А. Возбуждение и расследование уголовного дела о преступлении, совершенном должностным лицом иностранного государства // Международное уголовное право и международная юстиция. 2014. № 3. С. 5–8.

[2] Koops B.-J., Goodwin M. Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law // Tilburg Law School Legal Studies Research Paper Series. No. 05/2016. P. 75.

Так, в Государственной Думе Федерального Собрания РФ рассматривается разработанный Генеральной прокуратурой РФ (также с учетом зарубежного опыта) законопроект, направленный на имплементацию в УПК РФ норм международного права о проведении за рубежом допросов, в том числе путем использования систем видео-конференц-связи (вид электронного доказательства), консульскими должностными лицами РФ в дипломатических представительствах и консульских учреждениях РФ[1].

В соответствии с планом работы межведомственной рабочей группы по противодействию информационной преступности на 2023 год, утвержденным заместителем Генерального прокурора РФ 26.12.2022 (п. 6–7), осуществляются:

проработка вопроса о закреплении в законодательстве РФ обязанности операторов связи и организаторов распространения информации в сети «Интернет» обеспечивать сохранение «электронных доказательств» по запросам российских и иностранных компетентных органов, связанным с расследованием или судебным рассмотрением уголовного дела, свыше установленных действующим законом сроков их хранения в случаях истечения этих сроков, а также допустимых сроков обеспечения их сохранности и установлении административной ответственности за нарушение такой обязанности;

подготовка предложений по совершенствованию организации направления и исполнения запросов российских правоохранительных органов о сохранении и предоставлении «электронных доказательств», адресуемых филиалу или представительству иностранного лица, осуществляющего деятельность в сети «Интернет» на территории Российской Федерации, либо российскому юридическому лицу, учрежденному иностранным лицом, осуществляющим деятельность в сети «Интернет» на территории Российской Федерации (то есть так называемым «приземленным» иностранным ИТ-компаниям), на основании ст. 7 Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации».

Реализация перечисленных инициатив позволит существенным образом укрепить цифровой суверенитет России в антикриминальной сфере.

[1] Проект федерального закона № 280226-8 «О внесении изменений в статьи 453 и 456 Уголовно-процессуального кодекса Российской Федерации» (по вопросу о консульской функции по выполнению отдельных процессуальных действий по уголовным делам по запросам компетентных органов представляемого государства); Литвишко П.А. Актуальные направления развития международного взаимодействия в сфере уголовного судопроизводства, оперативно-разыскной деятельности и производства по делам об административных правонарушениях // Актуальные проблемы международного сотрудничества в борьбе с преступностью: Международная научно-практическая конференция, приуроченная к 20-летию образования Московского университета МВД России имени В.Я. Кикотя (25 февраля 2022 г.): сборник научных трудов / [сост. Ю. В. Пузырева]. М.: Московский университет МВД России имени В.Я. Кикотя, 2022. С. 93–101.

Литература

1. Богуш Г. Подлежат ли иностранные должностные лица ответственности по УК РФ? // Уголовное право. 2010. № 4. С. 12–19.
2. Зиновьева Е., Шитьков С. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38–51.
3. Литвишко П.А. Актуальные направления развития международного взаимодействия в сфере уголовного судопроизводства, оперативно-разыскной деятельности и производства по делам об административных правонарушениях // Актуальные проблемы международного сотрудничества в борьбе с преступностью: Международная научно-практическая конференция, приуроченная к 20-летию образования Московского университета МВД России имени В.Я. Кикотя (25 февраля 2022 г.): сборник научных трудов / [сост. Ю. В. Пузырева]. М.: Московский университет МВД России имени В.Я. Кикотя, 2022. С. 93–101.
4. Литвишко П.А. Возбуждение и расследование уголовного дела о преступлении, совершенном должностным лицом иностранного государства // Международное уголовное право и международная юстиция. 2014. № 3. С. 5–8.
5. Литвишко П.А. Процесс политизации деятельности международных судебных и следственных органов при рассмотрении ими дел в отношении Российской Федерации // Право в Вооруженных Силах – Военно-правовое обозрение. 2022. № 12(305). С. 137–143.
6. Сборник материалов по международному сотрудничеству Следственного комитета Российской Федерации. М., 2015. 304 с.
7. Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы: монография / под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2022. 168 с.
8. Терентьева Л.В. Разграничение экстратерриториальной и территориальной юрисдикции в киберпространстве // Право и цифровая экономика. 2022. № 1(15). С. 41–51.
9. Buresh D.L. The Computer Crimes of Vasiliy Gorshkov and Alexey Ivanov // Journal of Advanced Forensic Sciences. 2022. Vol. 1. Issue 2. P. 27–32.
10. Koops B.-J., Goodwin M. Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law // Tilburg Law School Legal Studies Research Paper Series. No. 05/2016. 101 p.
11. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M.N. Schmitt, L. Vihul. Cambridge: Cambridge University Press, 2017. 598 p.

Е.А. Логинов

К вопросу киберпреступности в современном мире: проблемы и перспективы

Аннотация. Высокий уровень киберпреступности, ее высокая общественная опасность, латентность и отсутствие эффективного противодействия со стороны правоохранительных органов, делают актуальной разработку научно обоснованной стратегии и тактики борьбы с киберпреступностью.

В статье на основе анализа действующего уголовного законодательства и судебной практики рассмотрены особенности некоторых элементов криминалистической характеристики киберпреступления для использования в расследовании и предупреждении данных преступлений.

Ключевые слова: киберпреступность, IT-технологии, Интернет, правоохранительные органы, киберпространство, мировое сотрудничество.

За последние десятилетия число киберпреступлений в мире увеличилось во много раз, мотивы и цели киберпреступников меняются с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц[1].

Понятие «киберпреступности» на сегодняшний получило большое распространение в связи с информационно-телекоммуникационным прорывом, произошедшим в XXI в. Киберпреступность – совокупность преступлений, совершаемых в «киберпространстве» с помощью или посредством компьютерных систем или компьютерных сетей. К «киберпреступлению» относится любое преступление, совершенное с применением различных способов и средств создания, обработки, передачи компьютерной информации.

Термин «киберпреступность» также часто употребляется вместе с термином «компьютерная преступность», причем часто синонимично. Стоит отметить, что термин «киберпреступность» более расширенный, чем «компьютерная преступность», так как более точно отражает природу такого явления, как преступность в информационном пространстве[2].

Говоря о киберпреступности, необходимо понимать, что данное явление является следствием мирового распространения IT-технологий, если же сравнивать киберпреступность с другими видами преступной деятельности, то киберпреступность растет гораздо большими темпами. Данная тенденция связано со следующими факторами: постоянное увеличение числа пользователей компьютеров и сети Интернет; высокий уровень профессионализма

---

[1] Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху: монография / О. А. Степанов. - Москва: Издательство Юрайт, 2023. С. 37.

[2]См.: Криминалистика: учебник / Е.А. Логинов, О.Н. Садовников; под ред. профессора Е.А. Логинова. – М.: МГИМО МИД России, 2019. С. 254.

преступников в киберпространстве; интенсивное совершенствование и развитие IT-технологий. Все, что связано с развитием IT- технологий, является почвой для совершения киберпреступлений.

Основными источниками экономических преступлений, совершаемых в киберпространстве являются незаконная предпринимательская и банковская деятельность[1]. Интернет, помимо площадки незаконной деятельности, является местом для легализации денег, полученных преступным путем. Всемирная сеть и образованное ею киберпространство создали единственную среду и уникальные условия для осуществления преступной деятельности (легализация денежных средств, полученных преступным путём, получение быстрого и стабильного дохода). Легализация денежных средств в киберпространстве создаёт трудности в правоприменительной практике, и это, в свою очередь, приводит к необходимости совершенствования законодательства.

В совокупность способов легализации денежных средств, полученных в результате совершения киберпреступления входят: использование социальных сетей, сайты-аукционы, сайты-объявления, помимо данных средств злоумышленник может открывать собственные сайты разной направленности.

С появлением новых технологий наблюдается появление новых, более сложных видов преступности. Это свидетельствует о том, что преступники достаточно оперативно используют результаты научно-технического прогресса в своих целях. Данная тенденция представляет серьёзную угрозу всем общественным отношениям, складывающимся в киберпространстве, поскольку на данном этапе развития киберпространство и общество уже неразрывны. Главными причинами и условиями существования экономической киберпреступности являются анонимность пользователей киберпространства и анонимность информационных сетей, техническое несовершенство, а также низкий уровень информационной безопасности людей[2]. Правоохранительным органам становится известна лишь малая часть совершаемых экономических киберпреступлений.

Как уже было сказано, киберпреступность имеет глобальный характер. К примеру, киберпреступление против определенной компании в определенной стране может быть совершенно с территории другого государства. Поэтому наиболее легким и верным в вычислении является не показатель количества совершенных киберпреступлений, а индекс киберзащищенности. Фрагмент «Глобального индекса кибербезопасности», ежегодно составляемый экспертами ООН, за 2021 год представлен в следующей таблице:

[1]Глотина И.М. Киберпреступность как теневой бизнес // Экономические науки. – 2016. – №6 (388). – С. 54.

[2] Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. - 2-е изд., испр. и доп. - Москва: Издательство Юрайт, 2023. – С. 43.

Место	Страна	Индекс кибербезопасности
1	Великобритания	0.931
2	Соединенные штаты Америки	0.926
3	Франция	0.918
4	Литва	0.908
5	Эстония	0.905
	……..	
26	Россия	0.836

При составлении рейтинга, представленного в таблице, эксперты - составители учитывают пять основных критериев[1]:

1 Юридическая составляющая: наличие правовых систем и структур, занимающихся вопросами кибербезопасности и киберпреступлений.

2 Техническая составляющая: технические возможности в области кибербезопасности.

3 Составляющая организационной подготовленности: существование институтов координации политики и стратегий развития кибербезопасности на государственном уровне.

4 Составляющая образовательного и исследовательского потенциала: наличие научно-исследовательских, образовательных и подготовительных программ, а также сертифицированных специалистов и госучреждений, способствующих наращиванию потенциала в сфере информационной безопасности.

5 Составляющая готовности к сотрудничеству: наличие партнерств, механизмов сотрудничества и систем обмена информацией.

Положение России в рейтинге по кибербезопасности можно обосновать огромным ростом киберпреступлений, зарегистрированных в Российской Федерации. С использованием высоких технологий совершается каждое четвертое преступление[2].

Киберпреступность сегодня наносит огромный ущерб как частным, так и государственным предприятиям, а также увеличивает расходы на IT-безопасность. Мировые расходы на продукты и услуги в области кибербезопасности в 2022 году (расчеты не охватывают различные категории кибербезопасности, включая Интернет вещей, Интернет промышленность) превышают расходы по сравнению с 2021 годом на 12,4%, а в 2023 году прогнозируется рост на 15,7% по сравнению с 2022 годом и достижения отметки расходов в 124 миллиарда долларов США[3].

[1] Global Cybersecurity Index (GCI) 2021. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf (дата обращения 29.03.2023)

[2] https://xn--b1aew.xn--p1ai/reports/item/35396677 (дата обращения 29.03.2023).

[3] Головинов О. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики – 2016. – Т. 6. – №1 – С. 79.

Таким образом, высокая социальная опасность киберпреступности объясняется ее транснациональным и организованным характером, поэтому ни одно государство сегодня не способно активно противодействовать этой угрозе самостоятельно, в связи с чем неотложной является потребность активизации международного сотрудничества. Эффективная борьба с киберпреступностью требует коллективных усилий. Для этого необходимо вести постоянную разъяснительную работу среди населения. Требуется длительный и, что немаловажно, упорный воспитательный процесс для того, чтобы люди осознавали необходимость мер предосторожности. Для того чтобы эффективно противостоять киберпреступности, масштабы которой столь разительно выросли за последние годы, государственным структурам и коммерческим компаниям необходимо рассматривать информационную безопасность в качестве одного из ключевых компонентов своей деятельности. Наиболее приоритетными должны стать вопросы ответственности, соблюдения российского законодательства в области информационной безопасности и повышения уровня культуры безопасности граждан.

Литература

1. Глотина И.М. Киберпреступность как теневой бизнес // Экономические науки. – 2016. – №6 (388). – С. 54.
2. Головинов О. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики – 2016. – Т. 6. – №1 – С. 79.
3. Криминалистика: учебник / Е.А. Логинов, О.Н. Садовников; под ред. профессора Е.А. Логинова. – М.: МГИМО МИД России, 2019. С. 254.
4. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху: монография / О. А. Степанов. - Москва: Издательство Юрайт, 2023. С. 37.
5. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. - 2-е изд., испр. и доп. - Москва: Издательство Юрайт, 2023. – С. 43.
6. Global Cybersecurity Index (GCI) 2021. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_GlobalCybersecurity-Index-EV5_print_2.pdf (дата обращения 29.03.2023).
7. https://xn--b1aew.xn--p1ai/reports/item/35396677 (дата обращения 29.03.2023).

А.Ю. Любавский

О необходимости развития алгоритмического мышления следователей в контексте расследования киберпреступлений

Аннотация. Статья посвящена особенностям и практическому значению формирования алгоритмического мышления следователей. Проведен анализ

применения алгоритмы в работе следователей. Приводятся доводы в пользу необходимости изучения основ алгоритмизации в ходе освоения учебной программы информатика и информационные технологии в профессиональной деятельности.
Ключевые слова: алгоритм, алгоритмизация, следователь, расследование, мышление, киберпреступление.

На сегодняшний день отмечается внедрение информационных технологий практически во все сферы современного общества. Внедрение информационных технологий не обошло стороной и криминальный мир. Одним из негативных последствий информационных технологий является появление и развитие преступлений, совершенных в сфере компьютерной информации (далее – киберпреступление).

Во всем мире растет количество киберпреступлений. По данным Министерства внутренних дел Российской Федерации количество преступлений в России с каждым годом увеличивается[1]

Киберпреступность представляет собой серьезную угрозу для общества[2]Сфера совершения киберпреступлений очень обширна, начиная с хакерских атак на критическую информационную инфраструктуру, заканчивая совершением мошеннических действий, причем материальный ущерб от такого рода преступлений исчисляется как тысячами рублей, так и сотнями тысяч, иными словами жертвами киберпреступников могут стать как рядовые граждане, так и целые государства[3].

Как правило, лица, совершающие киберпреступления являются специалистами в сфере информационных и сетевых технологий [3], имеют высшее, незаконченное высшее, среднее техническое образование в сфере IT-технологий. При совершении хакерских атак киберпреступники используют алгоритмы, и хорошо знают принципы и технологии работы вычислительных сетей[4].

Вышеперечисленные факты свидетельствуют о том, что в деятельности правоохранительных органов одной из первоочередных становится задача, связанная с расследованием новых видов преступлений. Киберпреступления имеют ряд особенностей, отличающий их от совершаемых традиционным способом. К таким особенностям следует отнести: трансграничность; трудности с определением места нахождения преступника, установления его личности и места совершения преступления; сложности с визуальным наблюдением и фиксацией цифровых доказательств и последствий совершенных преступлений[5].

---

[1] URL: https://www.rbc.ru/rbcfreenews/647227219a7947b85a9adf08

[2]URL:https://rg.ru/2022/12/22/za-10-mesiacev-2022-goda-sk-rassledoval-13-tysiach-kiberprestuplenij.html

[3] Бондарь Е.О. Киберпреступность как новая криминальная угроза // Вестник Московского университета МВД России. 2020 – С. 155-158.

[4] URL: https://www.securitylab.ru/news/215317.php

[5] Берова Д.М. Расследование киберпреступлений // Проблемы в российском законодательстве. Юридический журнал. 2018 – С. 123-126.

Ввиду специальных знаний, навыков, а также нередко и образования киберпреступника перед следователем стоит задача раскрыть не только мотивы злоумышленника, но и попросту научится думать, как преступник. Для раскрытия киберпреступления, на наш взгляд, следователю в своей работе необходимо развивать алгоритмическое мышление. Алгоритмы, которые изначально положены в основу программирования, является набором инструкций, описывающих порядок действий для решения определенной задачи. В отличии от математики, в программировании эти действия могут выполняться параллельно, если это не противоречит достижению конечного результата.

Если рассмотреть требования, предъявляемые к следователю то изначально предполагается наличие высшего юридического образования. Для осуществления своей деятельности он должен знать и уметь применять на практике нормы уголовного и уголовно-процессуального законодательства, криминалистику, юридическую психологию, логику и др. Все приведенные знания и навыки можно отнести к сфере гуманитарных наук, поэтому зачастую при подготовке и формировании компетенций обучающихся в данном направлении учебными заведениями не делют упор на такие дисциплины как математика, информатика либо информационные технологии.

Однако, ранее были приведены факты того, что в современном обществе изменился характер совершаемых преступлений[1]. Поэтому при подготовке следователей целесообразно развивать алгоритмическое мышление. Без алгоритмического мышления на сегодняшний день не обходится ни один процесс в современной жизни.

В первую очередь это дает возможность разрабатывать стратегию расследования киберпреступления, выдвигать обоснованные версии и доказывать гипотезы опытным путем, прогнозировать результаты расследования, анализировать и находить рациональные способы решения задачи путем оптимизации, разработанного алгоритма расследования.

Эффективным способом развития алгоритмического мышления является как решение классических математических задач посредством составления алгоритмов, так и разбор существующих ранее разработанных алгоритмов (алгоритмы осмотра места происшествия, предмета (персонального компьютера, смартфона). доказывания, допроса участников судопроизводства, проверки показаний и других следственных действий). Так же следует отметить, что развитие алгоритмического мышления следователей позволяет оптимизировать существующие алгоритмы и адаптировать под конкретную ситуацию. Чем легче обучаемый умеет понимать чужие алгоритмы и строить свои, тем эффективнее сможет раскрывать киберпреступления.

В пользу алгоритмического мышления выступает тот факт, что такой тип мышления отличается формальностью, логичностью, ясностью, что позволяет любую абстрактную идею преобразовать в последовательную инструкцию, которая в конечном итоге позволит достичь конечный результат. Кроме того, такой стиль мышления позволит видеть проблему в целом и разбивать процесс

[1] Долгачев А.О. Понятие и особенности киберпреступности // Научный поиск. 2017 – С. 47-50.

расследование преступления на мелкие подзадачи. Алгоритмический подход к решению задач требует повышения уровня строгости рассуждений и точности обоснований. Также в ходе профессиональной деятельности следователь четко и ясно сможет сформулировать и структурировать объем и состав информации, которая потребуется для завершения расследования.

Таким образом, рассмотрев все факты, приведенные в настоящей статье, можно заключить, что изменившийся характер и способы совершаемых преступлений с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", их криминалистическая характеристика. структура, особенности личности современных киберпреступников приводит к необходимости развития при подготовке будущих следователей развитие такого навыка, как алгоритмическое мышление, которое в совокупности со знанием уголовного и уголовно-процессуального права, криминалистики и других учебных дисциплин, позволит более эффективно проводить расследование преступлений, совершенных в сфере компьютерной информации.

Литература

1. Берова Д.М. Расследование киберпреступлений // Проблемы в российском законодательстве. Юридический журнал. 2018 – С. 123-126.
2. Бондарь Е.О. Киберпреступность как новая криминальная угроза // Вестник Московского университета МВД России. 2020 – С. 155-158.
3. Долгачев А.О. Понятие и особенности киберпреступности // Научный поиск. 2017 – С. 47-50.
4. URL: https://www.rbc.ru/rbcfreenews/647227219a7947b85a9adf08
5. URL:https://rg.ru/2022/12/22/za-10-mesiacev-2022-goda-sk-rassledoval-13-tysiach-kiberprestuplenij.html
6. URL: https://www.securitylab.ru/news/215317.php

Е.С. Лысенко
Е. Ю. Семенов

Отдельные вопросы деанонимизации лиц, совершающих преступления в сети интернет

Аннотация. Для совершения преступлений в сети интернет злоумышленники как правило использует различные средства для того, чтобы оставаться неизвестными – используют средства анонимизации. В статье рассматриваются некоторые подходы к установлению личности лиц, совершающих противоправные действия в сети интернет и применяющих специальные программные, технические и организационные методики для анонимизации.

Ключевые слова: интернет-преступления, подмена ip-адреса, анонимизация в сети интернет, деанонимизация в сети интернет.

Одной из причин большого количества киберпреступлений является то, что множество общественных отношений из сферы реального взаимодействия переходят к взаимодействию посредством киберпространства, в связи с этим и сфера совершения преступлений перемещается сюда же.

Другая причина в том, что злоумышленники не без оснований полагают, что, организуя и совершая преступления посредством информационно-телекоммуникационных технологий можно оставаться неизвестными для правоохранительных органов. Здесь играет роль ситуация анонимности (условной анонимности), наличие которой предполагает лицо, совершающее преступление.

Информационные технологии, предоставляющие возможность оставаться преступникам неизвестным для потенциальных жертв, мотивируют к совершению таких преступлений лиц, которые никогда бы не решились на поиск потенциальных жертв в рамках непосредственного общения. У потенциального преступника пропадает страх, который является сдерживающим фактором от общения с жертвами в реальной жизни в общественных или иных местах, где такое общение и соответственно преступный умысел лица может стать известен третьим лицам.

Совершение преступлений, с использованием информационных технологий часто сопряжено с использованием программного обеспечения позволяющего затруднить или полностью исключить возможность идентефицировать преступников. Как правило применяются такие технологии как VPN, Прокси-серверы, TOR, I2p и т.п.

Соединение посредством VPN позволяет создавать своего рода «туннель» между компьютером пользователя и сервером, посредством которого создается VPN соединение. Вся информация в рамках данного «туннеля» (VPN – соединения) зашифрована.

Основная особенность VPN, являющаяся привлекательной для лиц осуществляющих противоправные действия в том, что VPN-сервисы позволяют менять IP-адрес злоумышленника (предоставленный интернет-провайдером) на свой. По сути устройство, подключенное к сети посредством VPN соединения, выходит в открытую сеть через VPN – сервер и под IP, предоставленный сервисом.

То есть после того, как злоумышленник выходит в сеть интернет и, например, совершает в рамках какого-либо сайта преступные действия (развратные действия, распространение информации), этот конечный интернет-ресурс видит лишь ip-адрес VPN, а не истинный ip-адрес пользователя. Соответственно, в ответе на запрос от администратора данного интернет-сайта правоохранительные органы смогут получить ip-адрес, принадлежащий VPN – сервису, что не даст возможность установить данные злоумышленника и осуществлять дальнейшее расследование.

Одним из недостатков использования VPN сервисов для аноноимизации является возможность внезапного «разрыва» созданного защищенного соединения, что одновременно сопровождается подключением к публичной сети. Правоохранители, отслеживая защищенное соединение в таком случае

могут установить реальные данные отслеживаемого лица. Вместе с тем современные программные средства позволяют защитится от данного негативного фактора VPN соединения. Данные средства контролируют VPN-соединение и в случае его разрыва сначала блокируют передаваемую информацию, закрывают приложения, потом обновляют VPN-подключение[1].

Также следует отметить, что компании, организации предоставляющие услуги VPN соединений используют разные алгоритмы работы. Так виды и степень шифрования трафика у VPN-провайдеров могут отличаться. Отдельные VPN-провайдеры не скрывают сами факты подключения, а также сохраняют логи (справочные технические файлы – журналы). В логах может фиксироваться информация о посещаемых сайтах, реальных IP адресах клиентов и т.п.). Политика компании может предусматривать сотрудничество с правоохранительными органами в рамках обмена указанной информацией.

Указанные особенности VPN – сервисов позволяют правоохранительным органам Российской Федерации в отдельных случаях получать информацию о лицах, осуществляющих преступную деятельность в сети интернет, в том числе путем направления соответствующих запросов.

Простейшим методом, установления реального IP-адреса злоумышленника будет направления запроса VPN-сервису, адрес которого был установлен в результате оперативно-розыскных мероприятий, следственных или иных процессуальных действий.

Если IP-адрес принадлежит провайдеру VPN-сервиса, запрос направляется данному провайдеру с запросом предоставить информацию об IP-адресе злоумышленников, с указанием сайтов, и времени совершения противоправных действий).

Препятствием здесь как правило становиться то, что злоумышленник использует VPN-сервис (и сервер соответственно), который расположен вне юрисдикции Российской Федерации, и, не сотрудничает с правоохранительными органами, направляющими запросы.

Данная ситуация безвыходной на самом деле не является. Расследование может быть успешным с применением так называемого метода сопоставления. Например, злоумышленник совершал развратные действия в социальной сети. Администрация социальной сети предоставила IP преступника, который принадлежит VPN-сервису вне юрисдикции РФ, отказывающемуся сотрудничать с правоохранительными органами. В этот же период злоумышленник мог пользовался и другими интернет-сервисами и услугами: мессенджерами, электронной почтой, сервисами доставки, маркетплейсами, банкингом.

В обзор следует принять самые распространенные. Строить гипотезы о ресурсах, к которым возможно обращался преступник можно на основе анализа переписки преступника с жертвой. Установив примерный перечень ресурсов, которые мог посетить злоумышленник – следует направить запрос в администрации этих ресурсов, о предоставлении информации о том

[1] VPN: ещё раз просто о сложном // [URL: https://habr.com/ru/articles/534250/].

подключались ли к ним в установленное следствие время с IP-адреса VPN-сервиса которым пользовался злоумышленник. Например, в это же время злоумышленник воспользовался своей электронной почтой – соответственно будет зафиксирован вход на определенный аккаунт с искомого IP-адреса (адреса VPN-сервиса). Далее по запросу можно получить информацию о данных из аккаунта электронной почты. Например, запросить все IP-адреса с которых осуществлялось использование данного аккаунта ранее.

Применение данного метода может быть затруднено ввиду ряда факторов. VPN – сервисы, как правило предоставляют пользователю динамические ip-адреса, которые остаются неизменными лишь в рамках одной сессии сетевого подключения. То есть, направляя запросы, на сторонние интернет сайты нужно указывать конкретный временной промежуток использования ip VPN сервиса. Также следует учитывать, что в силу применения различными сервисами и провайдерами NAT-адресации (англ. NAT (Network Address Translation) – протокола преобразования сетевых адресов), один и тот же ip-адрес представляется множеству (до сотен и тысяч) пользователей виртуальной частной сети[1].

Также существует возможность деанонимизации злоумышленников, использующих ресурсы VPN-сервисов путем сопоставления соединений. Использование данного метода построено на гипотезе о том, что преступник для совершения противоправной деятельности подключается к сети интернет, через официально представленного в определенной местности интернет-провайдера («проводной» интернет или «мобильный» интернет). После того как преступник подключился к сети интернет через официального провайдера, он подключается к VPN-сервису, а далее уже совершает противоправные действия предполагая, что для любых внешних контактов IP-адрес его провайдера скрыт за IP-адресом VPN-сервиса. Здесь следует отметить, что провайдеру видно (известно) к каким сервисам, в том числе VPN осуществляют подключение его абоненты. Однако провайдеру неизвестно с какой целью это осуществляется (использование заблокированных ресурсов или противоправная деятельность). В данном случае положительный результат могут принести обращения всем представленным в определенной местности провайдерам сети интернет с запросом о том, подключался ли какой-либо из их абонентов к VPN-сервису с установленным IP-адресом в интересующее следствие время.

Применение данного метода может быть затруднено в связи с тем, что используемый злоумышленником VPN-сервис в силу его популярности также одновременно мог использоваться и большим количеством других лиц. Кроме того злоумышленник может использовать не один а несколько последовательно включенных VPN-сервисов, что существенно усложняет задачу исследования.

[1] Поздышев Роман Сергеевич Деанонимизация личности преступника в сети Интернет // Вестник Уральского юридического института МВД России. 2022. №2 (34). URL: https://cyberleninka.ru/article/n/deanonimizatsiya-lichnosti-prestupnika-v-seti-internet (дата обращения: 23.04.2023).

Одной из методик, которые могут помочь в деанонимизации злоумышленников, использующих VPN-сервисы является исследование информации, содержащейся в Cookies (куки) -файлах, важной особенностью которых является их неизменность.

Cookies – это текстовые файлы, которые сайт сохраняет на компьютере посетителя для того, чтобы он(сайт) мог его опознавать, для сбора статистики, сохранения персональных настроек и т.п.[1]. Также cookie-файл можно представить как уникальный номер, который интернет-сайт присваивает веб-браузеру при первом обращении, а впоследствии использует его для идентификации (опознания) при всех последующих интернет-соединениях. Еще одно сравнение, применимое к cookies – это отпечатки пальцев, по которому можно опознать лицо, повторно заходящее на определенный сайт.

К примеру, для совершения покупки покупатель заходит на сайт интернет-магазина, и добавляет в корзину какие-то товары, применяет какие-либо настройки, а затем закрывает вкладку браузера. Если покупатель снова зайдет на сайт интернет-магазина, то и товары в корзине и примененные настройки сохранятся. Все это происходит потому, что сайт интернет-магазина опознал покупателя по сохраненным на компьютере покупателя cookies.

Данные файлы могут постоянно храниться на компьютере пользователя, либо удаляться после завершения сессии (завершения работы с сайтом и закрытия браузера). То есть существуют временные и постоянные Cookies-файлы.

После того как пользователь вводит адрес сайта в браузере, браузер ищет на устройстве файлы cookie этого сайта. Если искомые файлы найдены, то они направляются на сервер данного сайта. Сайт, получив файлы и начинает их использовать для идентификации пользователя. Если браузер не находит cookie, и соответственно не перенаправляет их на сайт, то этот сайт считает пользователя новым посетителем. Как правило новым посетителям направляется запрос о создании Cookies-файлов.

Конкретная информация, которая может сохраняться в Cookies, зависит от сайта, который их создает. Это та информация, которая нужна сайту для дальнейшей работы с определенным пользователем. Основные типы данных сохраняемых в cookies являются следующие: личные данные пользователей (телефонные номера, данные о введенных документах, платежные данные); настройки примененные пользователем (город или иное поселение, язык, валюта, масштаб страницы); данные авторизации (логины, пароли); информация об устройстве с которого заходили на сайт (модель устройства, версия браузера); данные об активности пользователя (переходы на определенные страницы, «клики» на определенные объекты – баннеры, товары).

Исследование Cookies-файлов активно используется криминалистами при исследовании компьютеров подозреваемых для выяснения информации о сетевой активности и сбора соответствующей доказательной базы.

---

[1] Курс по анонимности и безопасности в сети:© CyberYozh security group https://book.cyberyozh.com/ru/deanonimizatsiya-polzovatelej-vpn-i-proxy-cherez-cookies/

Вместе с тем анализ на основе анализа cookies-файлов возможно установление личности злоумышленника, совершающего противоправные действия путем VPN-сервисов. Например, злоумышленник для совершения противоправной деятельности (размещение экстремистских материалов) подключается к сети интернет посредством VPN и авторизуется в социальной сети используя подложный аккаунт. Впоследствии он же, отключив VPN авторизуется в данной социальной сети используя свой реальный аккаунт, либо же его родственники делают на одном (домашнем) компьютере. Соответственно, появляется возможность идентифицировать злоумышленника направив к администрации социальной сети запрос с просьбой указать иные учетные записи и/или ip-адреса, которые использовались для подключения к социальной сети с использованием веб-браузера, данные о котором получены из анализа файлов cookies.

Еще одним способом собирать информацию о пользователях в сети интернет со стороны браузеров является технология снятия отпечатков браузера (также называемых отпечатками пальцев (finger print) устройства или онлайн-отпечатками пальцев, по сути являющихся цифровыми следами.

Снятие отпечатков браузера основано на работе специальных сценариев, которые запускаются в фоновом режиме браузера и используются скриптами веб-сайтов для сбора информации.

Современные web-сайты для обеспечения нормальной работоспособности работают путем использования специальных инструкций (скриптов), которые работая в фоновом режиме собирают определенную информацию, позволяющую в совокупности создавать уникальный онлайн-отпечаток браузера, который впоследствии может быть отслежен в сети интернет. Следует отметить, что сбор цифровых отпечатков осуществляется даже в браузером Tor.

Содержание отпечатка составляет информация об используемом устройстве, операционной системе, установленном браузере и всех установленных расширениях браузера, о местонахождении устройства, установленном программном обеспечении, разрешении экрана, драйверах и т.д. То есть аналогия с отпечатком пальца здесь не случайна. Получается, что описанные алгоритмы позволяют идентифицировать устройство по оставляемому им цифровому отпечатку.

Цифровой отпечаток браузера, позволяет идентифицировать устройство, на котором он установлен из большого количества других аналогичных устройств. Даже если отпечатки собраны на аналогичных устройствах (одинаковых моделях сотовых телефонов) они будут отличаться из-за разного набора программ, драйверов, отличающейся геолокации и т.д.

Таким образом злоумышленник может быть идентифицирован в сети интернет, по создаваемому его устройством уникальному цифровому отпечатку, по аналогии с процедурой идентификации, основанной на анализе данных из файлов cookies. При этом цифровой отпечаток браузера не может быть удален, как cookies файлы, он не может измениться между сеансами, не зависит от

очистки истории просмотра в браузере, от того включен ли в браузере режим «инкогнито» или нет[1].

В настоящее время использование цифровых отпечатков браузеров прежде всего распространено в коммерческой индустрии для направления конкретным лицам избирательной рекламы. Однако использование данной технологии в правоохранительной деятельности для деанонимизации преступников видится достаточно перспективным и требующем тщательного изучения.

Типичной следственной ситуацией является случай, когда злоумышленник, помимо применения средств анонимизации, для своей противоправной деятельности в сети интернет использует также специальный («черный») сотовый телефон. То есть для законной деятельности, «в обычной жизни» используется одно устройство, а для преступной деятельности приобретается другое устройство. Также приобретаться и SIM-карта, которая зарегистрирована на иное лицо, которое никак не может быть сопоставлено со злоумышленником. В описанной ситуации установить злоумышленника и доказать его причастность к противоправной деятельности достаточно сложно. Здесь используются методики, направленные на анализ возможных ошибок, которые совершил, или может совершить злоумышленник.

Так в одном из случаев, следователи столкнулись с совершением противоправной деятельности в сети Интернет с использованием не зарегистрированного на злоумышленника устройства и Sim-карты было установлено, что счет сотового телефона пополняется наличными денежными средствами через терминалы. Следователи предположили, что злоумышленник, пополняя счет сотового телефона для преступной деятельности, может одновременно пополнить и телефон, которым он пользуется официально. Для проверки данной версии были направлены запросы операторам платежных систем, с просьбой предоставить информацию о номерах, которые пополнялись вместе с номером, используемым для преступной деятельности (за 1-3 минут до и через 1-3 минуты после пополнения «официального» номера). Проводя опрос лиц, которым принадлежали пополняемые номера телефонов было установлено, что в одном из случав злоумышленник пополним номер телефона, принадлежавший его знакомой, которая и предоставила следователям информацию о злоумышленнике.

Отслеживание поведения злоумышленника на предмет совершения ошибки, приводящей к деанонимизации может привести к положительному результату – установлению личности злоумышленника. Например в одном из случаев преступник, пользуясь для противоправной деятельности специальным устройством, в определенный момент, вынужден был совершить звонок своему родственнику, используя это устройство (звонок был срочным, а «официальный»

[1] См. например: Алисултанова Э. Д., Исаева М. З., Болтиев Д. У. Анализ систем автономной идентификации пользователя сайта // Электронная наука. 2021. №2. URL: https://cyberleninka.ru/article/n/analiz-sistem-avtonomnoy-identifikatsii-polzovatelya-sayta (дата обращения: 24.04.2023).

телефон использовать было невозможно). Далее через данного родственника злоумышленник был установлен и задержан.

Приведенные методы установления личности подозреваемого лица в сети Интернет не дают точной гарантии получения положительного результата. Профессиональный преступник с легкостью может предусмотреть применение контрмер, которые помогут ему избежать идентификации таким путем.

Вместе с тем следует учитывать присущий любому лицу человеческий фактор. Любой, даже профессиональный преступник, предусмотрев все возможные средства анонимизации рано или поздно может совершить ошибку, из-за собственной невнимательности или легкомыслия, что в последствии позволит установить его личность, а также причастность к совершенному противоправному действию.

Соответственно сотрудникам, осуществляющим расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий следует применять все возможные методики и проверять все возможные версия, не допуская пренебрежения из убежденности в неэффективности метода.

О.В. Макарова

Использование инструментов мониторинга в противодействии киберпреступности (международный и зарубежный опыт)

Аннотация. В данной статье рассматривается международный опыт мониторинга практики противодействия киберпреступности с целью эффективной борьбы с этим растущим вызовом информационной эпохи. Исследование основывается на изучении международного и зарубежного опыта, включая лучшие практики и инструменты, применяемые в различных странах. В статье подчеркивается важность обмена опытом и сотрудничества между странами для совместной борьбы с киберпреступностью. Изучение и применение международного опыта в мониторинге политик противодействия киберпреступности может способствовать созданию более безопасной цифровой среды и защите интересов общества и государства.

Ключевые слова: киберпреступность, кибербезопасность, инструменты мониторинга, политика противодействия киберпреступности.

Борьба с киберпреступностью представляет собой одну из наиболее значимых задач организаций и государств в современном технологичном мире. С развитием технологий и распространением цифровой среды, возникает все больше угроз, связанных с нарушением информационной безопасности и незаконным доступом к компьютерным системам. Для эффективного противодействия киберпреступности важно использовать разнообразные инструменты, среди которых ключевую роль играет мониторинг существующих политик. Данная статья направлена на изучение международного и зарубежного

опыта в использовании инструментов мониторинга различных политик противодействия киберпреступности.

В зарубежной литературе киберпреступления определяются как преступления, совершенные с использованием электронных средств и методов, направленные против физических или юридических лиц.[1] Такие преступления могут включать в себя компьютерное мошенничество, кибершпионаж, кибернападения, кибертерроризм, распространение вредоносного программного обеспечения, нарушение авторских прав и многие другие формы незаконной деятельности.

В 2017 году затраты на борьбу с киберпреступностью в США достигли суммы около 600 миллиардов долларов. Однако, уже к 2019 году эти затраты увеличились на 118%, подчеркивая растущую сложность и масштаб проблемы.

Аналогичные тенденции можно наблюдать и в Канаде. По результатам одного из недавних исследований, проведенного в 2017 году на репрезентативной выборке из 10 000 предприятий, было обнаружено, что компании потратили сумму в размере 14 миллиардов канадских долларов за год на защиту своих систем от различных форм вредоносной активности в Интернете. Более одной пятой этих компаний также пострадали от кибератак, показывая уязвимость и реальность угрозы.[2]

В свете таких статистических данных становится очевидным, что противодействие киберпреступности и обеспечение кибербезопасности являются важными задачами как для организаций, так и государств.

Также важно отметить, что киберпреступления имеют международный и трансграничный характер. Преступники могут находиться в одной стране, а их жертвы и данные, которые они атакуют - в другой. Это создает сложности в обнаружении, преследовании и наказании преступников, а также в обеспечении сотрудничества между правоохранительными органами различных стран.

В борьбе с киберпреступностью международное сотрудничество и обмен информацией играют важную роль. Различные страны и международные организации разрабатывают соглашения и механизмы для обмена информацией о киберугрозах, сотрудничества в расследованиях и экстрадиции преступников. Примерами таких соглашений являются Будапештская конвенция о киберпреступности и соглашения о взаимной юридической помощи.

Несмотря на значительные инвестиции в политику предотвращения киберпреступлений и кибербезопасности, действенных инструментов, которые могут помочь политикам и общественности определить эффективность государственных мер по борьбе с преступлениями в Интернете все еще недостаточно. В зарубежной литературе рассматривается потенциал инструментов мониторинга для восполнения этого пробела. Мониторинг политики кибербезопасности основывается на систематическом сборе данных о

[1] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, “Comprehensive review of cybercrime detection techniques,” IEEE Access, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[2] Bilodeau, H., M. Lari, and M. Uhrbach. 2019. Cyber Security and Cybercrime Challenges of Canadian Businesses, 2017. Ottawa: Statistics Canada.

разработке и реализации различных способов борьбы с киберпреступностью.[1] Платформы мониторинга практик кибербезопасности способствуют созданию более надежной базы знаний об инициативах по предотвращению киберпреступности, разрабатываемых по всему миру, чтобы содействовать распространению эффективных политик и препятствовать принятию контрпродуктивных мер.

В международном сообществе было разработано несколько инициатив, направленных на консолидацию информации и обмен опытом в области кибербезопасности. Эти инициативы играют важную роль в обеспечении сотрудничества и координации усилий по борьбе с киберугрозами.

Индекс киберготовности (CRI - Cyber Readiness Index), разработанный в 2013 году, рассматривает уровень зрелости, который демонстрируют страны в своих усилиях по развитию потенциала кибербезопасности, и направлен на измерение оперативного потенциала страны по семи измерениям: соответствие национальной стратегии, уровень реагирования на инциденты, электронная преступность и правоприменение, обмен информацией, инвестиции в исследования и разработки, дипломатия и торговля, оборона и кризисное реагирование.[2] Для оценки каждого аспекта используются три уровня готовности: недостаточное количество данных (данные отсутствуют или недоступны), частичное функционирование (результаты наблюдаются, но их функциональность трудно измерить) и полное функционирование (функционирование можно наблюдать и измерить). По состоянию на май 2023 года, было выпущено 11 углубленных страновых профилей для Франции, Германии, Индии, Италии, Японии, Марокко, Нидерландов, Саудовской Аравии, Словакии, Великобритании и Соединенных Штатов Америки.

Панели кибербезопасности ЕС и Азиатско-Тихоокеанского региона (The EU and Asia-Pacific Cybersecurity Dashboards) нацелены на оценку комплекса мер кибербезопасности в 28 европейских и 10 азиатских странах. Каждая страна оценивается по 25 критериям, объединенных в пять тем: правовые основы, операционная деятельность, государственно-частное партнерство, отраслевые планы по кибербезопасности и образование. Каждый критерий оценивается как выполненный, частично выполненный или отсутствующий.

Следующим важным инструментом мониторинга в области кибербезопасности является Глобальный индекс кибербезопасности (Global Cybersecurity Index), который оценивает потенциал кибербезопасности 194 стран по пяти основным параметрам: правовые меры, технические меры, организационные меры, наращивание потенциала и сотрудничество. Этот индекс предоставляет систематическую оценку и сравнение уровня кибербезопасности различных стран, позволяя определить их сильные и слабые стороны в этой области.

---

[1] Dupont, Benoit. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice. 42. 500-515. 10.1080/0735648X.2019.1691855.

[2] Hathaway, M., C. Demchak, J. Kerben, J. McArdle, and F. Spidalieri. 2015. Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index. Washington DC: Potomac Institute for Policy Studies.

База данных Международного обзора кибер-разработок (International Cyber Developments Review - INCYDER также служит важным источником информации. Она содержит перечень правовых и политических документов, принятых различными международными и региональными организациями, такими как Организация Объединенных Наций (ООН), Организация экономического сотрудничества и развития (ОЭСР), Большая семерка (G7), Европейский союз (ЕС) и другими. Эти документы являются основой для разработки политик и стратегий в области кибербезопасности и отражают совокупный опыт и знания международного сообщества.

Использование платформ мониторинга, рассмотренных ранее, позволяет оценить и анализировать состояние и развитие политик и мер в области кибербезопасности на международном уровне. Это помогает странам и организациям лучше понимать текущие вызовы и требования в области кибербезопасности, а также разрабатывать эффективные стратегии и политики для содействия безопасному и устойчивому киберпространству.

В целом, изучение зарубежного опыта в области противодействия киберпреступности позволяет понять различные аспекты этой проблемы, эффективные стратегии и инструменты мониторинга, которые применяются для защиты от киберугроз и преследования преступников. Это знание может быть ценным для разработки соответствующих правовых и технических механизмов в России с целью эффективного противодействия киберпреступности и обеспечения информационной безопасности.

Литература

1. Al-Khater W. A., Al-Maadeed S., Ahmed A. A., Sadiq A. S., Khan M. K. “Comprehensive review of cybercrime detection techniques,” IEEE Access, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.
2. Bilodeau, H., M. Lari, and M. Uhrbach. 2019. Cyber Security and Cybercrime Challenges of Canadian Businesses, 2017. Ottawa: Statistics Canada.
3. Dupont, Benoit. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice. 42. 500-515. 10.1080/0735648X.2019.1691855.
4. Hathaway, M., C. Demchak, J. Kerben, J. McArdle, and F. Spidalieri. 2015. Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index. Washington DC: Potomac Institute for Policy Studies.

Е.А. Матвеева
В.А. Шестак

Современная стратегия борьбы с киберпреступностью в Республике Ирландия

Аннотация. В статье рассматривается практика применения в Республике Ирландия одной из форм системного воздействия на преступность – борьбы с

киберпреступностью. Государством принята стратегия развития, в рамках которой разработаны и функционируют информационные платформы и программы, призванные обеспечить устойчивое снижение уровня киберпреступности в обществе. Исследованы рабочие варианты криминологических разработок, выявлены основные направления их применения.

Ключевые слова: воздействие на преступность, стратегия развития, компьютерные преступления, онлайн-платформы, Ирландия.

В связи с глобализацией в современном мире появляется все больше возможностей и способов совершения различных преступлений. Так, феномен, который относительно недавно невозможно было даже представить, теперь стал одной из ключевых проблем в мире. Речь идет о киберпреступлениях.

Согласно Кембриджскому словарю киберпреступления (или компьютерные преступления) – это незаконные, противоправные действия с использованием компьютера[1], структурно состоящие из:

«традиционных» преступлений (например, мошенничество, подлог, неправомерное использование персональных данных);

преступлений, связанных с контентом (в частности, распространение материалов о сексуальном насилии над детьми в сети-Интернет, разжигание ненависти или подстрекательство к совершению террористических актов);

преступлений, непосредственно связанных с компьютерами и информационными системами (к примеру, атаки на информационные системы, распространение вредоносных программ, взлом с целью кражи конфиденциальных, личных или отраслевых данных и атаки типа «отказ в обслуживании» с целью нанесения финансового или репутационного ущерба);

преступлений, связанных с оборотом незаконных товаров и услуг (от наркотиков до онлайн-материалов о сексуальном насилии и эксплуатации детей и списках украденных номеров кредитных карт).

Объем международного рынка киберпреступлений составляет 1,5 трлн долларов США[2], что сопоставимо с ВВП Австралии за 2022 год по данным Всемирного банка[3]. Согласно исследованиям школы Кларка в Университете Мэриленда за сутки в мире происходит около 2244 киберпреступлений, то есть 1 кибератака в 36 секунд[4]. Глобальные издержки на борьбу с

[1]Cambridge Dictionary. [Электронный ресурс]. Режим доступа: https://dictionary.cambridge.org/dictionary/english/cybercrime (Дата обращения: 22.10.2022)

[2] Cybercrime Magazine. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Дата обращения: 22.10.2022)

[3] World Bank national accounts data, and OECD National Accounts data files. [Электронный ресурс]. Режим доступа: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

[4] A. James Clark School of Engineering. Study: Hackers Attack Every 39 Seconds. [Электронный ресурс]. Режим доступа: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (Дата обращения: 22.10.2022)

киберпреступностью за 2022 составят 170,4 млрд долларов США. Ожидается, что к 2025 году они достигнут 10,5 трлн долларов[1].

Республика Ирландия является одной из ведущих стран мира в борьбе с киберпреступностью. Хотя в Республике законодательно не закреплено определение киберпреступлений (поэтому киберпреступность там понимается в широком смысле), государство проводит ряд мероприятий, призванных обеспечить устойчивое снижение уровня киберпреступности в обществе. С 2014 года в Ирландии отмечался интенсивный рост киберпреступности. Обеспечение кибербезопасности в стране скоординировано стало решаться в рамках первой правительственной стратегии развития по обеспечению безопасности в сети-Интернет 2018 года (далее – Стратегия), с принятием которой интенсивность роста киберпреступлений замедлилась. Стратегия отражает общий подход Правительства Республики Ирландия и осуществляется по пяти следующим направлениям: принятие законов о новых составах преступлений; использование технического оборудования и создание возможности для удаления незаконных и вредоносных материалов; работа с онлайн-платформами, базирующимися в Республике Ирландии, для продвижения мер безопасности в сети-Интернет; взаимодействие с государствами-членами ЕС и международными партнерами для обеспечения безопасности в сети-Интернет.

Реализация мер по названным направлениям возложена на шесть различных государственных ведомств, включая Министерство юстиции, а именно Отдел по борьбе киберпреступностью (далее – ОБК). ОБК обеспечивает представительство в ходе национальных и международных встреч, связанных с борьбой с киберпреступностью. ОБК разработаны Интернет-платформы и программы, которые могут быть классифицированы следующим образом: программы, предоставляющие информацию о кибербезопасности и возможных киберпреступлениях, и образовательные программы, направленные на обучение учителей, детей и их родителям основам кибербезопасности.

В рамках первой классификации в Республике Ирландия была создана единая онлайн-точка доступа Be Safe Online как часть государственного портала gov.ie (подобно российскому порталу mos.ru), которая предоставляет информацию о безопасности в сети-Интернет. Кроме того, борьба с незаконным и вредоносным использованием сети-Интернет требует ответных мер на национальном, европейском и международном уровнях. Республика Ирландия, являясь государством-членом ЕС, приняла инициативу «Безопасный Интернет», разработанную ЕС. В рамках данной инициативы Ирландия обеспечивает повышение осведомленности населения, телефон доверия и горячую линию. Эти услуги предоставляются партнерскими организациями, а Отдел киберпреступности обеспечивает координацию данной деятельности.

Партнерами инициативы ЕС «Безопасный Интернет» является ряд организаций, создавших собственные платформы. Так, hotline.ie, основанная в

[1] Cybercrime To Cost the World $10.5 Trillion Annually By 2025. [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Дата обращения: 22.10.2022)

1999 году, предоставляет безопасную конфиденциальную услугу, позволяющую общественности сообщать о подозрительном незаконном содержании в сети-Интернет. Она является основным национальным каналом Республики Ирландия, по которому представители общественности могут анонимно и конфиденциально сообщать о предполагаемом незаконном онлайн-контенте, особенно о материалах, связанных с сексуальными надругательствами над детьми, и о действиях, связанных с сексуальной эксплуатацией детей. С момента создания Hotline.ie тесно сотрудничает с An Garda Síochána (полицией Ирландии) и поставщиками онлайн-услуг, чтобы оперативно удалять из Интернета материалы о сексуальном насилии над детьми и обеспечивать идентификацию и защиту детей на изображениях.

Ирландская ассоциация интернет-провайдеров (ISPAI) создана для управления горячей линией – службой, которая позволяет общественности сообщать о предполагаемом незаконном контенте или действиях, обнаруженных в сети-Интернет.

К образовательным программам, обучающим основам кибербезопасности, можно отнести следующие платформы. Так, Webwise.ie является ирландским Центром информирования о безопасности в Интернете и частью Службы профессионального развития учителей, службы поддержки, финансируемой Министерством образования. Она занимается повышением осведомленности, разрабатывает материалы и программы для школ и проводит ежегодное мероприятие, посвященное Дню безопасного Интернета в Республике Ирландии. Webwise.ie способствует более безопасному и лучшему использованию Интернета посредством информационно-просветительских и образовательных инициатив, ориентированных на учителей, детей, молодежь и родителей. Webwise.ie разрабатывает и распространяет ресурсы, которые помогают учителям интегрировать цифровое пространство и онлайн-безопасность в преподавание и обучение в своих школах. Webwise.ie также предоставляет информацию, советы и инструменты для родителей, чтобы поддержать их участие в онлайн-жизни своих детей. С помощью Молодежной консультативной группы Webwise.ie, она разрабатывает ориентированные на молодежь ресурсы по повышению осведомленности и обучающие программы.

Ирландское общество по предотвращению жестокого обращения с детьми (ISPCC) управляет линией помощи (Childine), которая предоставляет услуги 24/7 (круглосуточно и без выходных). Несовершеннолетние лица пострадавшие от преступлений, с которыми они столкнулись в сети-Интернет, могут обратиться за советом и помощью в данную службу.

Начальная школа Национального родительского совета управляет линией помощи для родителей и взрослых, специальной линией помощи для решения вопросов, связанных с безопасностью в сети-Интернет, включая киберзапугивание. Начальная школа Национального родительского совета также предоставляет курсы для обучения основам кибербезопасности.

Ирландский центр безопасного Интернета (SIC) представляет собой партнерство четырех ведущих организаций, миссия которых заключается в том, чтобы сделать Интернет лучше для детей и молодежи, при координации

Министерства юстиции, Отдела по борьбе с киберпреступностью. Центры безопасного Интернета софинансируются Европейским союзом в рамках программы Connecting Europe Facility Safer Internet Program и обычно предлагают три вида услуг: национальный информационный центр, телефон доверия и горячая линия. Центры безопасного Интернета сотрудничают и обмениваются ресурсами и передовым опытом через сеть INSAFE-INHOPE.

Таким образом, в современных условиях в Республике Ирландия активно применяются технические механизмы противодействия киберпреступлениям. Все программы и платформы ставят своей целью информирование граждан о киберпреступности и защиту их устройств от несанкционированного доступа Интернет-мошенников. Кроме того, благодаря разработанным платформам совершенствуется программа безопасности пользователей в сети-Интернет. На протяжении нескольких лет (с 2018 года) наблюдается устойчивая тенденция к снижению темпов роста киберпреступлений в стране, что свидетельствует об эффективности принятой Стратегии.

Литература

1. A. James Clark School of Engineering. Study: Hackers Attack Every 39 Seconds. [Электронный ресурс]. Режим доступа: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (Дата обращения: 22.10.2022)
2. Campbell, L. (2008). The Culture of Control in Ireland: Theorising Recent Developments in Criminal Justice. Web Journal of Current Legal Issues. [Электронный ресурс]. Режим доступа: http://webjcli.ncl.ac.uk/2008/issue1/campbell1.html (Дата обращения: 22.10.2022)
3. Cybercrime Magazine. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Дата обращения: 22.10.2022)
4. Cybercrime To Cost the World $10.5 Trillion Annually By 2025. [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Дата обращения: 22.10.2022)
5. GrantThornton. The Cost of Cybercrime 2022. [Электронный ресурс]. Режим доступа: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---cost-of-cybercrime-2022.pdf (Дата обращения: 22.10.2022)
6. World Bank national accounts data, and OECD National Accounts data files. [Электронный ресурс]. Режим доступа: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Л.Р. Муллагалеева

Использование киберпедофилами и малолетними потерпевшими электронных кошельков: актуальные проблемы.

Аннотация. В статье рассматривается проблема использования киберпедофилами и малолетними потерпевшими электронных кошельков. Отражены особенности использования киберпедофилами игр в социальных сетях для совершения насильственных действий сексуального характера в отношении малолетних потерпевших. Обосновывается необходимость усложнения процедуры регистрации электронного кошелька.

Ключевые слова: киберпреступность, электронный кошелек, малолетние, педофилы, социальная сеть.

Уголовное законодательство не приводит перечень преступлений, относящихся к киберпреступлениям. В большинстве случаев под киберпреступностью понимают деятельность, направленную для извлечения материальной выгоды.

Но киберпреступниками могут быть не только мошенники в привычном в настоящее время понимании, как лица «атакующие» телефонными звонками, либо присылающие в социальных сетях ссылки на сомнительные сайты. Органы предварительного следствия все чаще и чаще расследуют уголовные дела в отношении так называемых киберпедофилов. По большей части цель киберпедофилов -это удовлетворение половых потребностей, но в практической деятельности встречается и еще одна цель – получение денежных средств. При этом желание извлечь материальную выгоду преследуют не только обвиняемые, но и несовершеннолетние потерпевшие.

Большую опасность для несовершеннолетних представляют игры в социальной сети «ВКонтакте»: «Аватария», «Бутылочка». Для завлечения несовершеннолетних к диалогу в социальных сетях, киберпедофилы анализируют состав игроков по возрасту в таких играх.

Выявив заведомо малолетних, представляющих сексуальный интерес для педофила завязывается переписка в личных сообщениях социальной сети. Сообщение педофила может выглядеть следующим образом: «Привет. Если нужны голоса, можно у меня заработать»[1]. Получение голосов в игре «Аватария», в которой в настоящее время более 3 000 000 участников[2], это то, чем можно заманить играющего в «Аватарию» малолетнего.

Малолетние и не представляют какую опасность несет для них в дальнейшем переписка с незнакомым пользователем, готовым переслать им голоса или перевести денег для покупки голосов.

---

[1] Уголовное дело № 513/58-2019 // Архив Абдулинского районного суда Оренбургской области.

[2] Аватария. URL:https://vk.com/avataryaclub (Дата обращения: 17.04.2023).

Социальная сеть «ВКонтакте» разъясняет, что голоса ВКонтакте — универсальная условная единица платформы. Возможен обмен голосов на подарки и стикеры, а также на платные возможности приложений ВКонтакте. И тут же разъясняется: «Сайты, которые предлагают бесплатные голоса или обещают «умножить» их, являются мошенническими. Ни в коем случае не вводите там пароль от своего профиля, не соглашайтесь скачивать какие-либо программы или выполнять задания, иначе вы рискуете потерять аккаунт».

Голоса можно обменять обратно на обычные деньги и вывести их[1].

Обвиняемый Т. сообщил, что «ВКонтакте» он искал страницы лиц женского пола, которые за голоса «ВКонтакте» готовы были присылать ему фото и видео в обнаженном виде. Один голос стоил примерно 7 рублей, всего он потратил около 10 000 рублей в период с 2018 по 2019 год. Находил именно малолетних девочек, так как только они соглашались за «голоса» присылать фотографии и видеозаписи, девушки постарше не все соглашались на подобное[2].

В настоящее время «ВКонтакте» больше нельзя кому-либо перевести голоса. Тогда как ранее при возможности перевода голосов между пользователями социальной сети пострадало немалое количество детей. Так, 11-летняя потерпевшая Н. органам предварительного следствия сообщила о том, что за голоса она могла совершать покупки в играх, купить музыку. Но сама она не имела возможности их купить, так как у нее нет своей банковской карты. Поверив незнакомому пользователю согласилась за голоса присылать ему фотографии и видеозаписи в обнаженном виде. За присланные ею видеозаписи киберпедофил присылал ей больше голосов, чем за изготовленные ею фотографии[3].

Но так как теперь нет возможности пересылать голоса, это не означает, что проблема решена. Так, малолетние активно используют современные возможности электронных платежных систем.

В России самым популярным электронным кошельком является Qiwi. Электронный кошелек был запущен OSMP Group самой значимой российской сетью банкоматов. Основное различие между Qiwi и другими электронными кошельками является то, что к счетам Qiwi доступ можно получить как через терминалы, так и через любой смартфон[4].

---

[1] Заработок на играх ВК: с удовольствием и пользой.URL: https://smmx.ru/vk/dohod/zarabotok-na-igrah.html. (Дата обращения: 17.04.2023).

[2] Уголовное дело № 513/58-2019 // Архив Абдулинского районного суда Оренбургской области.

[3] Уголовное дело № 513/58-2019 // Архив Абдулинского районного суда Оренбургской области.

[4] Наговицына В.А., Савинова Е.А. Расчеты с помощью электронных кошельков в современных условиях // Тенденции и перспективы развития банковской системы в современных экономических условиях. 2023. URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-novyh-form-platezhey-v-elektronnoy-kommertsii (Дата обращения: 12.04.2023).

Выделяются следующие плюсы использования электронным кошельком:- простота использования;- скорость оплаты;- конфиденциальность и безопасность[1].

Но не во всех случаях простота использования электронного кошелька имеет положительный эффект.

Так, 10-летняя потерпевшая Л. указала, что ей написал в социальной сети «ВКонтакте» ранее незнакомый пользователь и предложил покупать у нее фотографии за голоса. Л. согласилась и начала отправлять свои фотографии в одежде. Но киберпедофила интересовали именно фотографии в обнаженном виде. Л. решила, что лучше отправлять фотографии не за голоса, а за деньги. Посмотрев видеоролик по созданию Qiwi-кошелька в сети Интернет, решила его создать на свой номер телефона, но снимать деньги с электронного кошелька возможно только через банк. Так как сама в силу 10-летнего возраста не могла снимать деньги с Qiwi-кошелька и поэтому решила сказать маме, что нашла приложение, через которое можно зарабатывать деньги и мама начала снимать деньги с помощью банковской карты. За одну фотографию киберпедофил присылал ей по 10 рублей, отправила она ему всего более сотни фотографий. Педофил начал шантажировать тем, что в случае отказа присылать фотографии, он распространит в сети Интернет имеющиеся у него изображения, что он в дальнейшем и сделал.

Только при расследовании одного уголовного дела установлено, что из 9 малолетних потерпевших, 5 использовали электронный кошелек Qiwi.

Но встречаются в следственной практике и случаи, когда педофилы за отказ детей фотографироваться и снимать видеозаписи в обнаженном виде предлагают следующий вариант. Так, С. заставлял переводить деньги детей за отказ присылать фотографии и видеозаписи, то есть, если ребенок не хочет выполнять желание педофила, то может перевести ему деньги с помощью электронного кошелька Qiwi[2].

Как следует из следственной практики, регистрация электронного кошелька Qiwi не представляет сложностей, даже для десятилетних детей, так как для регистрации необходимо ввести только используемый абонентский номер. Но подобная упрощенная регистрация влечет и негативные последствия для несовершеннолетних. В связи с этим необходимо усложнение процедуры регистрации электронных кошельков.

К примеру, на сайте «КАРШЕРИНГИ.РУ» указано обязательное условие при регистрации - сделать селфи-снимок с водительским удостоверением[3]. Усложненная регистрация в каршеринг-сервисе вероятнее всего объясняется желанием избежать рисков в виде материальных потерь. Но разве психическое

[1] Молдован А.А. Электронные деньги: Яндекс деньги, WEBMONEY, PAYPAL, QIWI: риски и проблемы управления безопасностью // «Научно-практический электронный журнал «Аллея Науки» №3(42) 2020 Alley-science.ru. URL:https://www.elibrary.ru/item.asp?id=42855986 (Дата обращения: 14.04.2023).

[2] Уголовное дело № 52/65-2018 // Архив Промышленного районного суда г. Оренбурга.

[3] Регистрация в кашеринг-сервисе. URL: https://carsharingi.ru/registration (дата обращения: 15.04.2023).

здоровье детей не является более приоритетным, чем желание владельцев электронных платежных систем извлечь финансовую выгоду. В связи с этим необходимо и при регистрации электронных кошельков по вышеуказанному примеру требовать селфи-фотографию с паспортом, что соответственно приведет к тому, что дети до 14 лет не смогут создать сами себе электронные кошельки.

Литература

1. Молдован А.А. Электронные деньги: Яндекс деньги, WEBMONEY, PAYPAL, QIWI: риски и проблемы управления безопасностью // «Научно-практический электронный журнал «Аллея Науки» №3(42) 2020 Alley-science.ru. URL:https://www.elibrary.ru/item.asp?id=42855986 (Дата обращения: 14.04.2023).
2. Наговицына В.А., Савинова Е.А. Расчеты с помощью электронных кошельков в современных условиях // Тенденции и перспективы развития банковской системы в современных экономических условиях. 2023. URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-novyh-form-platezhey-v elektronnoy-kommertsii (Дата обращения: 12.04.2023).
3. Аватария. URL:https://vk.com/avataryaclub (Дата обращения: 17.04.2023).
4. Заработок на играх ВК: с удовольствием и пользой.URL: https://smmx.ru/vk/dohod/zarabotok-na-igrah.html. (Дата обращения: 17.04.2023).
5. Регистрация в каршеринг-сервисе. URL: https://carsharingi.ru/registration (дата обращения: 15.04.2023).
6. Уголовное дело № 52/65-2018 // Архив Промышленного районного суда г. Оренбурга.
7. Уголовное дело № 513/58-2019 // Архив Абдулинского районного суда Оренбургской области.

Н.Г. Муратова

Генезис применения математических и информационно-технологических методов при противодействии киберпреступлениям

Аннотация. Проблематика исследования о методах противодействия современной преступности разнообразна: электронные доказательства цифровая криминалистика, математические методы, компьютерные технологии, электронное уголовное дело, технологии искусственного интеллекта. Акцент проблематики: противодействия преступному информационному полю. Автор аргументирует мысль о том, что при этом надо обеспечить некоторые уровни сопровождения расследования дела. Первый уровень - правовое сопровождение расследования уголовного дела, второй - цифровой уровень сопровождения расследования уголовного дела, третий уровень – информационно-биометрическое сопровождение расследования уголовного дела

Ключевые слова: генезис математических методов, электронные доказательства, информационные технологии, противодействие преступности.

Технологическое комплексное сопровождение расследования уголовного дела в современных условиях неизбежно как по форме, так и по содержанию. Особое внимание требуется при выявлении и фиксации преступлений в электронно-информационном и информационно-телекоммуникационном пространстве (в том числе сети Интернет).

С учетом заявленной тематики внимание можно сосредоточить на *математических методах, электронных и информационных технологиях* при противодействии киберпреступлениям, или другими словами, на технологическом сопровождении расследования таких категорий преступлений. Мы видим в лексиконе правоприменителей современный глоссарий, определяющий информационные технологии: цифровая (электронная) валюта, криптовалюта, фиатная валюта, майнинг, блокчейн, хеш, хеширования, облачные вычисления, игровой (технологический) автомат,[1] «компьютерная атака», «компьютерный инцидент», «безопасность критической информационной инфраструктуры».[2]

Еще в далеком прошлом ученые начали говорить о значении математики, например, при оценке свидетельских показаний, применяя методы теории вероятности, идеи применения количественных показателей и возможности выиграть или проиграть иски[3]. Отмечаются идеи немецкого математика, философа и юриста Готфлида Вильгельма Лейбница, который «служил при Петре 1 и его считали основоположником дифференциальных и интегральных исчислений, и, в будущем, кибернетики».[4]

В теории права и уголовно-процессуальном праве существуют научные позиции относительно применения математических методов. В литературе понятие «математическая юриспруденция» введена Д.А.Керимовым в 1972г.[5]. Д.Н.Горшунов пишет, что в отличии от математической абстракции, юридическая абстракция «происходит не через последовательное решение

---

[1] Постановление Пленума Верховного Суда РФ от 15 декабря 2022г. № 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» // https://www.garant.ru/hotlaw/federal/1591816/ - дата обращения 22.12.2022.

[2]Федеральный закон РФ от Федеральный закон от 26 июля 2017 г. № 187-ФЗ вводит понятия «О безопасности критической информационной инфраструктуры Российской Федерации»

[3] Пьер Симон Лаплас (1775 год), Симеон Пуассон, (1837), Огуст Курно (1877) , Дж.Шуберт, (1959), Стюарт Нагель, (1961) Математические методы //studme.org/84127/parvo/matematicheskie_metody –дата вхождения 25.01.2020.

[4] Горшунов Д.Н. Математические методы исследования системы права// Ученые записки казанского государственного университета. Гуманитарные науки. Т.150. кн.5., Казань: 2008. - С.29.

[5] Керимов Д.А. Философские проблемы права. – М.: Мысль, 1972. - С.299; Керимов Д.А. Методология права. Предмет, функции, проблемы философии права, 2-е изд. – Москва: Аванта, 2001.

задачи, выведение формулы, а через обнаружение признаков и степени достаточности».[1] При изучении социальных явлений и процессов в рамках юридических наук отмечаются эффективное использование теории вероятности, математической статистики, математической логики, теории информации, исследование операций и другие.[2] Об «основных методах исследования и построения систем поддержки принятия решения» говорит А.А. Бессонов, актуализируя «использование функциональных возможностей языка программирования».[3] Можно отметить некоторые выявленные основы применения математических методов.[4] В криминалистике предлагается использовать математические (формулы, таблицы, числовые последовательности, геометрические образы), имитационные и эвристические модели при расследовании должностных преступлений коррупционной направленности.[5] Существует мнение, что математика даёт возможность осуществить обработку цифровых данных, использовать математическую логику, комбинаторику, математическую статистику и методы теории вероятности.[6] Отмечается, что при изучении математических методов в юридической практике важную роль играет статистика, обработка информации, возможность выявить достоверный прогноз на основании имеющегося

[1] Горшунов Д.Г. Математические методы в исследовании системы права// Ученые записки казанского государственного университета. Том.150. Гуманитарные науки. – Казань, 2008. С.31.

[2]Бурсина А.В. Математика в юриспруденции////www//http://studwood.ru/602236/parvo/-дата вхождения 25.01.2020.

[3]Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступности. Монография: Проспект, 2021. -816 с.

[4] Автор данного исследования ранее приняла участие в проекте для издания входящего в перечень Scopus и это позволило более внимательно изучить литературу и заявленную проблематику: обосновано формирование Концепции применения математических методов и алгоритмов в процессе принятия уголовно-процессуальных решений, которая предполагает: во-первых, формулирование концепта процессуального решения, во-вторых, определение системы вероятностных оснований для принятия процессуальных решений, в-третьих, установление рейтинговых критериев оптимального процессуального решения; в-четвертых, определения алгоритма вариативного результата процессуального решения по уголовному делу; в пятых, изучение мониторингового эффекта судебных ошибок // Муратова Н.Г., Соловьева Н.А., Рудковский В.А., Фантров П.П. Институциональная основа внедрения математических методов и алгоритмизации в процесс принятия решений в уголовном судопроизводстве Nadezhda Muratova1, Natalya Solovyeva2, Vladimir Shinkaruk3, Victor Rudkovskiy4, and Pavel Fantrov5 1 Kremlevskaya Street, 18, Kazan, Russia, muratowan@mail.ru 2 Universitskiy Prospekt, 100, Volgograd, Russia, solovieva_na@volsu.ru 3 Universitskiy Prospekt, 100, Volgograd, Russia, shinkaruk@volsu.ru 4 Universitskiy Prospekt, 100, Volgograd, Russia, rudkovskiy@volsu.ru 5 Universitskiy Prospekt, 100, Volgograd, Russia, pavelfantrov@volsu.ru //Digitalization of the decision-making process in criminal proceedings//SHS Web of Conferences 109, 01026 (2021) https://doi.org/10.1051/shsconf/202110901026

[5]Ковалев С.В. Математические методы криминалистического исследования преступлении коррупционной направленности в сфере экономики www//http://go.mail.ru/;docplayer.ru/62328917 – дата вхождения 25.01.2020.

[6]Лобков Н.В. Математические методы в профессиональной деятельности военного юриста//www//http://scienceforum.ru//2015/article/2015012439 – дата вхождения 25.01.2020

статистического материала.[1] Так, А. А. Бессонов предлагает ряд перспективных научно-прикладных перспектив при исследовании «методов математической статистики и алгоритмов искусственного интеллекта в научном изучении преступлений».[2]

В УК РФ всё больше составов преступлений, в конструктивных или квалифицирующих признаках которых указана электронная информация. Достаточно рассмотреть диспозиции следующих преступлений, чтобы убедиться в необходимости формирования концептуальных основ применения искусственного интеллекта в криминалистике и уголовном процессе: ст.272 УК РФ, ст.273 УК РФ, ст.274 УК РФ, ст.274.1 УК РФ, ст.159.3УК РФ, ст.159.6 УК РФ, ст.205.2 УК РФ, ст.207.1 УК РФ, ст.207.2 УК РФ), ст.171.2 УК РФ и др. В УПК РФ появился перечень следственных действий с использованием видео-конференц-связи (ФЗ от 20.12.2021 № 501-ФЗ). ФЗ РФ «Об оперативно-розыскной деятельности» (ч. 3, ч. 4 ст. 6) регламентирует возможность использовать информационные системы, видео – и аудиозапись, кино- и фото-сьемка, получение компьютерной информации. В России в соответствии с ФЗ от 29.12.2022 № 572-ФЗ появляется единая биометрическая система - государственная информационная система "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных", которая содержит биометрические персональные данные физических лиц».[3] Кроме того, в соответствии Федеральным законом от 24.04.2020. №123-ФЗ будет применяться экспериментальный правовой режим для внедрения технологий искусственного интеллекта в течение пяти лет в городе Москва.[4] Отмечают, что с появлением новых технологий появляются новые формы преступности.[5] Например, СМИ неоднократно публикуют факты

[1] Ильин И. Математика в жизни юриста//Молодой ученый, 2016 №17. – С.89-91.

[2] Бессонов А.А. Преимущества и ограничения использования технологий искусственного интеллекта в расследовании преступлений// Наука и технологии XX1 века: тренды и перспективы: сборник статей по итогам 1V Профессорского форума 2021г. В 2 томах: Т.1 Москва: Российское профессорское собрание, 2021. – С.14. (- 208с.)

[3] Федеральный закон № 572-ФЗ от 29.12.2022 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты РФ и признании утратившими силу отдельных положений законодательных актов РФ» // https://bazanpa.ru/gd-rf-zakon-n572-fz-ot29122022-h5841898/- дата обращения 26.05.2023.

[4] Федеральный закон №123-ФЗ от 24.04.2020. «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»// http://publication.pravo.gov.ru/Document/View/0001202004240030/Официальный портал правовой информации (государственная система правовой информации) – дата обращения 27.04.2020.

[5] Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: монография/О.С.Гузеева; Акад.Генюпрокуратуры Рос.Федерации. – М., 2015. С.13-14.

неправомерного доступа к учетным записям пользователей интернета и платежных систем.[1]

Генеральной прокуратурой РФ разработана и утверждена Концепция трансформации органов и организаций прокуратуры, которая обеспечивает понимание целей, задач и принципов применения информационных технологий при реализации полномочий прокуроров.[2] Активно обсуждается «Концепция электронного доказательства в уголовном судопроизводстве»[3], а также идеи об уголовно-правовом регулировании робототехники[4]. Ранее автором данного исследования сформулирована авторская идея о формировании концептуальных основ применения искусственного интеллекта в криминалистике и уголовном процессе».[5] Большое значение имеют комплексные меры по противодействию трансграничной преступности и, в том числе преступлениям, совершаемым с использованием информационных технологий.[6] Интересно, что в Казахстане появился Единый реестр досудебных расследований (ЕРДР) и в УПК была введена ст.42-1 «Формат уголовного судопроизводства».[7] Опубликована работа

---

[1]Иван Попов - В 11 регионах России задержана группировка из 30 хакеров//https://rg.ru/2020/03/24/v-11-regionah-rossii-zaderzhana-gruppirovka-iz-30-hakerov.html -дата обращения 21.04.2023

[2]Официальный сайт Генеральной прокуратуре РФ //https://www.garant.ru/products/ipo/prime/doc/71670972/-23.04.2023

[3]Концепция электронного доказательства в уголовном судопроизводстве - А. А. Дмитриева, П. С. Пастухов : https://doi.org/10.21202/jdtl.2023.11//https://www.lawjournal.digital/jour/article/view/155 - дата обращения 02.04.2023.

[4] Бегишев И.Р. Уголовно-правовое регулирование робототехники : монография. – М.: Блок-Принт, 2022. – С.44-45.

[5] «это система складывающихся в информационных правоотношениях взглядов, идей и явлений в сфере криминалистического и уголовно-процессуального процесса расследования преступлений с целью оптимального управления массивом статистическим данных и доказательственных сведений по уголовным делам при формулировании объективных выводов и решений при оценке процессуальной и криминалистической ситуации» - Муратова Н. Г. Искусственный интеллект, уголовный процесс и криминалистика: концептуальный подход Уголовный процесс и криминалистика: теория, практика, дидактика : сб. материалов VI Всерос. науч.-практ. конф. (Рязань, 16 дек. 2020 г.). – Рязань : ИП Коняхин А.В. (Book Jet), 2021. –С.226-230.

[6] Межгосударственная Программа совместных мер борьбы с преступностью. - Утверждена Решением Совета глав государств СНГ от 28 сентября 2018 года «О межгосударственной программе совместных мер борьбы с преступностью на 2019-2023 годы» (Принято в г.Душамбе 28.09.2018.) // https://e-ecolog.ru/docs/KDgwgrBafEZLEEui6YdSI/ful- дата обращения 25.04.2023.

[7] В 2017 году по инициативе Генеральной прокуратуры Республики Казахстан была разработана IT система электронного уголовного дела (Е-уголовное дело). Данное нововведение позволяет лицу, ведущему уголовный процесс, с учетом мнения участников уголовного процесса и технических возможностей вести уголовное судопроизводство в электронном формате, о чем он выносит мотивированное постановление. Электронное уголовное дело позволяет контролировать действия и решения лиц, ведущих уголовный процесс, служить сдерживающим фактором для различного рода укрытий, злоупотреблений и фальсификаций доказательств. Весь процесс прозрачен для контрольных органов и должностных лиц.» // Балгынтаев Асет Оралгазыевич - Электронное уголовное

о формировании нормативного регулирования единой цифровой среды адвокатуры.[1] Привлекают внимание рассуждения о теоретических основах формирования единой нормативной базы вещественных доказательств по уголовным делам.[2]

С учетом изложенного, необходимо на современном этапе развития технологий расследования выделить следующие уровни сопровождения расследования: первый уровень - правовое сопровождение расследования уголовного дела, второй уровень - цифровой уровень сопровождения расследования уголовного дела, третий уровень – информационно-биометрическое сопровождение расследования уголовного дела.

Таким образом, генезис применения математических и информационно-технологических методов при противодействии киберпреступлениям предполагает необходимость в формировании Концепции электронно-технологического сопровождения расследования уголовного дела, которая содержала бы комплексное, научное, профессионально-экспертного, оперативное, электронно-цифровое, техническое и финансово-аналитическое обеспечение расследования уголовного дела.

Литература

1. Федеральный закон РФ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // http://publication.pravo.gov.ru/Document/View/0001202004240030/Официальный портал правовой информации (государственная система правовой информации) – дата обращения 27.04.2020.
2. Федеральный закон №123-ФЗ от 24.04.2020. «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».
3. Федеральный закон № 572-ФЗ от 29.12.2022 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты РФ и признании утратившими силу отдельных положений законодательных актов РФ».

судопроизводство в Республике Казахстан //https://online.zakon.kz/Document/?doc_id=34878697&pos=6;-106#pos=6;-106-дата обращения 24.04.2023.

[1] Концептуальные основы нормативного регулирования единой цифровой среды адвокатуры России: монография / под науч. ред. Ю. С. Пилипенко, С. И. Володиной. М., 2022.—304 с.

[2] Муратов К.Д. Вещественные доказательства в сфере межотраслевых связей уголовного судопроизводства//Российский теоретический и научно-практический журнал общественных наук (экономика и право). Журнал прикладных исследований. – 2022 (август). – Т. 2. № 8. – С.185-192.

4. Постановление Пленума Верховного Суда РФ от 15 декабря 2022г. № 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».
5. Межгосударственная Программа совместных мер борьбы с преступностью. - Утверждена Решением Совета глав государств СНГ от 28 сентября 2018 года «О межгосударственной программе совместных мер борьбы с преступностью на 2019-2023 годы» (Принято в г.Душанбе 28.09.2018.)
6. Балгынтаев А.О. - Электронное уголовное судопроизводство в Республике Казахстан //https://online.zakon.kz/Document/?doc_id=34878697&pos=6;-106#pos=6;-106-дата обращения 24.04.2023.
7. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступности. Монография: Проспект, 2021. -816с.
8. Бессонов А.А. Преимущества и ограничения использования технологий искусственного интеллекта в расследовании преступлений// Наука и технологии XX1 века: тренды и перспективы: сборник статей по итогам 1V Профессорского форума 2021г. В 2 томах: Т.1 Москва: Российское профессорское собрание, 2021.
9. Бегишев И.Р. Уголовно-правовое регулирование робототехники : монография. – М.: Блок-Принт, 2022. – С.44-45.
10. Бурсина А.В. Математика в юриспруденции////www//http://studwood.ru/602236/parvo/
11. Горшунов Д.Н. Математические методы исследования системы права// Ученые записки казанского государственного университета. Гуманитарные науки. Т.150. кн.5., Казань: 2008. - С.29-31.
12. Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: монография/О.С.Гузеева; Акад.Ген.прокуратуры Рос.Федерации. – М., 2015. С.13-14.
13. Зализняк А.А. Древненовгородский диалект. – М.,1995, - с.345. Зализняк А.А Наблюдение за берестяными грамотами//История языка в древнейший период – М.,1984. Хрестоматия по истории отечественного государства и права) X-1917год/Состав.д.ю.н.,проф.в.а.Томсинов – М.:ИКД ЗЕРЦАЛО-М, 2004. – С.24-251.
14. Ищенко Е.П. Виртуальный криминал. –Москва: Проспект, 2015.
15. Ильин И. Математика в жизни юриста//Молодой ученый, 2016 №17. – С.89-91.
16. Иван Попов - В 11 регионах России задержана группировка из 30 хакеров//https://rg.ru/2020/03/24/v-11-regionah-rossii-zaderzhana-gruppirovka-iz-30-hakerov.html -дата обращения 21.04.2023
17. Керимов Д.А. Философские проблемы права. – М.: Мысль, 1972. - С.299; Керимов Д.А. Методология права. Предмет, функции, проблемы философии права, 2-е изд. – Москва: Аванта, 2001.

18. Концептуальные основы нормативного регулирования единой цифровой среды адвокатуры России: монография / под науч. ред. Ю. С. Пилипенко, С. И. Володиной. М., 2022.
19. Ковалев С.В. Математические методы криминалистического исследования преступлении коррупционной направленности в сфере экономики www//http://go.mail.ru/;docplayer.ru/62328917.
20. Концепция электронного доказательства в уголовном судопроизводстве - А. А. Дмитриева, П. С. Пастухов : https://doi.org/10.21202/jdtl.2023.11//https://www.lawjournal.digital/jour/article/view/155.
21. Лобков Н.В. Математические методы в профессиональной деятельности военного юриста//www//http://scienceforum.ru//2015/article/20150124390.
22. Муратова Н. Г. Искусственный интеллект, уголовный процесс и криминалистика: концептуальный подход Уголовный процесс и криминалистика: теория, практика, дидактика : сб. материалов VI Всерос. науч.-практ. конф. (Рязань, 16 дек. 2020 г.). – Рязань : ИП Коняхин А.В. (Book Jet), 2021. –С.226-230.
23. Муратова Н.Г., Соловьева Н.А., Рудковский В.А., Фантров П.П. Институциональная основа внедрения математических методов и алгоритмизации в процесс принятия решений в уголовном судопроизводстве.2021
24. Муратов К.Д. Вещественные доказательства в сфере межотраслевых связей уголовного судопроизводства//Российский теоретический и научно-практический журнал общественных наук (экономика и право). Журнал прикладных исследований. – 2022 (август). – Т. 2. № 8. – С.185-192.

Н.Р. Нургалеев, К.В. Максимов

Противодействие кибернаркопреступности в Республике Башкортостан

Аннотация. В статье рассмотрены некоторые аспекты противодействия кибернаркопреступности на территории Республики Башкортостан. В работе отражены имеющиеся проблемы и результаты деятельности подразделений МВД по Республике Башкортостан в выявлении и раскрытии преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий.

Ключевые слова: незаконный оборот наркотиков, кибернаркопреступность, Республика Башкортостан, подразделения по контролю за оборотом наркотиков, МВД России.

Современное развитие информационно-телекоммуникационных технологий (далее – IT-технологий) и социальных отношений, возникших благодаря им, характеризуется непрерывным ростом преступлений, в т.ч. связанных с незаконным оборотом наркотиков (далее – НОН). Однако если ранее

принимаемые меры предупреждения данных видов общественно опасных деяний были фрагментарны и противоречивы[1], то в настоящее время правоохранительная деятельность в данном направлении носит более системный и эффективный характер.

Противодействие НОН является одним из основных направлений деятельности МВД по Республике Башкортостан (далее – МВД по РБ) в рамках реализации мероприятий, определенных Стратегией государственной антинаркотической политики до 2030 года[2], а также государственной программой «Обеспечение общественной безопасности в Республике Башкортостан» на 2021-2026 гг.[3]

Проведенный анализ позволяет утверждать, что как и в большинстве регионов России, в Республике Башкортостан сбыт наркотиков осуществляется в преобладающем большинстве случаев бесконтактным способом путем оборудования тайников-закладок с использованием новейших IT-технологий. Использование «темного» сегмента сети Интернет, так называемых «анонимайзеров», «криптовалютных миксеров», «теневых маркетплейсов» позволяют злоумышленникам обойти блокировку интернет-ресурсов и практически исключает возможность отслеживания соединений, финансовых операций, установления местонахождения пользователя и идентификации его личности[4].

Совершаемые в большинстве случаев дистанционные сделки по продаже и покупке наркотиков определяет стратегию и тактику действий оперативных сотрудников по выявлению лиц, причастных к незаконной деятельности.

В целях повышения эффективности противодействия кибернаркопреступности специализированные подразделения по противодействию наркоугрозе в сети Интернет и организованной преступной деятельности созданы в Управлении по контролю за оборотом наркотиков МВД по РБ (приказ МВД по РБ от 05.12.2019 №922) и Отделе по контролю за оборотом наркотиков Управления МВД России по г.Уфе (приказом МВД по РБ от 14.05.2021 № 394). Кроме того, еще в 17 территориальных ОВД на территории региона функционируют подразделения наркоконтроля, в задачи которых с учетом преобладающего объема дистанционных сделок с наркотиками также

---

[1] Подробнее см.: Дремлюга Р.И. Интернет-преступность : моногр. – Владивосток : Изд-во Дальневост. ун-та, 2008. – 240 с. – ISBN 978-5-7444-2114-4. – текст: непосредственный.

[2] Указ Президента РФ от 23.11.2020 №733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2030 года» // Официальный портал правовой информации. URL: www.pravo.gov.ru.

[3] Постановление Правительства Республики Башкортостан от 02.10.2020 № 586 (ред. от 30.12.2021) «Об утверждении государственной программы "Обеспечение общественной безопасности в Республике Башкортостан"» // Официальный интернет-портал правовой информации Республики Башкортостан. URL: www.npa.bashkortostan.ru..

[4] Детков А.А. Актуальные проблемы документирования бесконтактного сбыта наркотических средств // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : материалы двадцатой международной научно-практической конференции / под ред. Д.Л. Проказина. – Барнаул : Барнаульский юридический институт МВД России, 2022. – Ч. 1. С. 14-15.

входит противодействие кибернаркопреступности.

Создание вышеуказанных специализированных подразделений по противодействию кибернаркопреступности способствовало повышению эффективности в данном направлении деятельности. Так, в 2022 г. ОВД республики выявлено 2266 (+473) и раскрыто 975 (+165) кибернаркопреступлений соответственно. Показатель раскрываемости по ним составил 45,3% (в 2021 г. 44,5%). В их числе выявлено 1529 (+324) подобных преступлений, связанных со сбытом наркотиков, раскрыто 224 (+26).

В 2022 г. МВД по Республике Башкортостан раскрыто 59 эпизодов преступной деятельности, совершенных 44 участниками в составе 9 организованных групп и преступных сообществ, осуществлявших бесконтактный сбыт наркотиков через интернет-магазины «Zfermer», «Король специй», «Пират», «Мила Ричи». «Караван», «Бламо», «Ланкастер» посредством оборудования тайников-закладок на территории региона.

Особенно необходимо отметить достигнутые результаты в выявлении и раскрытии наркопреступлений, совершенных в составе преступного сообщества. Так, в 2022 г. в суд направлено уголовное дело в отношении 5 участников преступного сообщества по 20 эпизодам их преступной деятельности, включая организацию преступного сообщества и легализацию доходов от наркобизнеса на сумму 1,874 млн рублей. Для сбыта наркотиков на территории Башкортостана (7 эпизодов), Татарстана и Удмуртии, Краснодарского края, Белгородской, Волгоградской, Воронежской, Нижегородской, Пензенской, Ростовской, Самарской, Саратовской и Челябинской областей преступники, у которых в 2021 г. было изъято 14,9 кг наркотиков, использовали интернет-магазин «Zfermer».

В 2022 г. сотрудниками ОВД республики пресечена деятельность пяти подпольных лабораторий в Иглинском (март, ноябрь), Аургазинском (июль), Бирском (август) и Уфимском (ноябрь) районах, организаторы которых занимались синтезом и сбытом через различные интернет-магазины наркотических средств мефедрон (4-метилметкатинон) и α-пирролидиновалерофенон (α-PVP), а также выращиванием конопли с высоким содержанием тетрагидроканнабинола.

Тенденция развития кибернаркопреступности сочетается с тенденцией увеличения доли синтетических наркотиков в общей структуре изъятых органами внутренних дел наркотических средств и психотропных веществ. Так, за 2022 г. доля «синтетики» в общей массе изъятых ОВД психоактивных веществ составила с 46,4% до 58,0%.

Мероприятия, направленные на выявление преступлений, совершенных с использованием ИТТ, осуществлялись в ходе всех организованных МВД по Республике Башкортостан целенаправленных антинаркотических оперативно-профилактических операций и мероприятий: 6 этапов региональной межведомственной комплексной оперативно-профилактической операции «Мак», 3 этапа комплексного оперативно-профилактического мероприятия «Наркозаслон», по 2 этапа ОПМ «Уклонист», Общероссийской акции «Сообщи, где торгуют смертью» и «Призывник», федеральной межведомственной комплексной оперативно-профилактической операции «Дети России».

Задачам противодействия наркопреступности отвечает и проводимая МВД по РБ деятельность по пресечению пронаркотического контента в сети интернет. Так, в соответствии с постановлением Правительства РФ от 26.10.2012 № 1101, МВД по РБ осуществляется работа по противодействию распространению пронаркотического контента в сети Интернет. В т.г. сотрудниками ОВД выявлено 3870 (+1) пронаркотических сайтов, информация о которых направлена в Роскомнадзор для блокирования, доступ к 3043 (+2) сайтам ограничен.

На постоянной основе осуществляется взаимодействие с финансовыми учреждениями, банковскими структурами, налоговыми органами, интернет-провайдерами, транспортными компаниями. Однако к проблемным вопросам в данном направлении можно отнести отсутствие взаимодействия с находящимися за пределами юрисдикции Российской Федерации кредитно-финансовыми учреждениями, осуществляющими обмен криптовалют в сети «Интернет».

Таким образом, органами внутренних дел на территории Республики Башкортостан, при координирующей роли Управления по контролю за оборотом наркотиков МВД по РБ, приняты организационно-штатные и иные практические меры по активизации противодействия кибернаркопреступности, о чем свидетельствует проведенный анализ результатов по выявлению и раскрытию преступлений указанной категории. Принимаемые в настоящее время организационные меры по кадровому и материально-техническому укреплению специализированных IT-подразделений безусловно будут способствовать дальнейшему повышению эффективности деятельности в данном направлении. Однако как минимум в ближайшей перспективе будет сохраняться актуальность необходимости своевременной научной и методической проработки постоянно возникающих проблемных вопросов, связанных с организацией эффективного противодействия кибернаркопреступности.

Анализируя проблемы, стоящие перед оперативными подразделениями по борьбе с кибернаркопреступностью, следует отметить необходимость системного и своевременного совершенствования антинаркотического законодательства и укрепления технической оснащенности оперативных подразделений[1].

Литература

1. Дремлюга Р.И. Интернет-преступность : моногр. – Владивосток : Изд-во Дальневост. ун-та, 2008. 240 с. ISBN 978-5-7444-2114-4. – текст: непосредственный.
2. Детков А.А. Актуальные проблемы документирования бесконтактного сбыта наркотических средств // Актуальные проблемы борьбы с

[1] Подробнее см.: Билоус Е.Н., Кублова М.Г. Актуальные проблемы противодействия преступлениям по линии незаконного оборота наркотиков с использованием информационно-телекоммуникационных сетей и пути их решения // Криминалистика: вчера, сегодня, завтра. 2022 № 2 (22). С. 7-16

преступлениями и иными правонарушениями : материалы двадцатой международной научно-практической конференции / под ред. Д.Л. Проказина. Барнаул : Барнаульский юридический институт МВД России, 2022. Ч. 1. С.14-15.
3. Билоус Е.Н., Кублова М.Г. Актуальные проблемы противодействия преступлениям по линии незаконного оборота наркотиков с использованием информационно-телекоммуникационных сетей и пути их решения // Криминалистика: вчера, сегодня, завтра. 2022 № 2 (22). С. 7-16
4. Постановление Правительства Республики Башкортостан от 02.10.2020 № 586 (ред. от 30.12.2021) «Об утверждении государственной программы "Обеспечение общественной безопасности в Республике Башкортостан"» // Официальный интернет-портал правовой информации Республики Башкортостан. URL: www.npa.bashkortostan.ru.
5. Указ Президента РФ от 23.11.2020 №733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2030 года» // Официальный портал правовой информации. URL: www.pravo.gov.ru.

И. Н. Озеров,
А. М.Журбенко

Использование цифровых следов в раскрытии и расследовании преступлений в финансово-кредитной сфере

Аннотация. В статье представлено определение понятия цифрового следа и его описание, рассмотрены информационные возможности обнаружения и использования цифровых следов несущих криминалистически значимую информацию о преступлении для последующего раскрытия и расследования. Представлена классификация экономических следов в информационном пространстве.

Ключевые слова: цифровой след, финансово-кредитная система, интернет-пользователь.

В настоящее время информационно-технологический прогресс имеет довольно высокий, при этом постоянный темп развития. Его влияние распространяется абсолютно на все сферы жизни общества. При этом, помимо повышения качества жизни, данный процесс имеет и свои отрицательные черты. С появлением новых технологий и информационных ресурсов, появляются новые способы совершения преступлений. Это послужило толчком перехода совершения преступлений в кредитно-финансовой сфере с использованием информационного пространства.

Актуальность выбранной темы исследования обусловлена формированием методики использования цифровых следов, оставленных при совершении преступления в финансово-кредитной сфере, с целью дальнейшего раскрытия и расследования преступлений. Эффективность расследования преступлений в

финансово-кредитной сфере в основном подчинена скорости принятия решений о производстве следственных и иных действий, направленных прежде всего, на обнаружение и фиксацию доказательств в электронном виде [5].

Как было на протяжении всего существования человечества, преступники очень быстро осваивают новые сферы, с целью понижения вероятности обнаружения их деятельности правоохранительными органами. Так случилось и с внедрением в жизнь общества новейших технологий. Преступный элемент очень быстро освоил данную сферу, что, в последствии формирует новый вызов для сотрудников правоохранительных органов. Так освоение информационно-технологической сферы повлекло трансформацию преступной деятельности в экономической сфере, а следовательно цифровизации преступлений в финансово-кредитной сфере.

Для формирования общего представления о состоянии преступности в рассматриваемой нами сфере, обратимся к отчету Главного информационно-аналитического центра МВД России. Согласно отчету указанного центра, за 2022 год, доля преступлений, которые были совершены посредством применения цифровых технологий в экономической сфере, выросла на 7.1%, но эта цифра меркнет перед темпом роста общих преступлений в информационно-телекоммуникационной сфере, он составил 51.1% [6].

Для того, чтобы как можно подробнее раскрыть выбранную тему исследования, необходимо дать понятие такому элементу рассматриваемого преступления, как цифровой след.

На сегодняшний день, определение цифрового следа можно сформулировать в виде определенной совокупности информации, которую, непосредственно, пользователи сети Интернет размещают на просторах информационного пространства, при этом, указанная информация, как правило, содержит данные о самом пользователе, который ее предоставляет. Подобная информация образуется, прежде всего, при посещении лицом почтовых онлайн-сервисов, различного рода приложений и сайтов, а также, в результате использования социальных сетей и мессенджеров. При этом, указанное выше определение, не является юридически закрепленным, а представляет собой лишь понятие цифрового следа в рамках повседневной жизнедеятельности человека. Однако, на законодательном уровне, все же существует информация о данном элементе. Так, Концепцией комплексного регулирования в сфере цифровой экономики приводится следующая классификация цифрового следа:

- активный след (представляет собой данные пользователя, которые он, в результате посещения сайтов, использования приложений, социальных сетей и мессенджеров, осознанно и намеренно оставляет на просторах указанных ресурсов);

- пассивный след (данные, которые оставлены пользователем в результате посещения различных сайтов, как правило, в результате соглашения с политикой использования тех или иных ресурсов, а также, данные, которые сохраняются на просторах информационного пространства в результате использования всевозможного программного обеспечения, требующего подключения к сети

Интернет. При этом, главной особенностью в данном случае, выступает факт ненамеренного предоставления персональных данных пользователем).

Однако, предоставленный перечень не является исчерпывающим, а представляет лишь ту классификацию, которую предоставляет нам действующее законодательство Российской Федерации. Однако, современные ученые и юристы выделяют еще ряд классификаций, а также представляют свое понятие цифрового следа. Рассмотрим часть классификаций, а также определение цифрового следа, чтобы как можно подробнее разобраться в данном вопросе.

Ряд юристов, таких как Бычков В.В., Багмет А.М., Скобелин С.Ю., Ильин Н.Н. рассматривая цифровой след в рамках криминалистического понимания, представляют его в виде абсолютно любой информации, которая представлена в виде различных электронных сигналов, при этом не зависимой от способов ее хранения, передачи и обработки, но являющейся криминалистически значимой. Стоит сказать, что данное определение никак не исключает сферу использования цифрового следа на просторах различных информационно-телекоммуникационных сетей, а лишь передает ее компьютерную природу существования. Однако, подобная формулировка имеет огромное значение для криминалистики, так как позволяет отнести к цифровым следам, не только данные, которые были использованы на просторах информационной сети, но и те, которые были созданы, обработаны и переданы без непосредственного использования Интернет-соединения.

Далее рассмотрим ряд классификаций, которые были даны вышеуказанными лицами.

По месту хранения:

- на различных съемных носителях, таких как USB флеш-накопителях, съемных SSD- и HDD- дисках и так далее;
- в памяти компьютерных систем, а также информационных сетей.

В зависимости от образа цифрового следа:

- образцы, которые представлены в виде того или иного информационного продукта, например, в виде скриншота сайта, или растрового изображения с информацией о пользователе;
- образцы, предоставленные в виде бумажного носителя, например, информация о различных транзакциях, распечатанная на листе [1].

Однако, в рамках криминалистического исследования цифрового следа, наибольшую значимость для дальнейшего раскрытия и расследования преступлений, представляет следующая классификация:

- электронные образцы документов, а именно бухгалтерских учетов, договоров, а также печатные копии указанных документов;
- информационные данные, содержащие в себе интернет-ресурсы, которые являются доказательством о ведении преступниками экономической деятельности. Подобными данными, например, могут выступать каталоги товаров, размещенные на сайтах, скриншоты, передающие содержимое того или иного интернет-магазина и т.д.

- данные, полученные из мессенджеров или различных социальных сетей с информацией о совершении каких-либо транзакций или других операций в экономической сфере;

- данные о финансовых активах, принадлежащих преступнику, предоставленные в цифровом виде [2].

Рассмотрев понятия цифрового следа и его классификации, перейдем к рассмотрению процесса расследования и раскрытия преступлений в финансово-кредитной сфере с использованием в процессе раскрытия указанного вида следов на территории нашей страны.

Следует сказать, что большая часть финансовых операций в информационной среде, на территории России, происходит посредством использования программного обеспечения, на базе 1С-программирования. Так, указанные операции, как правило, формируются в виде определенных бухгалтерских учетов, которые, в свою очередь, формируются в программе «1С:Предприятие».

Получение доступа к электронному файлу подобного образца предоставляет сразу ряд цифровых следов, которые в дальнейшем могут оказать довольно большую помощь в раскрытии преступления.

Во-первых, файлы указанного формата несут в себе информацию о различных экономических регистрах, базах данных и учетах, которые могут использоваться для определения круга подозреваемых, а также выявления счетов, на которые поступали или с которых переводились денежные средства.

Во-вторых, исходный код файла, может нести информацию о цифровом устройстве, с которого производилось его создание, обработка и дальнейшие передача или хранение, вплоть до IP-адреса устройства.

Далее, в зависимости от полученной информации, может быть несколько путей развития расследования, рассмотрим каждый из них.

При получении названий организаций, информации о лицах или счетах, сотрудниками оперативных подразделений могут использоваться блокчейн-технологии. Они позволяют отследить финансовые транзакции на всем пути их следования, с момента отправки до момента получения на определенный счет или снятия наличными. Так, например, большинство информационных преступлений в финансово-кредитной сфере, основаны на мошеннических действиях. Использование блокчейн-технологий позволяет не только определить конечный счет, на который поступили денежные средства, но получить информацию о данных лица, которому принадлежит этот счет, либо же IP-адрес устройства, через которое осуществлялись мошеннические действия.

Однако, следует упомянуть, что ряд действий может производиться лишь по судебному решению, во избежание нарушения прав человека, установленных Конституцией Российской Федерации [4].

В случае с обнаружением данных об устройстве, с которого производились преступные действия, сотрудниками полиции могут проводиться биллинговые мероприятия. Они позволяют отследить точное местоположение устройства, с которого, непосредственно, производилось подключение к сети Интернет, а, следовательно, определить адрес лица, которому принадлежит данное устройство и непосредственно сузить круг подозреваемых лиц до минимума [2].

Мы считаем, что для более простого использования технологии сбора и систематизации информации об интернет-пользователях достаточно обратиться к уже созданным технологиям отечественных IT- компаний. Согласно представленной информации о сервисе «Яндекс Крипта» предназначенного для сбора рекламодателям таких важных метаданных об интернет-пользователях как возраст, место проживания, доход, интересы и т.д. [3].

Однако, рассмотренные выше примеры, являются лишь последовательностью действий сотрудников полиции, при наличии у них каких-либо первоначальных данных. При этом, для получения подобных данных из имеющихся электронных документов, необходимо проведения целого ряда экспертиз, что занимает довольно длительное время, в виду чего, расследование и раскрытие подобных преступлений является довольно длительным и трудоемким процессом.

Подводя итоги проведенному исследованию, можно сделать вывод, что обнаружение цифровых следов в результате расследования и раскрытия преступлений в сфере финансово-кредитных операций, на сегодняшний день, является важным элементом, позволяющим значительно ускорить процесс раскрытия преступления в данной сфере, при правильном использовании полученных следов и хранящихся в них информации.

Литература

1. Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н. Цифровые следы преступлений: монография. М.: Проспект, 2021. С. 168.
2. Буйнов Д.О. Виды цифровых следов преступлений в сфере экономической деятельности и особенности их исследования экспертом: М.: Актуальные проблемы российского права, 2022. 140-149 с.
3. Журбенко А.М., Махмутов А.Р. К вопросу о формировании единого банка цифровых следов интернет – пользователей для раскрытия преступлений // Сборник материалов международной научно-практической конференции, посвященной 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ. В 2-х частях. Орел, 2022. 143-146 с.
4. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 04.07.2020 – Текст: электронный.
5. Озеров И.Н., Журбенко А.М. Некоторые криминалистические аспекты расследования преступлений в финансово-кредитной сфере // Журнал.: Актуальные проблемы борьбы с преступлениями и иными правонарушениями, Барнаул, 2022. 227-229 с.
6. Состояние преступности в Российской Федерации за 2022 г. // Главный информационно-аналитический центр МВД РФ. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 16.04.2022).

Н.В. Османова

Некоторые аспекты уголовного судопроизводства по делам о киберпреступлениях

Аннотация. В статье приводятся некоторые аспекты уголовного преследования по уголовным делам о киберпреступлениях. Отмечаются особенности начала уголовного судопроизводства по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, определения места производства расследования, доказывания по уголовным делам, взаимодействия следователя с органами дознания, администрацией социальных сетей, мессенджеров при расследовании преступлений.

Ключевые слова: уголовное преследование, киберпреступление, начало уголовного судопроизводства, поводы возбуждения уголовного дела, место совершения преступления, информационные и телекоммуникационные технологии.

Уголовное судопроизводство по уголовным делам о киберпреступлениях характеризуются особенностями начала уголовного судопроизводства по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, определения места производства предварительного расследования, доказывания по уголовным делам, взаимодействия следователя с органами дознания, администрацией социальных сетей, мессенджеров при расследовании преступлений. Указанное обусловило не только криминалистические особенности выявления, раскрытия, расследования таких преступлений [3, 68], но и внесение соответствующих изменений в уголовно-процессуальный закон (ст. 186.1, 164 УПК РФ).

Особенности уголовного судопроизводства по уголовным делам о преступлениях, совершенных с использованием современных информационных и телекоммуникационных технологий, обусловлены:

– началом процессуальной проверки по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий;

– уголовно-процессуальной спецификой определения места производства расследования;

– предметом доказывания по уголовным делам о преступлениях, совершенных с использованием современных информационных и телекоммуникационных технологий;

– особой процедурой изъятия электронных носителей информации и копирования с них информации при производстве следственных действий;

– производством контроля и записи переговоров, получением информации о соединениях между абонентами и (или) абонентскими устройствами;

– обязательным взаимодействием следователя с органами дознания, администрацией социальных сетей, мессенджеров при расследовании преступлений.

Остановимся на некоторых из перечисленных аспектов.

Типичными поводами возбуждения уголовного дела о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, являются:

– заявление лица о том, что в отношении него совершено преступление, например: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ); вымогательство, совершенное с использованием сети Интернет (ст. 163 УК РФ); нарушены его авторские права (ст. 146 УК РФ);

– заявление матери, отца, усыновителя, опекуна или попечителя (законного представителя) о том, что, например, совершена видеосъемка несовершеннолетнего в целях изготовления и распространения порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей (п. «г» ч. 2 ст. 242.2 УК РФ);

– рапорт об обнаружении признаков преступления, например, о незаконном сбыте наркотических средств, психотропных веществ или их аналогов, совершенном с использованием электронных или информационно-телекоммуникационных сетей (п. «б» ч. 2 ст. 228.1 УК РФ). Сеть Интернет может быть использована также для коммуникации с потенциальным покупателем, получения сведений об оплате и информирования о месте нахождения наркотических средств [2, 84]. Такие сведения в последующем (после их установления и анализа) становятся основанием для составления рапорта об обнаружении признаков преступления;

– постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании п. 4 ч. 1 ст. 140 УПК РФ. Такие материалы, как правило, формируются в ходе надзорного производства, а также по жалобам граждан.

Преступления, совершенные с использованием сети Интернет, о совершении которых становится известно правоохранительным органам посредством подачи лицом заявления, обладают высокой латентностью.

Особый способ совершения рассматриваемых преступлений позволяет скрыть или намеренно исказить идентификационные данные, что обусловливает достаточно редкую встречаемость в правоприменительной практике добровольного письменного или устного сообщения лица о совершенном им преступлении (явки с повинной) в качестве повода для возбуждения уголовного дела (п. 2 ч. 1 ст. 140 УПК РФ).

Особенностью проведения проверки по сообщению о преступлении и дальнейшего предварительного расследования является установление места нахождения указанных выше предметов и объектов и их значения в установлении обстоятельств, подлежащих доказыванию.

В досудебном производстве по уголовным делам о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, нередко возникают вопросы, связанные с определением места

производства предварительного расследования и субъекта уголовного преследования. При поступлении сообщения о преступлении необходимо решить вопрос о территориальной подследственности. В соответствии со ст. 152 УПК РФ предварительное расследование производится по месту совершения деяния, содержащего признаки преступления.

При совершении преступлений с использованием информационно-телекоммуникационной сети определяющим является момент окончания преступления.

С учетом сложившейся следственной и судебной практик правоприменители преимущественно ориентируются на место нахождения IP-адреса, с которого осуществлялись противоправные действия. Если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них.

При соединении в одном производстве уголовных дел о совершенных с использованием информационно-телекоммуникационных технологий преступлениях, подследственных разным органам предварительного расследования, подследственность определяется прокурором с соблюдением подследственности, установленной ст. 151 УПК РФ. Споры о подследственности уголовного дела разрешает прокурор.

Предварительное расследование может также производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков.

Если преступление совершено вне пределов Российской Федерации, то место производства по уголовному делу определяется с учетом правил привлечения к уголовной ответственности (ст. 12 УК РФ) и требований ст. 459 УПК РФ по месту жительства или месту пребывания потерпевшего в Российской Федерации, либо по месту нахождения большинства свидетелей, либо по месту жительства или месту пребывания обвиняемого в Российской Федерации, если потерпевший проживает или пребывает вне пределов Российской Федерации.

При расследовании уголовных дел о преступлениях, объективная сторона которых выражается в размещении в информационно-телекоммуникационной сети запрещенной информации, могут быть выявлены обстоятельства, являющиеся основаниями для изменения территориальной подследственности. По мнению А.А. Казакова необходимость применения ч. 4 ст. 152 УПК РФ может быть обусловлена случаями, когда место выхода в сеть не совпадет с местом жительства подозреваемого (обвиняемого). В ситуациях, когда размещенные в сети сведения носили строго адресный характер, в зависимости от установленных обстоятельств, а также при необходимости собирания доказательств по месту жительства потерпевшего (демонстрировавшего переписку родственникам и знакомым, делившегося с ними переживаниями и т.д.) предварительное расследование может производиться по месту нахождения потерпевшего [1, 159].

При совершении преступлений с использованием информационно-телекоммуникационных технологий с разных IP-адресов (территориально

удаленных друг от друга), направленных на причинение вреда сразу нескольким потерпевшим, целесообразно рассмотреть вопрос о производстве предварительного следствия следственной группой (ст. 163 УПК РФ), о чем выносится отдельное постановление или указывается в постановлении о возбуждении уголовного дела. К работе следственной группы также могут быть привлечены сотрудники органа дознания, осуществляющего оперативно-розыскную деятельность и, как правило, специализирующегося на раскрытии IT-преступлений. Особенностью формируемых для расследования таких преступлений следственно-оперативных групп является применение для обеспечения их скоординированных действий территориально-обособленных подгрупп, которым поручено расследование преступлений, совершенных на определенной территории.

При определении места производства расследования следует также учитывать изменения, внесенные Федеральным законом от 07.04.2020 № 112-ФЗ в ч. 4.1 ст. 152 УПК РФ, согласно которым: «Если преступление совершено вне пределов Российской Федерации, уголовное дело расследуется … по месту, определенному Председателем Следственного комитета Российской Федерации, при условии, что преступление совершено иностранным гражданином или лицом без гражданства, не проживающими постоянно в Российской Федерации, и направлено против интересов Российской Федерации».

В любом случае решение об изменении подследственности должно быть мотивированным с конкретным указанием конкретных фактических данных и в соответствии с уголовно-процессуальным законом.

Доказательства по уголовным делам о рассматриваемых преступлениях могут иметь признаки как вещественных доказательств (ст. 81 УПК РФ), так и иных документов (ст. 84 УПК РФ).

Выявление, раскрытие и расследование преступлений, совершенных с использованием информационных и телекоммуникационных технологий, характеризуется наличием вещественных доказательств в виде предметов и документов, которые служили средствами для обнаружения преступления и установления обстоятельств уголовного дела (п. 3 ч. 1 ст. 81 УПК РФ).

К таким доказательствам могут быть отнесены:

– пользовательское оборудование (оконечное оборудование): персональный компьютер, мейнфрейм, устройство сбора данных, приёмник сигналов глобальной навигационной системы или любое другое оборудование, способное передавать или принимать данные;

– сетевые аппаратные средства: серверы, рабочие станции, активное оборудование, сетевые кабели и т.п.;

– компьютерная информация – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание 1 к ст. 272 УК РФ);

– документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами;

– материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

– запоминающие устройства и носители данных: микросхемы памяти, магнитные и лазерные диски, флэш-карты и т.п.;

– системное программное обеспечение (операционные системы) и другие доказательства.

Иные документы как доказательства по уголовному делу могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут быть отнесены материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации.

Всеобщая информационная глобализация требует от следователя наличие специальных знаний в области информационных технологий, что порой вызывает трудности. Профессор А.С. Шаталов отмечает одну из главных особенностей преступлений, совершенных с использованием современных информационных технологий: их предотвращение, выявление, раскрытие и расследование невозможно без современных информационных технологий. В связи с чем возникла необходимость подготовки специалистов для борьбы с такими преступлениями, переподготовке действующих кадров с тем, чтобы разоблачать преступников посредством обнаружения, фиксации, изъятия и использования разного рода «электронных доказательств» [3, 70]. Осознавая потребности практических сотрудником, законодателем было предусмотрено участие специалиста при изъятии электронных носителей информации (ч. 2 ст. 164.1 УПК РФ).

Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

К специальным процессуальным средствам, позволяющим установить обстоятельства, подлежащие доказыванию, также относятся получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) и производство контроля и записи переговоров (ст. 186 УПК РФ).

Согласно ч. 8 ст. 186 УПК РФ на основании постановления следователя фонограмма в полном объеме приобщается к материалам уголовного дела как вещественное доказательство и хранится в опечатанном виде в условиях, обеспечивающих ее сохранность и возможность повторного прослушивания.

Об осмотре и прослушивании фонограммы составляется протокол. В данном протоколе дословно должна быть изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к делу.

Взаимодействие следователя с органами дознания, администрацией социальных сетей, мессенджеров. Собирание доказательств по уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий, может осуществляться следователем также путем производства иных процессуальных действий. Иные процессуальные действия, направленные на собирание доказательств, предусмотрены законом, но в отличие от следственных действий процедура их производства детально не регламентирована. Так, ч. 4 ст. 21 УПК РФ, например, устанавливает правило, согласно которому требования, поручения и запросы следователя, предъявленные в пределах его полномочий, установленных уголовно-процессуальным законом, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ч. 3.1 ст. 10.1) организатор распространения сведений в сети Интернет обязан предоставлять информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

К такой информации относятся: (а) информация о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информация об этих пользователях в течение одного года с момента окончания осуществления таких действий; (б) текстовые сообщения пользователей сети Интернет, голосовая информация, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет. Такие сообщения хранятся до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения информации устанавливаются Правительством Российской Федерации.

Рассмотренные особенности уголовного судопроизводства по делам о киберпреступлениях обусловлены необходимостью принятия ответных мер в отношении происходящих преступных явлений в современных условиях всеобщей компьютеризации и информатизации общества при условии соблюдения прав граждан и соблюдения соотношения интересов частных и публичных.

Литература

1. *Казаков А.А.* Об определении территориальной подследственности по уголовным делам о преступлениях экстремистской направленности // Расследование преступлений: проблемы и пути их решения. 2018. № 2(20). С. 157-159.
2. *Торговченков В.И., Иванов С.А.* Особенности предупреждения бесконтактных способов сбыта наркотических веществ в Российской Федерации // Законы России: опыт, анализ, практика. 2016. № 12. С 84-88.

3. *Шаталов А.С.* Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 68-83.

Н.В. Павловская

Актуальные проблемы противодействия кибермошенничеству

Аннотация. В статье рассматриваются результаты анализа данных правовой статистики, отражающие современную криминальную ситуацию, связанную с мошенничеством, совершаемым с использованием информационно-телекоммуникационных технологий. Исследуются данные социологических исследований, свидетельствующие о расширении масштабов распространения данного вида преступности. Приводятся результаты изучения экспертного мнения относительно состояния и основных причин виктимизации, связанной с телефонным и интернет-мошенничеством. Особое внимание уделяется вопросам виктимологической профилактики и предупреждения данного вида преступности.

Ключевые слова: преступность, мошенничество, информационно-коммуникационные технологии, жертвы преступлений, противодействие преступности, предупреждение преступности, виктимологическая профилактика

Глобализация информационного пространства с каждым годом оказывает все более заметное влияние на нашу повседневную жизнь, охватывая практически все сферы жизни современного общества, открывая новые возможности для обучения, работы, облегчает и ускоряет процессы получения финансовых услуг и т.д. По данным Росстата, сетью «Интернет» в России пользуются 88,6% граждан[1] и 86,6% организаций[2]. Растет доля продаж через Интернет в объеме оборота розничной торговли[3], что подтверждают и данные социологических исследований. Так, более половины россиян, имеющих опыт приобретения товаров и услуг через Интернет, стали чаще совершать онлайн-покупки за последние один-два года (55%)[4]. В тоже время в условиях информационной глобализации существенно возрастают криминальные угрозы и риски. Особенно ярко эти тенденции проявляются в развитии криминальной ситуации, связанной с мошенничеством.

Результаты проводимых исследований показывают, что с каждым годом мошенничество становится все более распространенным. Почти каждое шестое

[1] URL: https://rosstat.gov.ru/storage/mediabank/lqv3T0Rk/info-ob2020.pdf (дата обращения: 22.03.2023).
[2] URL: https://rosstat.gov.ru/storage/mediabank/tJdNU3uy/ikt_3.xls (дата обращения: 22.03.2023).
[3] URL: https://rosstat.gov.ru/storage/mediabank/Internet_torgovlya_12.xlsx (дата обращения: 22.03.2023).
[4] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/pokupki-v-internete-doverie-protiv-moshennichestva (дата обращения: 22.03.2023).

зарегистрированное в Российской Федерации преступление – это один из видов мошенничества (ст. 159–159^6 УК РФ). Ежегодно их суммарное количество превышает 330 тыс. деяний. Современные мошенники активно используют методы социальной инженерии, приспосабливаются к происходящим изменениям в политической обстановке, экономической ситуации, законодательном регулировании, учитывают актуальные социальные настроения и страхи, умело пользуются современными информационными технологиями и средствами мобильной связи, компьютерной и иной техникой. Сейчас одни только деяния, предусмотренные ст. 159 УК РФ, занимают почти половину всего массива зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (в 2022 г. – 47,9%). В современных исследованиях такие преступления обычно именуют кибермошенничеством.

Статистические данные свидетельствуют о неуклонном увеличении количества таких деяний, хотя темпы его прироста за последние два года значительно сократились (если в 2020 г. регистрировалось свыше 210 тыс. преступлений данного вида, +75,6% в сравнении с предыдущим годом, то в 2021 г. – свыше 238 тыс., +13,3%, в 2022 г. – свыше 257 тыс., +4,8%). Об увеличении интенсивности телефонного и интернет-мошенничества в прошедшем году свидетельствуют и данные социологических опросов. Так, по сравнению с 2021 г. число опрошенных ВЦИОМ, сталкивавшихся с мошенническими звонками и СМС-сообщениями, возросло с 76% до 83%[1]. Близкие результаты показали опросы Аналитического центра НАФИ: в апреле 2022 г. 58% респондентов заявляли, что сталкивались с попытками мошенничества, а в октябре – уже 82%, при этом самым распространенным видом дистанционного мошенничества стали предложения в сети «Интернет» заработать на «инвестициях» – с ними сталкивались 55% опрошенных респондентов, этот вид обмана обогнал даже звонки от сотрудников «банка» или «правоохранительных органов»[2].

Большое значение в связи с этим получают исследования, направленные на изучение виктимологических аспектов кибермошенничества. Результаты изучения портрета жертв подобных преступлений позволят установить усредненные, типичные их социально-демографические признаки, характерные психологические особенности, наиболее распространенные причины виктимизации и могут служить научной основой для разработки специальных рекомендаций по осуществлению профилактических мероприятий. По статистике, общее число потерпевших от преступлений, предусмотренных статьями 159–159^6 УК РФ превышает 350 тыс., из них около 90% составляют физические лица, 10% приходится на юридических лиц. Потерпевшими от мошенничества женщины становятся чуть чаще, чем мужчины (55,4%

[1] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-i-kak-s-nim-borotsja (дата обращения: 20.01.2023).

[2] URL: https://nafi.ru/analytics/82-rossiyan-stalkivalis-s-popytkami-moshennichestva/ (дата обращения: 22.03.2023).

потерпевших и 44,6% соответственно). В тоже время опрошенные эксперты[1] оценивают виктимность женщин более высоко, в качестве наиболее типичных жертв телефонного и интернет-мошенничества их указали 87,8% респондентов. Это может свидетельствовать о том, что женщины реже обращаются в правоохранительные органы с сообщением о совершенном в отношении них преступлении. Наиболее массовую возрастную группу потерпевших от мошенничества, согласно статистическим данным, составляют лица 30-49 лет (42,1%). Еще 14,5% приходится на лиц в возрасте 50-59 лет, а 10% – на молодежь (18-24 лет). В общем числе потерпевших от мошенничеств пенсионеры по старости занимают около четверти (24,2%). При этом полученные в ходе проведения исследования экспертные оценки также несколько отличаются от данных статистики. Более половины опрошенных (53,1%) считают, что чаще всего жертвами преступных посягательств данного вида становятся именно пожилые люди (старше 60 лет), или люди старшего возраста (50-59 лет) – так ответили 42% респондентов.

Увеличивает риск виктимизации, по мнению опрошенных экспертов, отсутствие семьи – чаще всего жертвами телефонных и интернет-мошенников становятся одинокие люди (так считают 68,7% респондентов). Оценивая материальное положение потерпевших, большинство опрошенных экспертов высказали мнение, что это, как правило, люди с низким уровнем доходов (85,6%). Опрошенные в целом невысоко оценивают уровень образования потерпевших от преступлений рассматриваемого вида, при этом две трети экспертов назвали низким уровень компьютерной, правовой и финансовой грамотности большинства жертв таких преступлений (65,8%). Именно недостаток знаний и опыта в этих сферах большинство опрошенных считает основной причиной виктимизации жертв телефонного и интернет-мошенничества (66,7%).

Следует обратить внимание, что результаты исследования показывают, что в настоящее время гражданами в значительной мере недооцениваются имеющиеся возможности по самостоятельной защите от мошенников. С этим согласны также пятая часть опрошенных в ходе проведения исследования экспертов (20,1%). Подтверждают данный вывод социологические опросы, а также результаты иных криминологических исследований. Так, только 35% опрошенных пользуются специальными приложениями для защиты от спам-звонков, нежелательных звонков или приложениями, которые определяют незнакомые входящие номера на своем мобильном телефоне, причем среди лиц 60 лет и старше этот показатель еще ниже – только 17%[2]. Исследование, проведенное Простосердовым М.А., свидетельствует, что типичным для жертв мошенничеств, совершенных киберпространстве, является наличие низкой культуры информационной безопасности, пренебрежение средствам

[1] В 2022 г. по специально разработанным анкетам опрошены в качестве экспертов 554 прокурорских работников.

[2] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-i-kak-s-nim-borotsja (дата обращения: 20.01.2023).

компьютерной защиты (антивирусами) либо использование контрафактных средств защиты[1]. Родина Е.А. отмечает, что криминальная виктимизация пользователей сети «Интернет» в киберпространстве обусловлена в том числе недостаточностью предпринимаемых жертвами мер для сохранения конфиденциальной информации, незнанием или игнорированием ими базовых требований безопасности в киберпространстве, таких как необходимость своевременного обновления программного обеспечения компьютеров, недопустимость использования простых или одинаковых паролей для разных сервисов[2]. Исследователями отмечаются такие типичные психологические качества жертв кибермошенничества, как чрезмерная доверчивость, небрежность и легкомысленность, достаточно частым аспектом в поведении жертвы выступает корыстная направленность (стремление приобрести товар дешевле, обойти системы дополнительных платежей, избавиться от затрат и т.д.), они легко поддаются влиянию, внушаемы, для них характерно стремление получить максимальную выгоду с минимальными затратами[3].

Соответственно среди наиболее действенных мер противодействия рассматриваемым видам мошенничества на первое место опрошенные эксперты поставили правовое просвещение, повышение финансовой и компьютерной грамотности граждан (53,9% опрошенных). Эффективность постоянного информирования граждан о существующих способах совершения мошеннических действий, новых схемах и методах, используемых мошенниками, отметили 53,7%. Подобные мероприятия уже сейчас активно реализуются органами российской прокуратуры. Так, в 2022 г. проведено свыше 31 тыс. мероприятий по правовому просвещению, касающихся вопросов противодействия преступности в сфере использования информационно-коммуникационных технологий.

Следует отметить, что в прошедшем году в России принята специальная Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации[4], реализация которой, как ожидается, будет способствовать непосредственному повышению уровня грамотности широких слоев населения страны по вопросам информационной безопасности, сокращению финансового, морально-психологического и репутационного ущерба представителей широких слоев населения от преступлений, совершаемых с использованием информационно-коммуникационных технологий, сохранности их персональных данных, повышению уровня доверия к цифровым сервисам, и в целом – дальнейшей цифровизации экономики

---

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. … канд. юрид. наук. М., 2016. С. 25.

[2] Родина Е.А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве : автореф. дис. … канд. юрид. наук. Саратов, 2022. С. 10-11.

[3] Стяжкина С.А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 3. С. 549.

[4] Распоряжение Правительства Российской Федерации от 22.12.2022 № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации».

Российской Федерации.

Кроме того, в прошедшем году в Российской Федерации принят ряд дополнительных мер по совершенствованию организации борьбы с киберпреступностью. Так, в структуре центрального аппарата МВД России образовано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий[1], усовершенствован порядок межведомственного взаимодействия МВД России с Банком России в ходе расследования уголовных дел[2]. Одним из действенных способов предупреждения киберпреступлений является распространяющаяся в настоящее время практика возбуждения органами прокуратуры дел об административных правонарушениях в отношении недобросовестных операторов сотовой связи, которые не препятствуют осуществлению инициированных иностранным оператором соединений с подменой номеров и не прекращают оказание услуг по предоставлению связи и пропуску трафика в свою сеть[3].

В заключении следует отметить, что упомянутые проблемы противодействия кибермошенничеству затрагивают лишь некоторые аспекты исследуемой темы. Многочисленные предложения по совершенствованию противодействия данному виду преступности постоянно находятся в центре внимания российского общества, активно обсуждаются в СМИ, научном сообществе, прорабатываются правоохранительными и иными заинтересованными органами. По экспертным оценкам, результатам проводимых исследований можно сделать вывод, что актуальность и значимость проблем противодействия преступности данного вида в ближайшем будущем будет лишь возрастать, что обусловливает необходимость дальнейшего развития научных исследований в этой области.

Литература

1. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. … канд. юрид. наук. М., 2016. 28 с.
2. Родина Е.А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве : автореф. дис. … канд. юрид. наук. Саратов, 2022. 27 с.
3. Стяжкина С.А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2022. Т. 32, вып. 3. С. 546–552.

[1] Указ Президента Российской Федерации от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации».

[2] Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона "О банках и банковской деятельности" и статью 27 Федерального закона "О национальной платежной системе"».

[3] URL: https://rg.ru/2023/03/13/shtrafy-po-zvonku.html (дата обращения: 22.03.2023).

П.С. Пастухов

Адаптация уголовно-процессуальной и технико-криминалистической деятельности к исследованию цифровых следов

Аннотация. Рост преступлений в сфере компьютерной информации и преступлений с использованием информационно-телекоммуникационных технологий порождает все большее количество цифровых следов. Действующее уголовно-процессуальное законодательство и технико-криминалистическая деятельность должны быть адаптированы к работе с цифровыми следами. В этих целях необходимо вводить понятие криминалистическое исследование документов, предметов и электронных носителей информации. Правом проводить криминалистическое исследование предлагается наделить следователя, а по его результатам составлять отчет. В случае необходимости следователь может пригласить специалиста в соответствии с действующим законодательством. Специалист по результатам криминалистического исследования должен составлять заключение специалиста.

Ключевые слова. Цифровые следы, электронные носители информации, криминалистическое исследование, отчет следователя, заключение специалиста, формирование доказательств.

Использование в преступных целях компьютерных технологий влечет образование цифровых следов преступлений в информационной инфраструктуре общества, которые могут быть самые разнообразные, от простейшего файла и заканчивая сложными программами или облачными сервисами[1]. Основной цифровой след — это файл, т.к. компьютерная информация может находится в виде файла различных форматов. Именно в файле цифровая доказательственная информация извлекается и осматривается следователем. Самым массовым цифровым следом является лог файлы т.к. он отображается с использованием устройства или программы и многократно дублируется аппаратно-программными комплексами информационно-технологических систем. Использование пользователями индивидуальных компьютерных устройств, смартфонов, банковских карт влечет образование следов в виде IP-адресов, MAC-адресов, абонентских номеров и IMEI телефона, номеров банковских карт и других идентификаторов.

С целью идентификации и (или) аутентификации физических лиц и устройств законодатель вводит понятие идентификатор, под которым понимается уникальное обозначение сведений о лице или устройстве, необходимое для определения такого лица путем применения технических и (или)

[1] Цифровые следы преступлений : монография. Багмет А.М., Скобелин С.Ю. Москва : Проспект, 2021. - 168 с.

технологических способов[1]. Понятие идентификатора пользовательского оборудования (оконечного оборудования) в п. 3.1-1 ст. 2 ФЗ О связи понимается как идентификационный номер пользовательского оборудования (оконечного оборудования), в котором предусмотрена возможность использования идентификационного модуля[2].

Для успешного раскрытия и расследования преступлений уголовно-процессуальное законодательство должно отвечать современным вызовам преступности, применять информационно-технологические способы собирания доказательств. В этих целях российское уголовно-процессуальное законодательство вводит понятие «электронные носители информации»[3]. С криминалистической точки зрения следует говорит об образовании цифровых следов, которое происходит на электронных носителях информации. Текущая ситуация борьбы с преступностью требует адаптации уголовно-процессуальной и технико-криминалистической деятельности к исследованию цифровых следов на электронных носителях информации т.к. только интеграция этих видов деятельности способна увеличить эффективность раскрытия и расследования преступлений. Эти два вида деятельности являются двумя сторонами одного процесса – доказывания. Если уголовно-процессуальная деятельность определяет компетенцию должностных лиц, устанавливает уголовно-процессуальную форму доказательств как условие их допустимости, то технико-криминалистическая деятельность является технологической основой нормативной деятельности, определяет технико-криминалистические средства и методы для собирания, фиксации, изъятия и исследования доказательственной информации, содержащейся в следах преступлений[4].

Необычность электронного носителя информации по сравнению с другими материальными объектами, на которых сохранились трасологические, биологические и иные материальные следы преступлений создает ряд проблем для органов расследования. Среди основных проблем можно выделить необходимость использования специальных знаний посредством приглашения специалиста для осмотра, копирования и извлечении доказательственной информации из электронных носителей информации, имея ввиду нехватки таких специалистов. Другой проблемой можно назвать правовые сложности

---

[1] Федеральный закон от 29.12.2022 № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"// Собрание законодательства РФ, 02.01.2023, № 1 (часть I), ст. 19.

[2] Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 02.07.2021) "О связи"//Собрание законодательства РФ. 2003, № 28, ст. 2895.

[3] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023) // – Режим доступа: http://www.consultant.ru. – Текст: электронный.

[4] Пастухов П.С., Афанасьева С.И., Добровлянина О.В., Малыгин К.В. Криминалистические возможности и уголовно-процессуальные требования к формированию электронных доказательств/ Vth Khmyrovsky Criminalistic Readings 2021. 2022, EurAsian Scientific Editions SA, Geneva, Switzerland /EurAsian Scientific Editions Ltd, Hong Kong /EurAsian Scientific Editions OÜ, Tallinn, Estonia. P.36-42.

использования заключения специалиста в качестве самостоятельного доказательства (п.3.1 ч.2 ст. 74 УПК).

Не менее важной является проблема перегруженности экспертов, исследующих цифровые следы на электронных носителях информации т.к. изъятые электронные носители информации следователи автоматически направляют на экспертное исследование независимо от их сложности. В результате такого подхода компьютерно-техническое, информационно-технологическое экспертное исследование становится «узким горлышком» процесса доказывания, что требует более длительных сроков ожидания для получения следователем экспертного заключения.

Названные трудности расследования преступлений, связанные с извлечением доказательственной информации более рациональными способами, являются основной проблемой данной статьи. Поэтому целью статьи служит выработка предложений для органов предварительного расследования оптимальных средств и методов для получения доказательственной информации из электронных носителей информации через адаптацию уголовно-процессуальной и технико-криминалистической деятельности к исследованию на них цифровых следов[1].

Для достижения заявленной цели статьи необходимо проанализировать нормативные положения уголовно-процессуального кодекса, позволяющие рационализировать деятельность органов предварительного расследования через призму адаптации уголовно-процессуальной и технико-криминалистической для исследования цифровых следов преступлений. Анализ следует начать с электронного носителя, понятие которого содержится в п. 3.1.9 ГОСТ 2.051-2013, согласно которому – это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[2]. В отличие от других материальных следов преступлений и вещественных доказательств электронный носитель информации представляет собой «контейнер», требующий особого подхода в его осмотре, исследовании и изъятии из него электронной доказательственной информации с помощью средств вычислительной техники. В этой связи возрастает роль технико-криминалистической деятельности, способствующей извлечению доказательственной информации из электронных носителей как «контейнеров». Интеграционной нормой, объединяющей два названных вида деятельности, является часть шестая статьи 164 УПК. Указанная статья определяет, что при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. В этой норме зафиксированы 3

[1] Зайцев, О. А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестник Пермского университета. Юридические науки. – 2022. – № 56. – С. 281-308. – DOI 10.17072/1995-4190-2022-56-281-309. – EDN TBDSEX.

[2] ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения. Введен в действие Приказом Росстандарта от 22.11.2013 № 1628-ст // СПС Консультант плюс.

этапа работы со следами: обнаружение, фиксация и изъятие следов преступления. Четвертый этап работы со следами называется исследование, но о нем не упоминается в ч.6 ст.164 УПК. А между тем это наиважнейший этап работы со следами т.к. в ходе исследования устанавливаются доказательственные факты.

Введенная в УПК Федеральным законом от 27.12.2018 № 533-ФЗ специальная статья (164.1. УПК), регламентирующая особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий тоже не предусматривает их исследование. Часть вторая данной статьи обязывает изымать электронные носители информации в ходе производства следственных действий с участием специалиста, наделяет следователя полномочием в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты.

Заметим, в исследовании следов преступления выделяются два вида: предварительное и экспертное. Полномочия по исследованию следов преступления можно обнаружить в п.19 ст.5 УПК, в которой раскрывается сущность определения понятия неотложных следственных действий. При определении цели неотложных следственных действий законодатель указывает – обнаружение и фиксацию следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования.

О возможности исследования документов и предметов дознавателем, органом дознания, следователем, руководителем следственного органа на этапе предварительной проверки в стадии возбуждения уголовного дела говорится в ч.1 ст. 144 УПК. Современный следователь владеет основными компетенциями в сфере информационных технологий ввиду того, что в учебных программах изучают несколько дисциплин в названной сфере, а поэтому он имеет возможность самостоятельного исследования простейших цифровых следов и электронных носителей. К таким объектам исследования можно отнести следующие цифровые следы: файлы, лог файлы, IP-адреса, MAC адреса, абонентские номера и IMEI телефонов, метаданные файлов, программ, сайтов, биллинги сотовой связи, движение денежных средств в платежных и банковских системах, данные всех систем видеонаблюдения и видео регистрации и других информационно-технологических систем.

В случаях необходимости указанные должностные лица, осуществляющие предварительную проверку наделены полномочиями привлекать к участию в этих действиях специалистов (ч.1 ст. 144 УПК). Аналогичные полномочия специалиста по участию в процессуальных действиях и разъяснению сторонам и суду вопросов, входящих в его профессиональную компетенцию предусмотрены ст. 58 УПК.

Итак, уголовно-процессуальный закон предусматривает исследование документов, предметов и электронных носителей. При этом, сложность

цифровых следов и электронных носителей информации различается от простой флешки до облачных хранилищ. В целях рационализации уголовно-процессуальной и технико-криминалистической деятельности необходимо придать более определенный статус такому исследованию и получаемых при этом уголовно-процессуальных доказательств. Во-первых, это исследование необходимо назвать криминалистическим исследованием, наделяя его самостоятельным статусом иного процессуального действия (ч.1 ст.86 УПК) как одного из активных способов собирания доказательств. Во-вторых, наделить полномочиями по проведению криминалистического исследования следователя и специалиста. По результатам криминалистического исследования цифровых следов и электронных носителей информации наделить правом следователя составлять отчет об криминалистическом исследовании, который должен отличаться от протокола осмотра указанием на: одновременное использование нескольких технических устройств и сопоставление их между собой; отмечать технические, технологические и программные аспекты; указывать координатно-временные параметры устройств и лиц (геолокация); метаданные файлов, сайтов и программ.

Если криминалистическое исследование цифровых следов и электронных носителей информации проводит приглашенный специалист, то он должен составлять заключение специалиста с указанием выше названных параметров и аспектов. В-третьих, криминалистическое исследование как иное процессуальное действие будет сочетать возможности следственного осмотра и обыска, благодаря поисковым действиям в компьютерных устройствах, базам данных и информационно-технологическим сетям, что придает этому процессуальному действию кумулятивный эффект от нескольких следственных действий.

В заключение делаем вывод о том, что, наделяя исследование документов, предметов и электронных носителей под названием криминалистическое исследование и наделив его статусом иного процессуального действия как способа собирания доказательств, позволяет формировать уголовно-процессуальные доказательства в более короткие сроки. Такой подход к практике криминалистического исследования цифровых следов на электронных носителях информации расширит возможности следователя, разгрузит судебно-экспертную деятельность, т.е. оптимизирует и рационализирует уголовно-процессуальную и технико-криминалистическую деятельность в условиях цифровой трансформации общества.

Литература

1. Федеральный закон от 29.12.2022 № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской

Федерации"// Собрание законодательства РФ, 02.01.2023, № 1 (часть I), ст. 19.
2. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 02.07.2021) "О связи"//Собрание законодательства РФ. 2003, № 28, ст. 2895.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 18.03.2023)// – Режим доступа: http://www.consultant.ru. – Текст: электронный доступ.
4. ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения. Введен в действие Приказом Росстандарта от 22.11.2013 № 1628-ст // СПС Консультант плюс.
5. Зайцев, О. А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестник Пермского университета. Юридические науки. – 2022. – № 56. – С. 281-308. – DOI 10.17072/1995-4190-2022-56-281-309. – EDN TBDSEX.
6. Пастухов П.С., Афанасьева С.И., Добровлянина О.В., Малыгин К.В. Криминалистические возможности и уголовно-процессуальные требования к формированию электронных доказательств/ Vth Khmyrovsky Criminalistic Readings 2021. 2022, EurAsian Scientific Editions SA, Geneva, Switzerland /EurAsian Scientific Editions Ltd, Hong Kong /EurAsian Scientific Editions OÜ, Tallinn, Estonia. P.36-42.
7. Цифровые следы преступлений : монография. Багмет А.М., Скобелин С.Ю. Москва : Проспект, 2021. - 168 с.

С.В. Петраков

Порядок наложения ареста на криптовалюту

Аннотация. В статье автор рассматривает способы наложения ареста на криптовалюту. Обращается внимание, что с учетом отсутствия нормативного регулирования данного вопроса и различных следственных ситуаций, арест может реализовываться в разном порядке. Рекомендации приводятся с учетом обобщенной судебной практики.

Ключевые слова: криптовалюта, цифровая валюта, виртуальные активы, арест криптовалюты

В настоящее время уголовно-процессуальное законодательство не регламентирует порядок наложения ареста на криптовалюту. Вместе с тем в практической деятельности исходя из совершения преступлений с использованием криптовалют, а также владением лицами соответствующими виртуальными активами, актуализируется вопрос о порядке наложения ареста на

данные активы. В монографических работах, посвященных в том числе и аспекту работы с виртуальными активами, данный вопрос детально не раскрывается[1].

Несмотря на то, что в соответствии с подразделом 3 Гражданского кодекса Российской Федерации «Объекты гражданских прав» цифровая валюта (виртуальные активы (криптовалюта)) не указаны как объект гражданских прав, это не влияет на возможность наложения на нее ареста. На территории Российской Федерации в соответствии с Федеральным законом от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» к виртуальным активам (криптовалюте) на территории нашего государства применяется общий термин – цифровая валюта. Криптовалюта приобретается за электронные и безналичные денежные средства и может быть в них преобразован. Исходя из этого А.Н. Смоляков относит ее к иному имуществу в соответствии со ст. 128 ГК РФ[2].

Частичное признание цифровой валюты имуществом для целей ряда федеральных законов нашей страны, в соответствии с вышеуказанным законом № 259-ФЗ, в том числе непосредственно связанных с уголовно-процессуальным законом, является достаточным основанием для принятия органами предварительного следствия мер, направленных на последующее обеспечение реализации норм федерального закона от 2 октября 2007 года № 229-ФЗ «Об исполнительном производстве». Иное (формальное) отношение к реализации норм российского законодательства противоречило бы позиции Конституционного Суда Российской Федерации неоднократного указывавшего на единство и взаимосвязь общественных отношений, регулирующихся и охраняющихся различными законами лишь в силу области их применения.

В отношении цифровой валюты отсутствует единый регулятор осуществляющий ее арест или иное обременение. В связи с данной особенностью способом, обеспечивающим контроль ее перемещения, является переводов цифровой валюты на криптоадрес, подконтрольный следственному органу. У органов расследования применительно к аресту криптовалюты могут сложиться следующие ситуации по делу:

1) получен доступ к переводу цифровой валюты (при хранении на некастодиальном и кастодиальном сервисе), хранящейся на криптоадресе, доступ к которому осуществляется с компьютерного устройства, обнаруженного и изъятого у обвиняемого. В этом случае арест осуществляется путем перевода с криптоадреса, подконтрольного субъекту, на криптоадрес, подконтрольный следственному органу;

2) в ходе следственного действия (осмотр, обыск) криптовалюта обнаруженная на криптоадресе подконтрольном обвиняемому изъята путем ее

---

[1] Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы : монография / под общ. и науч. ред. С. П. Щербы. – Москва : Проспект, 2022. – С. 120-132.

[2] Смоляков, А. Н. Хищение безналичных, электронных денежных средств и цифровой валюты: вопросы юридической техники и дифференциации ответственности : автореф. дис. … канд. юрид. наук. – СПб., 2023. – С. 9.

перевода на криптоадрес подконтрольный следственному органу, доступ к которому имеют сотрудники органа. В этом случае арест осуществляется путем запрета операций по криптоадресу, на который была переведена криптовалюта;

3) органы могут повлиять на перевод криптовалюты (при хранении на кастодиальном сервисе), хранящейся на криптоадресе провайдера услуг виртуальных активов (криптобиржа Binance), связанного с личным кабинетом (аккаунтом) обвиняемого, открытым на интернет-сайте криптобиржи. Отличие от первой ситуации будет заключаться в том, что органам известно где хранится криптовалюта, но доступ к самому криптоадресу, с которым соотнесен личный кабинете лица, отсутствует. В этом случае арест осуществляется при исполнении судебного решения путем перевода криптовалюты работниками соответствующего сервиса на криптоадрес подконтрольный следственному органу.

Вне зависимости от сервиса, на котором открыт криптокошелек субъекта преступления (кастодиальный или некастодиальный), перевод и последующее хранение возможны на следующих видах криптокошельков:

1) «бумажный»;

2) аппаратный;

3) мобильный либо десктопный.

Плюсы и минусы хранения арестованной криптовалюты на данных криптокошельках.

1. «Бумажный» криптокошелек.

Плюсы:

- не требуется какого-либо технического устройства для открытия криптокошелька в целях перевода арестованной криптовалюты и как следствие – отсутствие финансовых расходов государства на приобретение соответствующих технических устройств;

- отсутствие SEED-фразы и как следствие – отсутствие возможности импортировать криптокошелек с арестованной криптовалютой на другом устройстве;

- приватный ключ, который автоматически генерируется и распечатывается на принтере, фактически не запомнить в силу его сложности.

Минус:

- приватный ключ всегда находится в сети криптовалюты, в связи с чем не исключается возможность неправомерного доступа к криптокошельку, особенно если размер арестованных средств будет существенным;

- риск использования интернет-страниц на которых происходит генерирование криптовадресов.

2. Аппаратный криптокошелек.

Плюсы:

- приватный ключ находится на самом аппаратном устройстве, а не в сети криптовалюты, в связи с чем исключается возможность постороннего вмешательства для перевода арестованной криптовалюты;

- для совершения перевода арестованных средств нужен сам аппартный криптокошелек, который необходимо подключить к компьютеру.

Минусы:

- необходим непосредственно аппаратный криптокошелек и как следствие – дополнительные финансовые расходы государства на приобретение соответствующих аппаратных криптокошельков;

- есть SEED-фраза и как следствие – сложности при записи SEED-фразы, чтобы каждый из участвующих лиц записал только часть слов для исключения того факта, что одно лицо (или все) будут знать данную фразу, так как возможность запоминания не исключается и соответственно имеется возможность импортировать криптокошелек с арестованной криптовалютой на другом устройстве;

- нет SEED-фразы (только Tangem) – риск использования смартфона по иному назначению.

3. Мобильный или десктопный криптокошелек.

Минусы:

- необходим непосредственно смартфон или ноутбук для открытия криптокошелька на который будут переведены арестованные средства и как следствие – дополнительные финансовые расходы государства на приобретение соответствующих компьютерных устройств;

- смартфон или ноутбук целесообразно сдать на хранение, так как не исключается его утрата, поломка, возможность неправомерного доступа и как следствие – компьютерное устройство не использовать по иному назначению;

- при генерировании SEED-фразы возникают вышеуказанные сложности;

- приватный ключ всегда находится в сети и как следствие – возникают вышеуказанные сложности.

Плюсы у данных криптокошельков, по сравнению с «бумажным» или аппаратным, отсутствуют, в связи с чем данные виды криптокошельков не целесообразно использовать для ареста криптовалюты. «Бумажные» кошельки также желательно не использовать если средства арестовываются в значительном размере. Поэтому единственным на данный момент времени адекватным способом хранения арестованной криптовалюты, является перемещение ее на адрес аппаратного криптокошелька, желательно не генерирующего SEED-фразу, для исключения случаев злоупотребления со стороны самих сотрудников. Вместе с тем, государству необходимо разработать для целей работы правоохранительных и контролирующих органов свой ресурс по генерированию криптоадресов, для того чтобы правоприменители не сталкивались с этой технической сложностью, а лишь переводили на адреса, которые будут генерироваться под каждое конкретное дело.

Еще одним важным аспектом ареста криптовалюты является комиссия за подтверждение транзакции перевода криптовалюты в любой из трех вышеуказанных ситуаций. Комиссия не зависит от воли правоприменителя, это предусмотрено самой системой. Следователю необходимо только обязательно зафиксировать размер комиссии который будет взыскан за подтверждение конкретной транзакции.

Литература

1. Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы : монография / под общ. и науч. ред. С. П. Щербы. – Москва : Проспект, 2022. – 168 с.
2. Смоляков, А. Н. Хищение безналичных, электронных денежных средств и цифровой валюты: вопросы юридической техники и дифференциации ответственности : автореф. дис. … канд. юрид. наук. – СПб., 2023. – 22 с.

А.М. Попов
В.А. Шурухнов

Особенности использования и применения компьютерно-технических средств и технологий при расследовании преступлений в условиях пандемии

Аннотация. В статье рассматриваются отдельные особенности и аспекты совершения преступлений в условиях пандемии и возможных эпидемиях. Также, в статье рассматриваются отдельные варианты и особенности производства следственных и иных процессуальных действий с соблюдением требований мер безопасности лиц, осуществляющих их производство и расследования в целом.

***Ключевые слова*:** пандемия, эпидемия, совершение преступлений, меры безопасности, расследование преступлений, следственные действия.

Потребность нового подхода при расследовании преступлений появилась в нашей стране в ходе создавшихся условий наступления последствий пандемии коронавирусной инфекции covid-19. Ее распространение обусловило внесение существенных изменений в процесс обнаружения, фиксации и изъятия объектов преступной деятельности.

Следует признать, что с указанными обстоятельствами в виде короновирусных ограничений подобного масштаба, наше общество столкнулось впервые. Однако, дальнейшие события показали, что это не конечный результат негативных последствий. Беспрецедентные меры воздействия на наше государство выразились во введении санкций и изоляции в мировом масштабе.

Общество оказалось не готово к реализации мер по защите населения от воздействия пандемии, что привело к обострению различных социально-экономических проблем. В частности, количество преступлений в период пандемии существенно увеличилось в связи с введением в России коронавирусных ограничений. Обусловлено это тем, что в этот период большая часть населения была помещена на карантин в местах постоянного проживания. Это обстоятельство значительно повлияло на рост преступлений в сфере IT-технологий и бытовых преступлений.

Следует отметить, что значительный рост преступлений в сфере IT-технологий наблюдается уже длительное время. Так, например, по данным МВД, в январе – декабре 2019 года зарегистрировано более 294 тысяч преступлений,

совершенных с использованием информационно-телекоммуникационных технологий или, что почти на 70% больше, чем за аналогичный период прошлого года. Половина таких преступлений совершается с использованием сети «Интернет», а более трети – средств мобильной связи[1].

Вместе с тем, по данным за 2020 год, в период распространения коронавирусной инфекции, показатели преступности существенно изменились. В частности, общее число зарегистрированных в стране преступлений увеличилось на 1%, тяжких и особо тяжких – на 14%. Основное влияние на рост тяжких преступлений по итогам 2020 года оказало увеличение количества криминальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий. В отчетном периоде число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%. При этом, безопаснее стало в общественных местах. Снизилась уличная преступность. Так, преступлений на улицах, площадях, в парках и скверах зарегистрировано меньше на 9,9%, в том числе грабежей – на 24,8%, краж – на 18,5%, разбойных нападений – на 23,3%[2].

По данным ведомства в 2021 году темп роста зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, замедлился. По итогам 12-ти месяцев 2021 года их количество выросло незначительно – на 1,4%[3].

В 2022 году, аналогично, показатели киберпреступности в целом остались стабильными. С использованием высоких технологий совершается каждое четвертое преступление. Зарегистрировано на 27,6% меньше краж, на 29% – фактов мошенничества с использованием электронных средств платежа, на 22,5% – криминальных деяний в сфере компьютерной информации. Раскрываемость преступлений, совершенных с использованием IT-технологий, возросла на 4,4%[4].

Достаточно спорно увязывать создавшуюся ситуацию именно с влиянием коронавирусной инфекции на состояние преступности рассматриваемых видов. Однако, следует отметить, что она безусловно является одной из причин такого развития событий.

---

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года. URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/. Дата обращения: 27.04.2023.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/. Дата обращения: 27.04.2023.

[3] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/. Дата обращения: 27.04.2023.

[4] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/. Дата обращения: 27.04.2023.

Существенное влияние на показатели преступности оказала неготовность правоохранительных органов к производству расследования преступлений в указанных условиях. Необходимость проведения следственных действий при наличии оснований полагать, что лица, имеющие отношение к преступлению, могут быть заражены инфекцией, вызвали серьезные опасения за безопасность участвующих в проведении следственных действий участников, что негативно отразилось на процессе их производства.

Проблема заключалась не только в возможности проведения самого следственного действия (особенно в случаях проведения невербальных следственных действий), но и результатов их производства (сохранение обнаруженных следов). Вопрос, каким образом поступать с обнаруженными и изъятыми в ходе производства следственных действий объектами, оставался открытым.

Существенное значение имеют особенности обработки изъятых объектов специальными препаратами для уничтожения инфекции, их влияние на свойства этих объектов и, как следствие, возможность их предварительного исследования и дальнейшего производства экспертиз.

Позитивные моменты в рассматриваемой сфере наблюдаются только при работе с компьютерно-техническими средствами и следами их применения при расследовании преступлений. В случае изъятия указанных объектов существует возможность их обработки соответствующими дезинфицирующими средствами с последующей просушкой. При этом, в данном случае появляется необходимость наличия специального помещения, в котором указанные объекты будут подвергаться такой обработке и проходить дальнейший карантин. Кроме этого сам процесс обработки потребует привлечения дополнительных средств и ресурсов. Только в ходе реализации указанного варианта появляется возможность соблюдения санитарных норм и дальнейшего безопасного использования объектов в процессе расследования преступлений (не только компьютерно-технических средств, но и иных материальных объектов)[1].

По-иному обстоят дела с проведением следственных действий в отношении компьютерной информации, особенно когда она находится на внешних, удаленных носителях (сервер, виртуальный сервер, хостинг, облачное хранилище и т.п.). В указанном случае у следователя появляется возможность удаленного изъятия информации из мест такого хранения без взаимодействия с материальными объектами[2].

---

[1] «МР 3.1.0170-20. 3.1. Профилактика инфекционных болезней. Эпидемиология и профилактика COVID-19. Методические рекомендации» (утв. Главным государственным санитарным врачом РФ 30.03.2020) (ред. от 30.04.2020). «Бюллетень нормативных и методических документов Госсанэпиднадзора», выпуск 2, июнь, 2020.

[2] См., например: Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков; Министерство науки и высшего образования Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). – Москва: Общество с ограниченной ответственностью «Проспект», 2022.

Наибольшую сложность, в процессе расследования преступлений в рассматриваемых условиях, представляет производство вербальных следственных действий. Особенно это актуально в случае их производства с лицами зараженными инфекционными заболеваниями. Одним из средств решения проблемы может быть использование помощи медицинских работников, которые могут обеспечивать условия использования технологии удаленного доступа посредством применения средств связи (телекоммуникационных) и т.п.

Уже сегодня, по результатам деятельности в условиях пандемии учеными и специалистами предлагаются различные средства и технологии решения рассматриваемой проблемы. С одной стороны, предлагается трансформация правового регулирования процесса расследования. С другой, изменение системы при производстве следственных и иных процессуальных действий.

В частности, например: «уголовно-процессуальный кодекс не предусматривает иного особого порядка назначения судебно-медицинской экспертизы в условиях эпидемии или пандемии, а значит в этой части законодателю нужно уже сейчас вносить изменения в законодательство. Первое – внесение поправок в часть 1 ст.208 УПК РФ и второе – ввести новую главу в Уголовно-процессуальный кодекс Российской Федерации особого порядка в условиях эпидемии или пандемии, где следовало бы включить и иные чрезвычайные ситуации (наводнения, пожары, военные действия и другие стихийные бедствия). И только после того, как условно больной коронавирусом подозреваемый или обвиняемый излечился, о чем может свидетельствовать медицинский документ, после отмены карантина можно будет решать вопрос о возобновлении предварительного следствия, дознания и разбирательства в суде»[1].

Кроме этого: «в особом порядке расследования уголовных дел следователем или дознавателем и судебного разбирательства в условиях эпидемии или пандемии можно было бы предложить проведение следственных действий на электронной платформе в удаленном режиме, как сейчас принято говорить на «удаленке». А именно – можно было бы разрешить проводить некоторые следственные и процессуальные действия через Интернет, включая производство допросов, например, через систему ZOOM, разумеется, с осуществлением записи и приобщением его в уголовном деле, которое, несмотря на отсутствие подписи участников судопроизводства, будет иметь доказательное значение.[2]

Помимо допроса с помощью записи в системе ZOOM можно разрешить следователю или дознавателю проводить очную ставку, опознание лица и предметов, знакомить подозреваемого или обвиняемого, а также их защитников

---

[1] Матинов, С. Г. Расследование и рассмотрение уголовных дел в условиях пандемии / С. Г. Матинов, Е. В. Решетов, З. Г. Матинова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2020. – № 7(122). – С. 106-108.

[2] См. ст. 189.1. УПК РФ Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи (введена Федеральным законом от 30.12.2021 № 501-ФЗ){прим. ред.}.

с назначением и заключением судебных экспертиз, а также знакомить причастных лиц с процессуальными постановлениями. Разумеется, следователь или дознаватель должны соблюсти все требования, нормы и порядок проведения указанных следственных действий, разъяснив всем причастным лицам их права и обязанности»[1].

Для реализации указанных положений, по мнению ученых, необходимо принятия рядя мер, например, допрос посредством видеоконференции, потребует определенных средств, времени на обустройство и обучение следователей. Необходимо будет выработать регламент проведения допроса в таких условиях, дополнить УПК положениями о порядке допроса, фиксации, оформлении результатов[2].

Предлагаются и достаточно экзотические способы проведения следственных действий, например: «эффективным средством проведения такого следственного действия как осмотр места происшествия может стать использование своего смартфона для проведения с сотрудниками следственных органов соответствующих процессуальных действий по расследованию преступлений, путем использования видео-конференц-связи через мессенджеры (What's app, Zoom, Telegram). Следователь будет объяснять, каким именно образом следует будет действовать потерпевшему чтобы провести осмотр места происшествия»[3].

При производстве невербальных следственных действий предлагаются и традиционные способы. Наиболее простое решение при производстве следственных и иных процессуальных действий на открытой территории. Например, посредством применения БПЛ, квадрокоптеров и иных подобных аппаратов[4].

Безусловно, все авторы практически единодушно заявляют о необходимости использования различных мессенджеров и социальных сетей для проведения следственных и иных процессуальных действий. Однако, следует учитывать, что в настоящее время в распоряжении российских граждан, организаций, учреждений и предприятий имеется ограниченное их количество (условно российский – Telegram, российские – Яндекс, ТамТам, ICQ, а также корпоративные мессенджеры – VK Teams, Интранетус, Мой Коннект и др.). Использование не сертифицированных, не российских технологий может

---

[1] Матинов С.Г., указ соч.

[2] Сотников, К. И. Некоторые аспекты организационно-процессуальной деятельности органов предварительного расследования в условиях пандемии коронавируса covid-19 / К. И. Сотников, Э. В. Лантух // Судебная экспертиза: прошлое, настоящее и взгляд в будущее: материалы международной научно-практической конференции, Санкт-Петербург, 14–15 мая 2020 года. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2020. – С. 333-338.

[3] Кабельков, С. Н. Особенности производства следственных и процессуальных действий в условиях пандемии / С. Н. Кабельков, А. И. Ибрагимов // Вестник ВИЭПП. – 2021. – № 2. – С. 82-89.

[4]Савельева, М. В. Беспилотный летательный аппарат как специальное технико-криминалистическое средство и объект криминалистического исследования / М. В. Савельева, А. Б. Смушкин // Вестник Томского государственного университета. – 2020. – № 461. – С. 235-241.

существенно негативно повлиять на процесс раскрытия преступлений, производство по уголовным делам, а также судебного разбирательства, так как не будет обеспечена возможность сохранения следственной тайны и приведет к утечке информации.

Такое положение может свидетельствовать о необходимости создания специализированного, временного в части периода использования (пандемия, эпидемия и т.п.), общедоступного или корпоративного мессенджера для нужд правоохранительных органов, в целях общения с лицами, вовлеченными в процессуальную или иную правоохранительную деятельность.

Для решения проблемы необходим комплексный подход, одним из элементов которого должны стать научные положения и разрабатываемые на их основе практические рекомендации производства следственных и иных процессуальных действий в условиях пандемии, в том числе, с использованием компьютерно-технических средств и технологий, которые позволят эффективно их проводить даже в условиях активного противодействия со стороны заинтересованных лиц.

В комплексный подход должна входить соответствующая подготовка следователей, осуществляемая с учетом обозначенных проблем.

Разработка научных положений и подготовка практических рекомендаций по исследуемому направлению должна отражать потребности практических органов в том направлении, которое позволит обеспечить их эффективное взаимодействие с другими подразделениями и службами с учетом специфических ведомственных систем реализации правоохранительной и иной деятельности.

Литература

1. Кабельков, С. Н. Особенности производства следственных и процессуальных действий в условиях пандемии / С. Н. Кабельков, А. И. Ибрагимов // Вестник ВИЭПП. – 2021. – № 2. – С. 82-89.
2. Матинов, С. Г. Расследование и рассмотрение уголовных дел в условиях пандемии / С. Г. Матинов, Е. В. Решетов, З. Г. Матинова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2020. – № 7(122). – С. 106-108.
3. Савельева, М. В. Беспилотный летательный аппарат как специальное технико-криминалистическое средство и объект криминалистического исследования / М. В. Савельева, А. Б. Смушкин // Вестник Томского государственного университета. – 2020. – № 461. – С. 235-241.
4. Сотников, К. И. Некоторые аспекты организационно-процессуальной деятельности органов предварительного расследования в условиях пандемии коронавируса covid-19 / К. И. Сотников, Э. В. Лантух // Судебная экспертиза: прошлое, настоящее и взгляд в будущее: материалы международной научно-практической конференции, Санкт-Петербург, 14–15 мая 2020 года. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2020. – С. 333-338.

5. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков; Министерство науки и высшего образования Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). – Москва: Общество с ограниченной ответственностью «Проспект», 2022. – 256 с.

А.Э. Побегайло

Нейронные сети как средство совершения преступления: уголовно-правовая и криминологическая характеристика

Аннотация. Использование нейронных сетей возрастает с каждым годом, как и их возможности. Создание ими текстового контента, так называемых «дипфейков» (поддельных цифровых видеозаписей и фотографий, а также голоса), может нести за собой общественную опасность. Понятие «нейронная сеть» отсутствует как в Уголовном законе, так и в Постановлениях Пленума Верховного Суда. В статье кратко рассматриваются основные преступные деяния, которые возможно совершить с использованием нейронных сетей, и предлагаются пути закрепления их как квалифицирующего признака.

Ключевые слова: нейронные сети, вопросы квалификации преступлений, киберпреступления, киберпреступность.

На современном этапе технологического развития общества, использование нейронных сетей значительно увеличилось. В публичный доступ вывели нейронные сети, которые позволяют решать самые разнообразные задачи – генерировать текст по различным вопросам, писать исполняемый код на различных языках программирования, распознавать изображения и видео, создавать их, управлять сложными электронными системами. Как уже случилось с иными достижениями технического прогресса, нейронные сети могут быть использованы для совершения разного рода преступлений.

Нейронная сеть – это математическая модель, построенная на принципах структуры и функциональных аспектов биологических нейронных сетей. Она состоит из взаимосвязанных искусственных нейронов, которые обрабатывают информацию и преобразуют ее с помощью распределенного и параллельного подхода. Искусственные нейроны в нейронной сети могут обрабатывать информацию одновременно и независимо друг от друга, что позволяет сети быстро адаптироваться и обучаться на больших объемах данных.

Одна из самых известных нейронных сетей, ChatGPT, была запущена 30 ноября 2022 года компанией OpenAI, базирующейся в Сан-Франциско, занимающейся исследованиями и внедрением искусственного интеллекта.

За пять дней после запуска ChatGPT преодолела отметку в 1 миллион пользователей, к концу января 2023 года она приобрела 57 млн. пользователей, а 1 февраля того же года уже более 100 миллионов пользователей[1].

По динамике роста пользовательской базы ChatGPT можно констатировать не просто широкое распространение ее использования, но и иных подобных продуктов в будущем. На настоящий момент существуют еще ряд генеративных нейронных сетей, производящих аудио-, видео-, и текстовый контент.

По мнению ученых, занимающихся данной проблематикой, основные риски использования нейронных сетей включают в себя ряд проблемных аспектов:

1. Нейронные сети часто требуют больших объемов данных для обучения, и это может создать риски, связанные с конфиденциальностью и безопасностью личной информации[2].

2. Алгоритмы глубокого обучения, включая используемые для принятия решений, могут отражать существующие дискриминационные предубеждения в данных, в связи с чем нейронная сеть делает неправильные выводы по поводу расы, религии, возраста или других характеристик[3][4].

3. Нейронные сети могут использоваться для создания вредоносного контента, имеющего ложный характер: дезинформации, фальшивых новостей или «глубоких подделок» (deepfakes, далее в тексте – «дипфейки»), которые могут приносить вред целому ряду общественных отношений и влиять на общественное мнение[5].

4. Ряд исследователей выражают опасения о том, что развитие сильного искусственного интеллекта может привести к созданию распределенного искусственного интеллекта, который сможет создавать свои копии и влиять на электронные системы в реальном мире без участия человека. Такой искусственный интеллект который может стать неконтролируемым, и представлять угрозу для человечества[6].

В российском уголовном кодексе не содержится определения нейронных сетей, а равно генерируемого ими контента. При этом они уже могут быть использованы для совершения целого ряда преступных деяний.

---

[1] Крецу К. Программисты, визионеры и гении бизнеса: кто придумал ChatGPT и куда они его ведут // – Forbes.ru. – 20.03.2023 [Электронный ресурс]. URL: https://www.forbes.ru/tekhnologii/486215-programmisty-vizionery-i-genii-biznesa-kto-pridumal-chatgpt-i-kuda-oni-ego-vedut

[2] Chang S., Li C. Privacy in neural network learning: threats and countermeasures // IEEE Network. – 2018. – Т. 32. – №. 4. – С. 61-67.

[3] Abid A., Farooqi M., Zou J. Persistent anti-muslim bias in large language models // Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. – 2021. – С. 298-306.

[4] Tamkin A. et al. Understanding the capabilities, limitations, and societal impact of large language models // arXiv preprint arXiv:2102.02503. – 2021.

[5] Kietzmann J. et al. Deepfakes: Trick or treat? // Business Horizons. – 2020. – Т. 63. – №. 2. – С. 135-146.

[6] Turchin A., Denkenberger D. Classification of global catastrophic risks connected with artificial intelligence //Ai & Society. – 2020. – Т. 35. – №. 1. – С. 147-163.

1. Создание фотореалистичных поддельных видео-, фото- или аудиозаписей («дипфейков), которые могут быть использованы для клеветы, мошенничества, а равно вымогательства (ст. 128.1, 159, 163 УК РФ).

2. Создание заведомо ложной информации с целью ввода в заблуждение общественности, запугивания ее, усиления расовой, национальной или иной розни, а равно доверия к источникам информации и государственным институтам (ст. 207, 207.1, 207.2, 207.3 УК РФ).

3. Использование синтезированных голосов для имитации реальных людей и совершения мошенничеств и хищения личной информации (ст. 159 УК РФ).

4. Создание спама, оскорбительных комментариев или порнографического контента (включая контент с участием несовершеннолетних) с помощью нейронных сетей в целях травли, дискредитации или нарушения законов о защите авторских прав (ст. 146, 242, 242.1 УК РФ).

5. Создание вредоносного программного обеспечения, обходящего обнаружение антивирусными программами или проникающего в системы безопасности. Они также могут использоваться для автоматизации процесса поиска уязвимостей в программном обеспечении и создания специализированных атак на конкретные цели (ст. 273 УК РФ).

6. Создание материалов, пропагандирующих терроризм, диверсионные или экстремистские идеи, включая создание манипулятивного видео- или аудио-контента (ст. 205.2, 280, 280.1, 280.4, 281.1, 281.3, 282 УК РФ).

Определение ответственности за действия, совершенные с использованием нейронных сетей, может вызывать некоторые проблемы. Алгоритмы, на основе которых нейросеть создает контент, могут быть сложными и непрозрачными. Это может затруднить квалификацию такого рода деяний, прежде всего при использовании виновным лицом автоматизации использования нейронной сети, в рамках которой он не контролирует распространение такого контента. Помимо данного вопроса, не урегулирован ни в законе, ни в доктрине признак повышенной опасности нейронной сети.

При использовании Интернета, общественную опасность несет, прежде всего, *признак публичности*, а при использовании нейросети, на наш взгляд – *признак доступности*. Если до появления и распространения нейросетей с удобным пользовательским интерфейсом, например, создание поддельных изображений, фотомонтажа и видеозаписи требовало специальных познаний для получения приемлемого результата, то с использованием нейросетей познаний требуется значительно меньше.

По сравнению с обычным созданием вредоносного программного обеспечения нейросеть не несет повышенной общественной опасности, поскольку для использования сгенерированных ей программ или иной компьютерной информации все равно необходимы специальные познания, будь то компилируемый код, или же сценарий Python.

Нейросеть не является заранее вредоносной, если только не была специально создана обучением исключительно на исходных кодах вредоносного программного обеспечения, но пока таких нейросетей в общем доступе нет.

Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации […]», к сожалению, не дает прямой трактовки терминов «вредоносная компьютерная программа», но дает толкование понятию «иная компьютерная информация».

Согласно п. 8 Постановления, основным признаком ее выступает признак *заведомости*, когда программа или иная компьютерная информация заранее направлена на указанные в законе преступные последствия[1]. При этом практически любую из существующих типов нейронных сетей к такой информации отнести нельзя, т. к. при их создании инженеры не предполагали достижения целей, перечисленных в ч. 1 ст. 273 УК РФ.

Вместе с тем, регулирование, в том числе и уголовно-правовое, нейронных сетей является насущной необходимостью. Количество совершенных киберпреступлений даже без использования нейронных сетей практически с каждым годом демонстрирует тенденцию к росту. Так, по данным Главного управления правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, в 2018 г. было зарегистрировано 174 674 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2019 г. – 294 409 (+40,7 %), в 2020 – 510 396 (+42,3 %), 2021 – 517 722 (+1,4 %), в 2022 – 522 065 (+0,8 %)[2].

Представляется, что необходимо предложить следующие пути регулирования нейросети как средства совершения преступления: 1) внести в текст соответствующих статей Уголовного кодекса РФ, квалифицирующего признака «…с использованием нейронной сети», по признаку доступности, увеличивающей общественную опасность деяния; 2) внести «…с использованием нейронной сети» как конститутивного признака ст. 273 и 274.1 УК РФ, поскольку для совершения данных преступлений, субъект в любом случае должен уже иметь специальные познания; 3) внести признак «с использованием нейронной сети, а равно искусственного интеллекта» в ст. 63 УК РФ в качестве одного из отягчающих обстоятельств; 4) дополнить указанное Постановление Пленума Верховного Суда от 15.12.2022 № 37 понятием нейронной сети как математической модели, построенной на принципах структуры и функциональных аспектов биологических нейронных сетей, способной к созданию, использованию и распространению цифровой

[1] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС «КонсультантПлюс».

[2] Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации // [Электронный ресурс]. – 2018, 2019, 2020, 2021, 2022. – Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации.

информации, включая текстовую информацию, видеозаписи, цифровые изображения, исполняемый код.

Литература

1. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС «КонсультантПлюс».
2. Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации // [Электронный ресурс]. – 2018, 2019, 2020, 2021, 2022. – Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации.
3. Крецу К. Программисты, визионеры и гении бизнеса: кто придумал ChatGPT и куда они его ведут // – Forbes.ru. – 20.03.2023 [Электронный ресурс]. URL: https://www.forbes.ru/tekhnologii/486215-programmisty-vizionery-i-genii-biznesa-kto-pridumal-chatgpt-i-kuda-oni-ego-vedut
4. Abid A., Farooqi M., Zou J. Persistent anti-muslim bias in large language models // Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. – 2021. – С. 298–306.
5. Chang S., Li C. Privacy in neural network learning: threats and countermeasures // IEEE Network. – 2018. – Т. 32. – №. 4. – С. 61–67.
6. Kietzmann J. et al. Deepfakes: Trick or treat? // Business Horizons. – 2020. – Т. 63. – №. 2. – С. 135–146.
7. Tamkin A. et al. Understanding the capabilities, limitations, and societal impact of large language models // arXiv preprint arXiv:2102.02503. – 2021.
8. Turchin A., Denkenberger D. Classification of global catastrophic risks connected with artificial intelligence //Ai & Society. – 2020. – Т. 35. – №. 1. – С. 147–163.

Л.Н. Посельская

Тактико-криминалистические особенности профилактической деятельности следователя по противодействию киберпреступности

Аннотация. В данной статье рассматриваются основные направления противодействия киберпреступности и меры предупреждения преступлений, совершенных с использованием цифровых технологий. Рассмотрены существующие проблемы в системе мер предупреждения киберпеступности.

Ключевые слова: направления противодействия киберпреступности, система мер профилактика преступлений, взаимодействие со средствами массовой информации СМИ.

Актуальные вопросы преступности в сфере информационных технологий обсуждаются на государственном и международном уровнях, что свидетельствует транснациональном характере киберпреступлений.

В борьбе с рассматриваемыми преступлениями важным является международное сотрудничество. Именно посредством обмена опытом в области борьбы с киберпреступлениями выявляются приоритетные задачи, которые направлены на эффективное противодействие такого вида преступной деятельности. С целью усиления эффективности борьбы с преступностью на международном уровне проводятся семинары, на которых разрабатываются и утверждаются планы мероприятий. В своей статье Л.А. Бураева отмечает, что «…одной из приоритетных задач является как раз использование профилактических мер со стороны правоохранительных органов».[1] Значимость обуславливается тем, что принятые меры воздействуют на детерминанты, причины развития, роста или снижения преступности.

Со стороны правоохранительных органов требуется использование комплекса мер, которые представляют собой более широкое понятие, чем борьба с преступностью, что позволяет их отождествлять как обще социальные, правовые, а также проведение целевых мероприятий, направленных на информирование населения об актуальных проблемах, их действиях и защите правоохранительных органов.

В этом смысле профилактическая деятельность органов предварительного расследования представляет собой систему мер предупреждения преступности. Правовая группа мер предупреждения включается в себя нормы законодательства, которые устанавливают ответственность за совершение преступлений с использованием информационно-телекоммуникационных технологий, в том числе в сфере информационной безопасности. Общепринятые международные правовые нормы были сформированы в конце 20 века.

Однако, с момента включения в Уголовный кодекс Российской Федерации новой главы: «Преступления в сфере компьютерной информации», в течение последних 15 лет не вносились более или менее существенных изменения в главы относительно использования компьютерных и информационно-телекоммуникационных технологий. По мнению отдельных авторов «…такое положение обусловило отставание правового регулирования от современных способов преступления, что привело к пробелам в законодательстве, неоднозначности понимания и определения действий преступников».[2]

Судебно – следственная практика характеризуется отсутствием единой системы в решении правовой оценки действий лиц, использующих при совершении преступлений цифровые технологии.

Вместе с тем, одних правовых мер недостаточно. При решении практических задач предупреждения преступлений, совершаемых с использованием

---

[1] Бураева, Л.А. Компьютерные преступления транснационального характера как глобальная угроза мировому сообществу // Проблемы экономики и юридической практики. – 2016. – № 5. – 226 с.

[2] Колчевский И.Б., Бицадзе Г.Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. – 2021. – № 2 (54).- 45 с.

цифровых, информационно-телекоммуникационных технологий важно обратить внимание на организационно-управленческое направление.

Мы поддерживаем ученых, занимавшихся данной проблемой, которые к данной группе относятся следующие меры предупреждения преступности:

«…предотвращение утечки, хищения, утраты, искажения и подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы и системы; обеспечение правового режима функционирования документированной информации как объекта собственности; сохранение государственной тайны и конфиденциальности документированной информации; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения».[1]

Важно учитывать, что в первую очередь необходимо сформировать убежденность в том, что обеспечение информационной безопасности является посильным для работы правоохранительных органов. Именно этот фактор играет особую роль в качестве сдерживающего механизма. Со стороны преступника должно быть четкое осознание того, что за его преступными деяниями последует наказание, а вероятность быть уличенным очень высока.

Третью группу составляют технические меры, которые включают в себя программные и аппаратные методы. К программным методам относятся те, которые защищают информацию посредством шифрования данных. В настоящее время существует множество надежных способов, которые обеспечат безопасность передачи информации. К аппаратным методам, как полагают авторы, исследовавшие данные проблемы, следует отнести те, которые направлены на защиту от физического воздействия. Так, например, для защиты информации устанавливают устройства идентификации личности, источники бесперебойного питания, шифрозамки и т.д.[2] Но, тем не менее, на многих предприятиях существует проблема, связанная с недостаточностью защиты данных, из чего в дальнейшем следует повышение риска совершения преступлений, направленных на получение несанкционированного доступа к данным, хищение или модификацию информации из организации. Также влияет уровень проведения инструктажа среди сотрудников предприятия, осуществление контроля и проверки среди персонала.

Следующая группа мер, направленных на противодействие и предупреждение киберпреступности стоит в возможности распространения информации об успешном раскрытии таких преступлений, что в целом правоохранительные органы выявляют и раскрывают названные преступления. Кроме этого, важная

---

[1] Суходолов А.П., Иванцов С.В., Борисов С.В., Спасенников Б.А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. – 2017. – № 1. – 17 с.

[2] Аль-Аммори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И.К. Методы и средства защиты информации // The Scientific Heritage. – 2020. – № 51-1. – 35 с.

роль отводится информированию населения об актуальных проблемах, и действиях правоохранительных органов по защите населения. В контексте противодействия киберпреступности следует отнести взаимодействие со средствами массовой информации (далее по тексту СМИ). Главной функцией СМИ является распространении полученных сведений о событиях, которые особенно важны как для граждан, так и для органов власти. СМИ и правоохранительные органы все больше взаимодействуют друг с другом, на основе профессиональной заинтересованности обеих сторон. Для СМИ важно поддерживать уровень престижа, получать поддержку посредством реализации мероприятий, направленных на розыск и изобличении преступников. Как отмечает В.Э. Гаджиев «СМИ способствуют повышению уровня правовой грамотности у населения. Правоохранительные органы являются одним из основных источников актуальной и интересной информации, которая отличается своей надежностью и достоверностью. Для широкой аудитории важно получение не только достоверной и актуальной информации, а тех сведений, которые вызовут определенные эмоции, что подтверждает интерес СМИ именно к криминальной области. Для многих СМИ поддержание рейтинга напрямую зависит от того, насколько остросюжетное будет сообщение».[1] При расследовании преступлений, совершаемых с использованием цифровых технологий, сотрудники органов внутренних дел также активно используют СМИ. Во-первых, посредством распространения достоверной информации возможно объективное отображение проблем, существующих в обеспечении правопорядка, а также предоставление действительной оценки деятельности правоохранительных органов. Для граждан особенно важно получить от СМИ исчерпывающую информацию о том, как работает правоохранительная система, основной целью которой является обеспечение защиты прав и свобод человека. Но и со стороны населения возможна передача необходимой информации следователю, что поспособствует раскрытию преступления и изобличению преступников. СМИ используется в качестве посредника для правоохранительных органов о помощи со стороны населения.

Далее, как одну из нетипичных мер противодействия киберпреступности следует отнести устранение факторов, влияющих на рост преступности в сфере компьютерной информации. Например, устранение таких факторов как устаревшие средства защиты информации путем обновления программного обеспечения могут не только не повлиять на ситуацию, но и привести к негативным последствиям. Связано это с тем, что новое программное обеспечение лишь кажется более надежным и безопасным для информации. Только в процессе использования и работы с новым программным обеспечением могут быть выявлены технические недочеты. А это значит, остается открытым вопрос, можем ли мы однозначно считать, что организация, установившая

[1] Гаджиев, В.Э. Некоторые аспекты использование средств массовой информации в ходе осуществления криминалистического предупреждения преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – №3 (17). – 87 с.

последнюю версию программного обеспечения, стала более защищенной, чем та, которая использует старую, но при этом проверенную временем.

Следующий момент, который влияет на разработку мер предупреждения компьютерной преступности, касается транснационального характера рассматриваемых преступлений. Примером международного сотрудничества в области профилактики компьютерной преступности может послужить Конференция «Код ИБ», в которой участвуют Россия, Казахстан, Узбекистан и Беларусь.[1] В рамках серии конференций обсуждаются актуальные проблемы IT-безопасности, достижения борьбы с IT-угрозами. В своем исследовании В.Г. Гриб отмечает, что «…данная Конференция действует с 2006 года. В 2008 году состоялась Первая международная конференция по безопасности и правовым проблемам противодействия киберпреступности».[2]

Главными задачами международных конференций является обсуждение актуальных проблем, прогнозирование тенденций роста преступности, а также разработка мероприятий по предупреждению преступности в сфере информационной безопасности.

Таким образом, в настоящей статье мы рассмотрели наиболее эффективные, на наш взгляд, меры противодействия киберпреступности, доступные для осуществления в деятельности правоохранительных органов. В целом же тема актуальная и объемная, и требует дальнейшего научного исследования.

Литература

1. Аль-Аммори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И.К. Методы и средства защиты информации // The Scientific Heritage. – 2020. – № 51-1. – 35 с.
2. Бураева, Л.А. Компьютерные преступления транснационального характера как глобальная угроза мировому сообществу // Проблемы экономики и юридической практики. – 2016. – №5. – 226 с.
3. Гаджиев, В.Э. Некоторые аспекты использование средств массовой информации в ходе осуществления криминалистического предупреждения преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – №3 (17). – 87 с.
4. Гриб В.Г. Проблемы международного правового обеспечения борьбы с компьютерными преступлениями // Образование и право. – 2018. – №8. - 56 с.
5. Колчевский И.Б., Бицадзе Г.Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. – 2021. – № 2 (54).45 с.

[1] См.: Конференция Код ИБ. Серия региональных конференций с самым широким охватом ИБ-профессионалов. // КодИБ. Режим доступа: https://codeib.ru/conf (дата обращения 29.4.2023 г.)

[2] Гриб В.Г. Проблемы международного правового обеспечения борьбы с компьютерными преступлениями // Образование и право. – 2018. – №8. - 56 с.

6. Суходолов А.П., Иванцов С.В., Борисов С.В., Спасенников Б.А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. – 2017. – №1. – 17 с.

В.А. Прорвич

Киберпреступления в сфере цифровой экономики и финансов: правовые и информационно-технологические аспекты

Аннотация. Рассмотрение особенностей системы цифровых прав, связанных законодателем с правилами информационных систем, в том числе, иностранных, позволило предложить критерии для классификации киберпреступлений в сфере экономики и финансов. Показана роль информационно-математического моделирования противоправных деяний в данной сфере для формирования развернутой уголовно-правовой характеристики преступлений данного вида. Сделан ряд акцентов на содержательные особенности юридических алгоритмов выполнения процессуальных действий, нацеленных на обработку информации, имеющей значение для уголовного дела, формирование на ее основе необходимых доказательств, а также их надлежащую проверку и оценку. На их основе возможно формирование криминалистических и экспертных методик, а также создание системы сертификации специального программного обеспечения для нужд уголовного судопроизводства по преступлениям в сфере цифровых прав.

Ключевые слова: киберпреступления, экономика и финансы, цифровые права, информационно-математическое моделирование, юридические алгоритмы, проверка и оценка доказательств, экспертные методики, сертификация компьютерных программ.

Проведенные исследования показывают, что при быстром росте количества преступлений в сфере цифровой экономики и финансов, их важнейшей особенностью становится системно организованный характер. Даже на государственном уровне ряда зарубежных стран отмечаются грубейшие нарушения действующего национального законодательства и международного права. При этом для выполнения преступных замыслов применяются современные средства компьютерной техники и информационно-телекоммуникационные технологии.

Ситуация в данной сфере существенно усложнилась со времени введения в российское законодательство Федеральным законом от 18.03.2019 № 34-ФЗ цифровых прав. В соответствии с новой редакцией ст. 128 и ст. 141.1 ГК РФ, цифровые права представляют собой «обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы». При этом не были введены положения о соответствии таких правил требованиям действующего законодательства, порядке выполнения проверки и об ответственности обладателей

информационных систем, создавших и использующих эти правила, за нарушение российского законодательства.

При введении в действующее законодательство положений о цифровых финансовых активах. Федеральным законом от 31 июля 2020 г. № 259-ФЗ было не только дано их определение, связанное с цифровыми правами. Важно обратить внимание на введение возможности использования при совершении сделок с ними правил иностранных информационных систем.

С точки зрения обеспечения надлежащей уголовно-правовой защиты субъектов цифровых прав приходится учитывать, что многие обладатели информационных систем не только устанавливают для них свои собственные правила, но и используют оригинальное программное обеспечение. Это существенно затрудняет контроль за совершением разнообразных транзакций в рамках данных информационных систем, тем более, иностранных, причем имеющийся в распоряжении следствия криминалистический инструментарий помогает далеко не всегда.

Кроме этого, важно обратить внимание на то, что цифровые права отнесены законодателем к обязательственным правам. То есть, субъекты таких прав в рамках договорных отношений принимают на себя определенные обязательства, получая в связи с этим соответствующие права требования. При этом разрешение гражданско-правовых коллизий в пользу российских обладателей цифровых прав на цифровые финансовые активы в судах иностранных государств в большинстве случаев заранее обречено на неудачу. Аналогичный вывод можно сделать и в отношении их уголовно-правовой защиты.

Это подтверждается решениями обладателей информационных систем иностранных банков, установивших такие правила, которые позволяют им «замораживать» российские государственные валютные активы на сумму более 300 млрд. долларов. Но кроме этого были заморожены еще более крупные суммы ценных бумаг и иностранных валют, принадлежащих частным лицам. Данные незаконные решения, имеющие признаки криминального сговора, во многих иностранных юрисдикциях уже пытаются довести до присвоения российских активов и их растраты в сверхкрупном размере.

Поскольку современная организованная финансовая и экономическая преступность приобретает принципиально новый характер, возникает ряд наиболее актуальных задач по созданию эффективных средств для своевременного выявления и пресечения ее проявлений. Одной из таких задач является выработка научно обоснованных и выверенных в правовом плане критериев для классификации киберпреступлений в финансово-экономической сфере. Это позволяет сфокусировать усилия ученых и специалистов на разработку современного инструментария для борьбы с ними. Кроме этого, создается и научная основа для прогнозирования появления новых видов высокотехнологичных преступлений в данной сфере, чтобы не только развивать инструментарий для борьбы с ними опережающими темпами, но и активизировать их профилактику.

По результатам проведенных исследований определены подходы к формированию критериев, позволяющих выделить несколько групп киберпреступлений в финансово-экономической сфере.

К первой группе преступлений в сфере цифровой экономики и финансов можно отнести семь подгрупп из несколько видов «традиционных» преступлений в сфере экономики, совершаемых с помощью компьютерной техники и информационно-сетевых технологий. В первой подгруппе ряд сходных признаков характерны для «киберкраж», «кибермошенничества», «киберприсвоения» и «киберрастраты», «кибервымогательства», а также для некоторых других видов преступлений, предусмотренных статьями, включенными в главу 21 УК РФ. К этой подгруппе можно отнести и «киберграбеж», характеризующий открытое хищение российских валютных средств рядом руководителей западных банков.

Во *вторую подгруппу* можно включить киберпреступления, связанные с незаконной предпринимательской деятельностью, в том числе, банковской, включая привлечение средств для построения финансовых пирамид, легализацию денежных средств и иного имущества, полученных преступным путем, а также некоторые другие финансовые преступления, предусмотренных статьями, включенными в главу 22 УК РФ, совершаемые с использованием компьютерной техники, всевозможных гаджетов, разнообразных устройств мобильной связи и современных информационных технологий.

В *третью подгруппу* – киберпреступления, связанные с незаконной продажей контрафактной и фальсифицированной продукции, незаконное использование товарных знаков, незаконный оборот драгоценных металлов и природных драгоценных камней, контрабанду и ряд других преступлений, включенных в главу 22 УК РФ, совершаемых с использованием информационных технологий.

К *четвертой подгруппе* можно отнести киберпреступления, связанные с организацией преднамеренных и фиктивных банкротств, совершенных с использованием современных информационных технологий.

В *пятую подгруппу* можно включить киберпреступления, связанные с незаконной организацией и проведением азартных игр,

К *шестой подгруппе* можно отнести киберпреступления, связанные с совершением незаконных валютных операций.

В *седьмую подгруппу* можно включить налоговые киберпреступления, совершаемые с использованием современных информационных технологий.

Кроме киберпреступлений в различных сферах экономики и финансов можно также выделить несколько других, подобных первой группе, «традиционных» преступлений в других сферах, например, киберэкстремизм, совершаемый с использованием Интернета, торговлю наркотиками, оружием, опасными материалами и веществами, а также другими запрещенными к легальному обороту товарами с помощью Даркнета, и т.п. Эти виды киберпреступлений нередко имеют опосредованные связи с преступлениями в сфере цифровой экономики и финансов.

Во вторую группу по результатам проведенных исследований предлагается включить те виды киберпреступлений в сфере цифровой экономики и финансов,

которые совершаются против отдельных информационных систем либо против информационной инфраструктуры в сфере экономики и финансов, принадлежащей физическим и юридическим лицам различного вида и уровня, а также муниципальным образованиям и государству. Их большая часть предусмотрена статьями, включенными в главу 28 УК РФ, хотя многие из них предусмотрены статьями, включенными в другие главы Особенной части УК РФ.

Они имеют принципиальные отличия от первой группы, как по объекту и объективной стороне, так и по субъекту и субъективной стороне преступлений соответствующих видов. Хотя при их приготовлении, совершении и сокрытии также используется весьма совершенная компьютерная техника и информационно-телекоммуникационные технологии, но их объект, способы совершения, а также последствия этих преступлений имеют существенные отличия, как и субъектный состав и субъективная сторона подобных преступлений.

На основе анализа и систематизации обязательных и факультативных признаков этих видов преступлений, отличающих их от признаков преступлений первой группы, в данной группе также можно выделить несколько подгрупп подобных киберпреступлений.

В третью группу предлагается включить ряд принципиально новых видов киберпреступлений в сфере экономики и финансов, которые совершаются в информационном пространстве компьютерных сетей с использованием определенной совокупности информационных систем, в том числе иностранных, функционирующих по определенным правилам в системе цифровых прав.

По результатам проведенных исследований в этой группе также можно выделить *ряд подгрупп* киберпреступлений, связанных с манипулированием рынков эмиссионных ценных бумаг – акций и облигаций различного вида, неэмиссионных ценных бумаг, выпускаемых в электронном виде и обращаемых с помощью определенных информационных систем, производных финансовых инструментов – форвардных контрактов, фьючерсов, депозитарных расписок и иных деривативов, биржевым и межбанковским оборотом иностранной валюты, а также с биржевым оборотом различных товаров.

Эта группа киберпреступлений имеет принципиальные отличия от первой и второй группы, которые уже подробно обсуждались выше.

Многие ученые и специалисты предлагают иные принципы для классификации киберпреступлений в сфере цифровой экономики и финансов. Их обсуждение выходит за рамки настоящей работы. Здесь лишь необходимо еще раз обратить внимание на ряд особенностей цифровых прав, используемых преступниками на разных стадиях приготовления, совершения и сокрытия киберпреступлений рассматриваемого вида. И прежде всего, речь идет об их связях с правилами информационных систем, в том числе иностранных, установленных законодателем.

В рамках киберпреступлений в финансово-экономической сфере выделается также значительная часть преступлений «смешанного» вида, которые совершаются, в том числе, с использованием определенных информационных

систем, что также требует выполнения анализа особенностей их правил. Поэтому при формировании соответствующих критериев для классификации киберпреступлений в различных сферах экономики и финансов эти аспекты должны учитываться.

Результаты проведенных исследований указывают на необходимость использования не «плоской», а *многомерной, матричной классификации таких преступлений*. Ее основы уже отражены в описанной выше иерархической структуре выделения основных групп и подгрупп киберпреступлений. Но введение дополнительных критериев, связанных с особенностями таких преступлений, требует новых, матричных подходов к их классификации. Аналогичные подходы могут использоваться и для классификации киберпреступлений иных видов.

Анализ особенностей правоприменения в рамках системы цифровых прав на уровне правил информационных систем, установленных их российскими и иностранными обладателями, показывает возникновение новых вызовов созданной системе уголовно-правовой защиты российских экономических субъектов различных видов и уровней. При этом речь идет не только о проблемах, связанных с несоответствием правил российских или иностранных информационных систем требованиям российского законодательства.

Нередко российские экономические субъекты добровольно соглашаются на формирование договорных отношений в сфере цифровых прав по правилам иностранных информационных систем, понимая, что защитить свои интересы в судах соответствующих государств окажется вряд ли возможно. Подобные ситуации открывают международному криминалу ряд новых возможностей для разработки преступных схем с участием российских и иностранных субъектов цифровых прав, включая обладателей цифровых финансовых активов.

Соответственно, следует ожидать от высокотехнологичного криминала не только новых сюрпризов технического характера, подобных использованию в преступных целях блокчейн-технологии, квантовых компьютеров и иных достижений в сфере информатики и кибернетики. Значительно активизируется «правотворчество» обладателей информационных систем по введению правил, создающих ряд специфических особенностей работы с информацией в компьютерно-сетевом виртуальном пространстве, характерных для правил иностранных информационных систем. Вполне очевидно, что такие правила ориентируются на правоприменение в рамках американской юрисдикции.

В данной ситуации существенно возрастает актуальность постановки и выполнения комплекса научных исследований и разработок, нацеленных на информационно-математическое моделирование девиантного поведения субъектов цифровых прав. По результатам соответствующих разработок можно сделать ряд предварительных выводов об особенностях формирования соответствующих «краевых задач» в рамках серии «последовательных приближений».

Наиболее сложные из них характерны для преступлений, связанных с манипулированием рынком, отличающихся не только высочайшей латентностью, но и использованием вероятностной модели совершения

преступных деяний в диспозиции уголовно-правовой нормы. При этом в нее заложена целевая установка на защиту от влияния криминала процессов рыночного ценообразования на ценные бумаги, производные финансовые инструменты и иные объекты, торгуемые на биржах. В то же время, квалифицирующим признакам специальных субъектов, совершающих данные преступления с использованием своих профессиональных компетенций и информационных технологий, должного внимания не уделено[1].

Кроме того, при выполнении моделирования преступлений в сфере цифровой экономики и финансов важно учитывать особенности их расследования. Они связаны не только с математическими особенностями формирования обязательных и факультативных признаков преступления, для выявления которых необходимо применение достаточно сложных алгоритмов математических расчетов. В соответствии с действующим законодательством все эмиссионные ценные бумаги выпускаются в виде электронных документов, а их регистрация, совершение сделок, оплата и регистрация прав нового обладателя осуществляется только в соответствующих информационных системах. Но порядок использования электронных документов и иной информации при формировании доказательств по уголовному делу пока еще законодательно не установлен.

Важно обратить внимание, что в рамках уголовно-процессуального законодательства уже фактически заложен ряд алгоритмов выявления и обработки информации, имеющей значение для уголовного дела. Применение их определенной совокупности для формирования необходимых доказательств по уголовному делу, их проверки и оценки, включая установление достаточности собранной совокупности доказательств, описано в недавно выпущенной книге[2]. Но для практической реализации тех возможностей, которые заложены в указанные выше юридические и математические алгоритмы, необходимо создание на их основе ряда специализированных компьютерных программ.

Здесь важно иметь в виду, что при создании современного программного обеспечения широко используются стандартизованные программные модули, позволяющие реализовать те процедуры обработки информации, которые предусмотрены описанными выше алгоритмами. Некоторые из разрабатываемых алгоритмов могут быть нацелены на создание соответствующих интерфейсов, позволяющих использовать уже имеющееся стандартизованное программное обеспечение.

Следует подчеркнуть, что описание данных алгоритмов на русском языке с использованием ряда специальных символов и схем открывает принципиально новые возможности для создания таких криминалистических и экспертных методик по преступлениям в сфере цифровых прав, которые будут одинаково

[1] Особенности уголовно-правовой характеристики преступлений, связанных с манипулированием рынком: научно-практическое пособие / В.А. Прорвич, А.П. Опальский, Е.В. Иванов, А.А. Лебедева, С.Д. Нартов, О.В. Залевский, В.А. Кузьменко. // Под ред. проф. В.А. Прорвича и проф. А.П. Опальского. – М.: Альпен-Принт, 2021.

[2] Новиков А.М., Прорвич В.А. Доказательства и доказывание в следственной практике: учебное пособие. М.: Московская академия Следственного комитета России, 2022.

понятны как следователям, так и другим участникам уголовного судопроизводства.

Не менее важно обратить внимание и на то, что в рамках данного подхода может быть создан и соответствующий инструментарий для формирования государственной системы сертификации компьютерных программ, используемых в уголовном судопроизводстве, в том числе, для получения, проверки и оценки необходимых доказательств о преступлениях рассматриваемого вида. Это позволит обеспечить выполнение ряда установок, сформулированных в рамках основ государственной политики в области обеспечения безопасности критической информационной инфраструктуры российской экономики и финансов.

Е.Н. Рахманова

Противодействие киберпреступности в Ассоциация государств Юго-Восточной Азии (АСЕАН)

Аннотация. Государства-члены АСЕАН сегодня лидеры среди государств с быстрорастущей цифровой экономикой. Это заставило Ассоциацию больше внимания обращать на риски и проблемы, связанные с киберпреступностью. На национальное законодательство в области киберпреступности влияние оказывают как международные документы, так и особенности каждого из государств. В то же время рост киберпреступлений, не ограниченных национальными границами, пространством и расстоянием, приводит к пониманию необходимости гармонизации законодательства в сфере кибербезопасности.

Ключевые слова: АСЕАН, законодательство, киберпреступность, кибербезопасность, противодействие.

Ассоциация государств Юго-Восточной Азии (АСЕАН) с населением более 650 млн человек в 10 странах мира быстрорастущий и третий по численности населения регион. Согласно Глобальному цифровому отчету за 2020 г., средний уровень проникновения Интернета в Юго-Восточной Азии составляет около 66 %[1]. Данные показатели постоянно растут на протяжении последних несколько лет и не показывают признаков замедления. Так, если в 2000 г. общее число интернет-пользователей в Таиланде составило примерно 2,3 млн пользователей, то в 2022 г.- 61,9 млн человек или 88% всего населения, в Малайзии - 93%, в Сингапуре - 92%, в Индонезии -72%, Мьянме 51%, в Камбодже – 57%[2]. В свою очередь число пользователей смартфонами достигло 326,3 млн в 2022 году, что

[1] 2020 Digital Global Report. URL: www.wearesocial.com (Дата обращения: 11.04.2023).

[2] Internet 2022 Usage in Asia. URL: https://www.internetworldstats.com/stats3.htm (Дата обращения: 11.04.2023).

составляет 88,0% всего населения АСЕАН[1].

АСЕАН основана 8 августа 1967 года. В ее состав входят 10 стран: Индонезия, Малайзия, Сингапур, Таиланд, Филиппины, Бруней, Вьетнам, Лаос, Мьянма и Камбоджа. Согласно Декларации АСЕАН 1967 г. (Бангкокская декларация)[2], Ассоциация создана для содействия региональному миру и стабильности в Юго-Восточной Азии, а также для поощрения активного сотрудничества и взаимной помощи по вопросам, представляющим общий интерес. Несмотря на то, что в 1967 году кибербезопасность не упоминалась в Бангкокской декларации, но она и иные соглашения заложили основу для регионального сотрудничества против киберпреступности и поддержки региональной кибербезопасности.

Компьютерные и цифровые технологии все больше интегрируются в повседневную жизнь региона. Значительное влияние на ситуацию оказала пандемия COVID-19, которая вынудила правительства и бизнес ускорить цифровую трансформацию, что, с одной стороны, имеет очевидный положительный экономический эффект, но, с другой стороны, преступники начали активно использовать его в своих интересах. Например, в Малайзии в 2020 году было зафиксировано 5 697 случаев кибермошенничества, в то время как за аналогичный период 2019 года 4 671. Аналогичная ситуация наблюдается и в других странах. При этом трансграничный характер и сложность киберпреступлений затрудняет их расследование.

Дискуссия о необходимости развития законодательства в сфере кибербезопасности началась в 2016 году на Министерской конференции АСЕАН по кибербезопасности (AMCC), состоявшейся во время Сингапурской международной кибернедели (SICW). В 2017 г. были приняты Стратегия сотрудничества АСЕАН в области кибербезопасности и Декларация АСЕАН о предотвращении киберпреступности и борьбе с ней.

За последние годы большинство государств-членов АСЕАН приняли законодательство о киберпреступности в таких областях как мошенничество и подделка документов, детская порнография и нарушения конфиденциальности, целостность и доступность компьютерных данных и систем и др. Но в связи с тем, что национальные приоритеты у каждого государства, входящего в АСЕАН, свои и зачастую не совпадают, возникают трудности в применении и гармонизации законодательства. В частности, по-разному определяется преступное поведение в киберпространстве, по-разному собираются и оцениваются электронные доказательства для расследования киберпреступлений и т.д. При этом поскольку киберпреступления носят, в основном, транснациональный и трансграничный характер, преступники используют существующие различия в законодательствах, что не может не осложнять трансграничное сотрудничество государств-членов АСЕАН.

---

[1]Southeast Asia Digital Users Forecast 2022. Rising Connectivity Is Driving Commerce Opportunities. URL: https://www.insiderintelligence.com/content/southeast-asia-digital-users-forecast-2022 (Дата обращения: 09.04.2023).

[2]ASEAN Declaration, 1967 (Signed in Bangkok, Thailand on 8 August 1967). URL: https://cil.nus.edu.sg/wp-content/uploads/2019/02/1967-ASEAN-Declaration.pdf (Дата обращения: 11.04.2023).

Наиболее эффективным способом взаимодействия и единственным пока работающим механизмом, связывающим воедино законы принимающей и запрашивающей стран, являются межгосударственные договоры о взаимной правовой помощи. Кроме того, в 2006 году государства-члены АСЕАН подписали общий Договор о взаимной правовой помощи по уголовным делам[1]. Но различия в правовых системах стран-членов, например, в понимании принципа двойной уголовной ответственности, являются серьезным препятствием для его реализации.

Большое влияние на развитие законодательства в сфере кибербезопасности АСЕАН оказывала и оказывает Конвенция Совета Европы о киберпреступности (Российская Федерация Конвенцию не ратифицировала)[2]. И поскольку к ней помимо государств-членов Совета Европы присоединись государства не входящие в него (например, Япония, Панама и Израиль) фактически она получила международный статус.

Из государств-членов АСЕАН пока единственной страной, которая ее подписала и ратифицировала, являются Филиппины. Как указал по этому поводу Председатель сенатского комитета по РСМД Лорен Легарда, «этот договор очень важен для защиты нашего народа от киберпреступности, особенно потому, что страна является убежищем номер один для тех, кто занимается детской порнографией». Ссылаясь на данные ЮНИСЕФ он обратил внимание на то, что в мире детской порнографии Филиппины занимают первое место. Восемь из каждых 10 филиппинских детей подвержены риску сексуального насилия или издевательствам в Интернете[3]. Остальные страны хотя и не присоединись к Конвенции, но стараются при разработке законодательства о киберпреступности учесть ее положения.

Интерес представляет законодательство Сингапура наиболее хорошо разработанное в АСЕАН. Вниманию Сингапура к проблемам кибербезопасности во многом способствовал рост кибератак и киберпреступлений. В последние годы они составляют почти одну пятую всех преступлений, совершенных в стране[4]. Приняты Закон о кибербезопасности[5], который имеет экстерриториальное действие и применяется, даже если преступление

---

[1] Yoserwan (2020) Harmonization of Law on Mutual Legal Assistance by Indonesia in Eradicating Transnational Economic Crime in ASEAN Economic Community //Advances in Social Science, Education and Humanities Research, V. 549. P.24-31.

[2] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: https://base.garant.ru/4089723/ (дата доступа: 11.04.2023).

[3] Senate approves treaty against cybercrime, child pornography. URL: https://www.rappler.com/nation/196437-senate-concur-ratification-budapest-convention-on-cybercrime/ (Дата обращения: 11.04.2023).

[4] Hariz Baharudin, Fewer cyber threats detected here last year, but online crime still rising: CSA report //The Straits Times (18 June 2019). URL: https://www.straitstimes.com/tech/cyber-crime-still-rising-accounts-for-almost-a-fifth-of-all-crime-in-singapore-csa-report (дата обращения: 10.04.2023).

[5] Cybersecurity Act 2018. URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/ (Дата обращения: 10.04.2023).

совершено за пределами Сингапура или лицом, проживающим за пределами Сингапура; Закон о защите персональных данных[1]; Закон о неправомерном использовании компьютеров[2]; вносятся изменения и дополнения в отраслевое законодательство, прежде всего, в уголовное.

Киберпреступления включают а) преступления, совершаемые при помощи компьютера (например, мошенничество в сети, вымогательство); и (б) преступные действия, направленные против компьютера/компьютерных систем (например, взлом). При этом киберпреступность находится в ведении Министерства внутренних дел и полиции Сингапура, а кибербезопасность, которая предполагает создание мер по предотвращению несанкционированного доступа или использования компьютера, или компьютерной системы и ее данных, находится в ведении Агентства кибербезопасности.

Отправной точкой борьбы с киберпреступлениями в данной стране является Закон о неправомерном использовании компьютеров. Он распространяется на несанкционированный доступ, использование или модификацию компьютеров, компьютерных материалов и компьютерных услуг.

Помимо преступлений, предусмотренных Законом, киберпреступления подпадают под действие Уголовного кодекса и Закона о защите от домогательств. В частности, УК предусматривает ответственность за онлайн-мошенничество, которое в связи с анонимностью в Интернете и упрощением совершения транзакций превратилось для Сингапура и остальных стран АСЕАН в серьезную проблему. Онлайн-мошенничество может также включать вымогательство по электронной почте, когда, например, мошенники угрожают опубликовать скриншоты жертвы, просматривающей порнографические материалы. Подобные действия признаются преступлением и в соответствии со ст. 385 УК наказывается лишением свободы на срок от 2 до 5 лет с избиением палкой.

Завершая краткий анализ, следует признать, что государства-члены АСЕАН также, как и сама Ассоциация добились определенного прогресса в повышении кибербезопасности за счет развития соответствующих программ, активной работы над созданием законодательства в сфере киберпреступности с учетом требований международного права. При этом перед АСЕАН стоит сложная задача — достижение консенсуса ее участников в области предупреждения киберпреступности. Очевидно, что ключом к успеху в борьбе с киберпреступностью является не только создание нормативной базы, но и гармонизация законов против киберпреступлений, а также постоянное сотрудничество государств в этой сфере как внутри АСЕАН, так и с другими странами.

[1] Personal Data Protection Act 2012. URL: https://sso.agc.gov.sg/Act/PDPA2012 (Дата обращения: 10.04.2023).

[2] Computer Misuse Act 1993 (This revised edition incorporates all amendments up to and including 1 December 2021 and comes into operation on 31 December 2021). URL: https://sso.agc.gov.sg/Act/CMA1993 (Дата обращения: 10.04.2023).

Литература

1. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. URL: https://base.garant.ru/4089723/ 2020
2. ASEAN Declaration, 1967 (Signed in Bangkok, Thailand on 8 August 1967) – URL: https://cil.nus.edu.sg/wp-content/uploads/2019/02/1967-ASEAN-Declaration.pdf.
3. Digital Global Report - URL: www.wearesocial.com
4. Computer Misuse Act 1993 (This revised edition incorporates all amendments up to and including 1 December 2021 and comes into operation on 31 December 2021). URL: https://sso.agc.gov.sg/Act/CMA1993
5. Cybersecurity Act 2018. URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/
6. Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
7. Hariz Baharudin (2019) Fewer cyber threats detected here last year, but online crime still rising: CSA report //The Straits Times (18 June 2019). URL: https://www.straitstimes.com/tech/cyber-crime-still-rising-accounts-for-almost-a-fifth-of-all-crime-in-singapore-csa-report
8. Internet 2022 Usage in Asia. URL: https://www.internetworldstats.com/stats3.htm
9. Personal Data Protection Act 2012. URL: https://sso.agc.gov.sg/Act/PDPA2012
10. Senate approves treaty against cybercrime, child pornography. URL: https://www.rappler.com/nation/196437-senate-concur-ratification-budapest-convention-on-cybercrime/
11. Southeast Asia Digital Users Forecast 2022. Rising Connectivity Is Driving Commerce Opportunities. URL: https://www.insiderintelligence.com/content/southeast-asia-digital-users-forecast-2022
12. Yoserwan (2020) Harmonization of Law on Mutual Legal Assistance by Indonesia in Eradicating Transnational Economic Crime in ASEAN Economic Community //Advances in Social Science, Education and Humanities Research, V. 549. P.24-31

М.М. Савченко

Хищения денежных средств в условиях экспансии современных цифровых технологий

Аннотация. В статье рассматриваются тенденции последних лет по стремительному увеличению количества хищений денежных средств, совершаемых с применением цифровых технологий. В основном, это происходит за счет роста краж безналичных денежных средств и мошенничеств с использованием электронных средств платежа. На основе статистических данных формулируется вывод, что основная часть хищений

совершается без использования сложных технических и программных средств, так как основана на воздействие методами социальной инженерии. Формулируются рекомендации для разработки организационных мер банковской безопасности, а также для правоохранительных органов по противодействию хищениям денежных средств с банковских счетов.

Ключевые слова: хищения, банковская карта, безналичные расчеты, электронное средство платежа, электронные деньги.

В последние годы в России наблюдается стремительное развитие дистанционных каналов банковского обслуживания. Количественный и качественный рост объемов операций с применением цифровых технологий, влияет на повышение привлекательности данного сектора для преступного сообщества.

Согласно статистике Банка России за последние десять лет резко выросло количество и объем операций по оплате товаров и услуг с использованием платежных карт: с 997,9 млн. (1 141 млрд. руб.) в 2010 году до 18129,8 млн. (40639,4 млрд. руб.) в 2022 году – то есть частота использования электронных средств платежа увеличилась более чем в 20 раз[1]. Общее количество счетов с дистанционным доступом также значительно увеличилось: с 52586,9 тыс. в 2010 году до 358 556,2 тыс. – на 01.01.2023 года.

Анализ доступности финансовых услуг в России позволяет делать вывод о достаточно высоком уровне основных среднедушевых показателей по сравнению с большинством стран, а по некоторым из них – о лидирующих позициях. Общее количества точек оказания платежных услуг в 2022 году достигло 4,6 млн единиц. [2].

Вместе с тем, наблюдается рост числа инцидентов информационной безопасности при переводе денежных средств, который заключается в увеличении числа и объемов банковских и платежных операций, совершаемых без согласия клиентов.

Анализ структуры операций в разрезе условий их проведения позволяет сделать вывод от том, что за период с 2015 по 2022 год существенно не меняется общий объем несанкционированных операций, совершенных через банкоматы и платежные терминалы, при этом весь стремительный рост достигается за счет операций, производимых с использованием сети Интернет и устройств мобильной связи (CNP-транзакций).

При анализе количества операций, совершенных без согласия клиентов, наблюдается постоянный рост доли таких операций, совершенных с использованием социальной инженерии. В 2021 году зафиксировано 83,9 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкоматах или терминалах на общую сумму 1 971,2

[1] Банк России. Статистика национальной платежной системы. https://www.cbr.ru/statistics/nps/psrf/

[2]Банк России. Индикаторы финансовой доступности за 2022 год. https://www.cbr.ru/Content/Document/File/145896/fin_uslugi_23.pdf

млн руб., из которых 22,5% операций произошло в результате использования злоумышленниками приемов и методов социальной инженерии.

На основании Формы федерального статистического наблюдения № 4-ЕГС, а также ведомственного отчета МВД России формы 1-А, проведено исследование объемов, структуры и динамики преступных посягательств, совершенных с использованием современных цифровых технологий, регистрируемых правоохранительными органами. В разделе 2 формы № 4 ЕГС содержится информация о зарегистрированных преступлениях по статьям Уголовного кодекса Российской Федерации[1].

Преступления, совершенные с использованием ДБО и электронных средств платежа, посягающие на денежные средства, размещенные на банковских счетах, с могут быть квалифицированы по различным статьям УК РФ.

Основными нормами, предусматривающими ответственность за такие деяния, являются:

- пункт «Г» части 3 статьи 158 УК РФ – «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3)»;

- статья 159.3 УК РФ – «Мошенничество с использованием электронных средств платежа»;

- статья 159.6 УК РФ – «Мошенничество в сфере компьютерной информации»[2]

Разграничение данных составов между собой в некоторых случаях является сложной задачей, что обусловливает неоднородную правоприменительную практику[3].

Анализ раздела 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий (ИТТ) или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации» формы №4-ЕГС позволяет сделать вывод о том, что в общей структуре краж наблюдаются определенные изменения. Так, за период 2018 – 2021 год, происходит значительный рост тайных хищений денежных средств, совершенных с использованием ИИТ: с 4942 в 1 квартале 2018 года до 49008 в 4 квартале 2021 года – то есть почти в 10 раз, при этом доля краж с использованием ИТТ в их общем количестве в последний квартал 2021 года составила более 25%.

По хищениям, совершенным с использованием обмана и злоупотребления доверием, наблюдается еще более существенное изменение структуры. Анализ показывает, что существенный рост (более чем в 3 раза) количества мошеннических деяний, совершенных с использованием ИТТ, происходит с одновременным сокращением, как доли, так и общего количества прочих

---

[1] Генеральная прокуратура Российской Федерации. Портал правовой статистики. http://crimestat.ru/analytics.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (действующая редакция) // СПС «КонсультантПлюс».

[3] Савченко М.М. Проблемы уголовно-правовой защиты безопасности денежных средств физических лиц, размещенных на счетах в банках // Юридическое образование и наука. 2021. № 4. С. 34 – 40.

мошенничеств. Так, в 4 квартале 2021 года с применением ИТТ совершено более 75% от всех зарегистрированных преступлений, предусмотренных статьями 159-159.6 УК РФ.

Приведенная выше статистика имеет прямую корреляцию с информацией, содержащейся в аналитических отчетах Банка России о высокой доле социальной инженерии в общем количестве операций, совершенных без согласия клиентов. Так, в 2022 году 50,4% хищений со счетов граждан совершалось с использованием методов социальной инженерии.

Термин «социальная инженерия» не имеет толкования в российском законодательстве и других нормативно-правовых актах, хотя достаточно часто применяется в контексте уязвимости систем банковской безопасности[1].

Таким образом, хищения, совершенные с использованием приемов и методов социальной инженерии (в том значении, в котором данный термин уже получил широкое распространение[2]) выходят за рамки одного вида преступлений, квалифицируемых как мошенничества. Приемы обмана, незаконного завладения конфиденциальной информацией и персональными данными, часто могут быть использованы также как промежуточные этапы тайных хищений денежных средств (кражи) со счетов с использованием платежных карт и систем удаленного банковского обслуживания.

Проведенное исследование позволяет сформулировать следующие выводы:

1. Рост количества посягательств, совершенных с использованием цифровых информационно-коммуникационных технологий связан в первую очередь с увеличением видов применяемых технологий и общего количества совершаемых операций.

2. Увеличение количества хищений денежных средств, совершенных с использованием цифровых информационно-телекоммуникационных технологий происходит, в том числе, за счет сокращения числа соответствующих видов деяний, совершенных иными способами.

2. Программно-техническая часть систем банковской безопасности, имея определенные уязвимости, в основном, способна устоять перед информационными атаками злоумышленников, так как постоянно развивается и на ее преодоление требуются достаточно большие временные и материальные затраты.

3. Наиболее уязвимыми для преступных посягательств остаются направления, непосредственно связанные с человеческим фактором в виде незаконного использования персональных данных либо разглашения конфиденциальной платежной информации самими потерпевшими.

4. Источниками утечки персональных данных чаще всего являются не банки,

---

[1] Полозюк, А. Г. С. С. Коняхина. Социальная инженерия - угроза информационной безопасности // Приоритетные научные направления: от теории к практике. – 2016. – № 29. – С. 68-72.

[2] Киселев, А. Ю. Социальная инженерия: человеческий фактор как проблема информационной безопасности // Дыльновские чтения : Материалы IV международной научно-практической конференции, Саратов, 10 февраля 2017 года. – Саратов: Издательство «Саратовский источник», 2017. – С. 169-173.

а другие операторы персональных данных: доски объявлений, сайты интернет-продаж, анкеты систем лояльности торгово-сервисных предприятий.

Таким образом, основные меры снижения количества несанкционированных операций и профилактики преступности в сфере дистанционного банковского обслуживания должны быть реализованы по следующим направлениям:

- информирование владельцев банковских счетов о наиболее распространенных способах совершения хищений;
- техническое усложнение доступа клиентов к определенным действиям в рамках дистанционного обслуживания: например, восстановление доступа к личному кабинету с использованием двух-трех-факторной идентификации; дополнительная идентификация при проведении операций свыше определенного лимита;
- дифференцированный подход к клиентам, позволяя им выбрать не только полный дистанционный режим доступа ко всем счетам и продуктам банка, но и ограниченный профиль (например, отключение от ДБО срочных вкладов, исключение возможности получения онлайн кредитов и т.п.).

Сформулированные подходы и рекомендации могут быть полезны как при разработке организационных мер банковской безопасности, так и в работе правоохранительных органов по противодействию хищениям денежных средств с банковских счетов.

Литература

1. Киселев, А. Ю. Социальная инженерия: человеческий фактор как проблема информационной безопасности // Дыльновские чтения : Материалы IV международной научно-практической конференции, Саратов, 10 февраля 2017 года. – Саратов: Издательство "Саратовский источник", 2017. – С. 169-173.
2. Полозюк, А. Г. Социальная инженерия - угроза информационной безопасности / А. Г. Полозюк, С. С. Коняхина // Приоритетные научные направления: от теории к практике. – 2016. – № 29. – С. 68-72.
3. Савченко М.М. Проблемы уголовно-правовой защиты безопасности денежных средств физических лиц, размещенных на счетах в банках // Юридическое образование и наука. 2021. № 4. С. 34 – 40.
4. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (действующая редакция) // СПС «КонсультантПлюс».

А.Ж. Саркисян

О киберпространстве в Российской Федерации (уголовно-правовой аспект)

Аннотация. В статье на основе анализа юридической литературы и законодательства о киберпространстве в Российской Федерации обосновано несколько суждений: термин «киберпространство» используется в научной

юридической литературе; термин «киберпространство» используется в законодательстве Российской Федерации, но как правило в подзаконных нормативных правовых актах; использование термина «киберпространство» и в научной юридической литературе и в законодательстве Российской Федерации необходимо признать необоснованным, ввиду неопределенности этого термина; в уголовном законодательстве целесообразно использовать термин «пространство», в том числе и для развития информационных технологий.

Ключевые слова: государство, Российская Федерация, законодательство, нормативный правовой акт, Конституция РФ от 12 декабря 1993 г., федеральный закон РФ, Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 8 июля 2006 г., Уголовный кодекс РФ, подзаконный нормативный правовой акт, сеть «Интернет», «киберпространство», пространство.

Предметом данной статьи является киберпространство, причем в уголовно-правовом аспекте, в Российской Федерации[1].

Первоначально о состоянии теории.

Так, авторы – единомышленники (Н.А. Молчанов и Е.К. Матевосова) сформулирловали «вывод о том, что меры укрепления доверия между государствами при отсутствии обязательных международно-правовых норм лишены инструментальной роли в разрешении многих проблем обеспечения безопасности в стремительно изменяющемся киберпространстве. Условием эффективного международного правотворчества в области информационной безопасности является диалог юристов, политиков и технических специалистов» («Коррелятивная связь правовых, организационных и технических мер обеспечения кибербезопасности требует от экспертного обсуждения любого вида и уровня тесного сотрудничества юристов, политиков и специалистов в поиске ответов на вопросы о том, какие обязательства государства готовы и должны на себя принимать, каким образом осуществлять контроль за их надлежащим исполнением и насколько предлагаемые меры реализуемы согласно внутренним законам и механике самого киберпространства»)[2].

Еще одна группа авторов – единомыленников (Н.А. Жильцов, О.И. Чердаков и С.Б. Куликов) говорят «о проблеме законодательного урегулирования правоотношений в киберпространстве, затрагиваются вопросы узаконения права собственности на виртуальные объекты онлайн-игр, предлагается авторское толкование понятий "социальная сеть", "интернет-пользователь", "виртуальная реальность", "цифровая среда", "виртуальное сообщество", "киберпространство"

[1] Мы разделяем суждение тех авторов, которые предлагают с 25.12.1991 г. для названия государства использовать исключительно этот термин (подробнее об этом см.: Галузо В.Н. Конституционно-правовой статус России: проблема именования государства // Вестник Московского университета МВД России. 2010. № 5. С. 119-123).

[2] См.: Молчанов Н.А., Матевосова Е.К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1. С. 133 - 141.

("виртуальное пространство" или "виртуальный мир" («Виртуальная реальность - искусственно созданный аппаратными средствами цифровой мир, позволяющий существовать виртуальному объекту в виде цифрового или оцифрованного образа, информационного или иного файла и интегрировать человека в виртуальный мир в виде цифрового объекта, аватара или иного суррогатного образа. Цифровая среда - виртуальное пространство, в котором существуют объекты виртуального мира и распространяются продукты цифровых технологий в форме электронных программ, цифровых платформ, где осуществляется обмен информацией. Виртуальное сообщество - это группа единомышленников, объединенная общими интересами с целью решения различного рода задач, начиная от коммуникации, обмена информацией и организации досуга, заканчивая коммерческими задачами. Киберпространство, или виртуальное пространство, или виртуальный мир - это электронно-цифровое пространство, созданное в интернет-сети, не имеющее территориальных границ, служащее для решения различного рода задач, начиная от социальных, заканчивая военными задачами»)[1].

Исследование Л.В. Терентьевой посвящено «условиям реализации суверенитета и юрисдикции государства в отношении внетерриториального информационно-коммуникационного пространства на платформе киберпространства» («В заключение следует отметить, что развитие киберпространства не обусловливает снижение значимости понятия "территория государства" как сферы распространения суверенной власти государства. Обогащение понятия "территория государства" на всем протяжении исторического развития за счет включения новых пространств (воздушные, морские и речные суда; космические корабли, станции и др.) при статике его правового значения, заключающегося в пространственных пределах осуществления полной юрисдикции государства, делает возможным расширение содержания данного понятия и за счет включения в него новых пространственных единиц, не имеющих территориального, осязаемого, плоскостного аспекта»)[2].

Многообразие суждений о киберпространстве во многом предопределено и несовершенством законодательства Российской Федерации.

В первую очередь обращаемся к Конституции РФ от 12 декабря 1993 г.[3] как к нормативному правовому акту с наивысшей юридической силой на территории Российской Федерации, в которой обнаруживаем несколько принципиально важных положений: «1. Российская Федерация - Россия есть демократическое федеративное правовое государство с республиканской формой правления» - ч. 1 ст. 1; «1. Каждому гарантируется свобода мысли и слова. 2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального,

[1] См.: Жильцов Н.А., Чердаков О.И., Куликов С.Б. Право в рамках киберпространства // Юрист. 2020. № 2. С. 58 - 65.

[2] Терентьева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве // Lex russica. 2019. № 7. С. 119 - 129.

[3] См.: РГ. 1993. 25 декабря; …; 2020. 4 июля.

расового, национального, религиозного или языкового превосходства. 3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них. 4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом. 5. Гарантируется свобода массовой информации. Цензура запрещается» - ст. 29.

Положения статьи 29 Конституции РФ относительно поиска и распространения информации обнаруживаем в Уголовном кодексе РФ от 24 мая 1996 г.[1]. В частности, в главе 2 (статьи 9-13) «Действие уголовного закона во времени и в пространстве»[2] относительно пространства нормы необходимо рассматривать в качестве бланкетных.

Термин «киберпространство» использован в подзаконных нормативных правовых актах: Постановление Правительства РФ «Об утверждении Правил предоставления в 2019 году субсидии из федерального бюджета бюджету Республики Саха (Якутия), источником финансового обеспечения которой являются бюджетные ассигнования резервного фонда Правительства Российской Федерации, в целях софинансирования расходных обязательств Республики Саха (Якутия), принимаемых в связи с организацией международной конференции высокого уровня "Сохранение языков народов мира и развитие языкового разнообразия в киберпространстве: контекст, политика, практика» № 859 от 5 июля 2019 г.[3].

Таким образом, исследования относительно киберпространства, причем в уголовно-правовом аспекте, в Российской Федерации необходимо продолжать.

Во-первых, термин «киберпространство» используется в научной юридической литературе.

Во-вторых, термин «киберпространство» используется в законодательстве Российской Федерации, но как правило в подзаконных нормативных правовых актах.

В-третьих, использование термина «киберпространство» и в научной юридической литературе и в законодательстве Российской Федерации необходимо признать необоснованным, ввиду неопределенности этого термина.

---

[1] См.: СЗ РФ. 1996. № 25. Ст. 2954; …; 2023. № 32 (часть I). Ст. 6145.

[2] Относительно термина «уголовный закон» в юридической литературе отмечается его несовершенство (см. об этом: Галузо В.Н. «Уголовный закон» или «уголовное законодательство» в Российской Федерации: проблема соотношения терминов / Актуальные проблемы современной науки. Секция «Право и правоприменение»: Сборник материалов международной научно-практической конференции, 23 мая 2014 г. / Науч. ред. С.Л. Никонович. Тамбов-Липецк: Изд-во Першина Р.В., 2014; Галузо В.Н., Никонович С.Л. Уголовное законодательство в системе законодательства Российской Федерации / Актуальные проблемы уголовного законодательства на современном этапе: Сборник научных трудов международной научно-практической конференции. Волгоград, 14-15 мая 2015 г. / Отв. ред. В.И. Третьяков. Краснослободск (Волгоградская область): ИП Головченко Е.А., 2015. С. 117-123).

[3] См.: СЗ РФ. 2019. № 28. Ст. 3783.

В-четвертых, в уголовном законодательстве целесообразно использовать термин «пространство», в том числе и для развития информационных технологий.

Литература

1. Галузо В.Н. Конституционно-правовой статус России: проблема именования государства // Вестник Московского университета МВД России. 2010. № 5. С. 119-123.
2. Молчанов Н.А., Матевосова Е.К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1. С. 133 - 141.
3. Жильцов Н.А., Чердаков О.И., Куликов С.Б. Право в рамках киберпространства // Юрист. 2020. № 2. С. 58 - 65.
4. Терентьева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве // Lex russica. 2019. № 7. С. 119 - 129.
5. Галузо В.Н. «Уголовный закон» или «уголовное законодательство» в Российской Федерации: проблема соотношения терминов / Актуальные проблемы современной науки. Секция «Право и правоприменение»: Сборник материалов международной научно-практической конференции, 23 мая 2014 г. / Науч. ред. С.Л. Никонович. Тамбов-Липецк: Изд-во Першина Р.В., 2014.
6. Галузо В.Н., Никонович С.Л. Уголовное законодательство в системе законодательства Российской Федерации / Актуальные проблемы уголовного законодательства на современном этапе: Сборник научных трудов международной научно-практической конференции. Волгоград, 14-15 мая 2015 г. / Отв. ред. В.И. Третьяков. Краснослободск (Волгоградская область): ИП Головченко Е.А., 2015. С. 117-123.

А.В. Серебренникова

Уголовно-правовая характеристика киберпреступлений в контексте обеспечения национальной безопасности

Аннотация. Целью настоящего исследования является необходимость продемонстрировать корректность законодательного отражения понятия «киберпреступность», а также дать характеристику тем составам правонарушений, к которым законодатель относит именно киберпреступления. В ходе исследования автор дает оценку требованиям ряда источников права, предусматривающих основы уголовно-правового противодействия компьютерным преступлениям, а также форматам, позволяющим устанавливать их принципы.

Ключевые слова: киберпространство, преступность, соглашение, цифровизация, мошенничество, экстремизм, терроризм.

По мнению ряда исследователей, формат правового представления и качества правового регулирования зависит в основном от учёта соответствующих условий, позволяющих правильно устанавливать вектор развития социального взаимодействия. Иногда эти условия становятся настолько важными и даже жизненно необходимыми, что принятие правил их использования со стороны человека может незаметно для него формировать в нем же самом негативное начало. В частности, автор диссертационного исследования «Судебная юрисдикция по трансграничным частноправовым спорам в киберпространстве» Л.В. Терентьева ставит вопрос влияния киберпространства на контекст дальнейшего развития традиционных отношений очень остро. В частности ученым подчёркивается необходимость тщательного пересмотра тех фундаментальных правовых начал, которые стали основой для зарождения ныне существующих принципов правового регулирования. По её мнению, уникальные свойства киберпространства стали причиной для социальной деформации, а также серьёзным вызовом для правовой науки в целом. К одной из проблем стоит отнести введение новых юрисдикций, а также отраслевых принципов, позволяющих исключить всевозможные негативные последствия влияния «киберпространства» на пространство реальное. В особенности это относится к противоправной деятельности, ставшей сопутствующим явлением в развитии цифровых технологий[1].

Так или иначе, но понятие «киберпреступность» в доктринальной логике признается в качестве производного явления, по большей части выражающего не сколько что-то естественно опасное для жизни и здоровья человека, сколько образованное им же самим для своего личного удобства, но, порождающее негативное начало. Как следствие, под её идентификацией следует понимать любое социальное действие или противодействие, совершенное с целью причинения вреда посредством использования не только компьютера, но и любого другого сетевого устройства, позволяющего проникать в сеть[2]. Это общий принцип, который указывает на то, что любое действие, реализованное посредством компьютерной технологии, вне зависимости от суммы и размера причинённого вреда, следует относить к киберпреступлениям. Так, отдельные киберпреступления совершаются для получения денег. С другой стороны некоторые из них совершаются для уничтожения или отключения компьютерной системы. Некоторые из них есть следствие распространения информации посредством интернет-пространства, направленной на развитие социальной

[1] Терентьева Л.В. Судебная юрисдикция по трансграничным частноправовым спорам в киберпространстве: дисс…докт. юрид. наук. Специальность: 12.00.03 – гражданское право; семейное право; предпринимательское право; международное частное право. Москва, 2021. 328 с.

[2] Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: дисс…канд.юрид. наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Казань. 2008. 187 с.

деформации. Более же предметная характеристика её признаков была дана в специальном международном акте - Конвенции о компьютерных преступлениях[1]. Здесь авторами законодательной мысли о подобном типе социально опасных деяний на первый план выведены признаки в виде именно правонарушений (например, связанные с распространением детской порнографии (ст.9), или повлёкшие за собой нарушение авторских прав (ст.10), подлог (ст.7), и др.), либо в совершении действий, которые могут признаны таковыми в силу того, что они сопряжены с использованием цифровых технологий (перехват данных (ст.3), воздействие на данные (ст.4), воздействие на функционирование системы (ст.5)). Кроме этого, в представленном документе смоделированы и такие понятия, которые в силу необходимости оценки и установления факта киберпреступного вмешательства, носят сопутствующее значение: компьютерная система, компьютерные данные, данные о потоках, и др. В отдельное направление выделен аспект корпоративной, в том числе и предусматривающей уголовную, ответственности, которая должна быть установлена в отношении юридических лиц, принимающих на себя обязательства по защите и сохранению конфиденциальности сведений, предоставленных пользователями. Стоит отметить, что в 2005 году Президентом России было издано специальное Распоряжение «О подписании Конвенции о киберпреступности»[2], в соответствии с которым наша страна должна была присоединиться к действию указанного международного акта, однако, спустя некоторое время аналогичным решением[3] указанное распоряжение было отменено. Как утверждается в официальной ноте, причиной такого решения стали несогласия российской стороны с некоторыми положениями Конвенции, прежде всего, затрагивающих вопросы национальной безопасности государства, а, конкретно, его суверенитета. В частности, в пункте «b» статьи 32 указанной Конвенции отражено, что, исходя из принципа возможности реализации трансграничного доступа к хранящимся компьютерным данным любая из Сторон, которая приняла на себя обязательства по исполнению требований Конвенции, вправе получать компьютерную информацию независимо от её географического местоположения, что с одной стороны, указывает на возможности международного взаимодействия, с другой - становится причиной несанкционированного доступа к сведениям, находящимся под особой защитой другой страны[4]. Учитывая, что международные отношения очень сложны, а грани правового соприкосновения достаточно зыбки, Россия принимать

[1] Конвенция о компьютерных преступлениях от 2001 года // [Электронный ресурс]. URL: https://rm.coe.int/1680081580 (дата обращения: 30.10.2022).

[2] Распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» (утратило силу) // СЗ РФ. 21.11.05. № 47. ст. 4929.

[3] Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 31.03.2008. №13. ст. 1295.

[4] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Заключено в г. Минске 01.06.2001) // СЗ РФ. 30 марта 2009 г. № 13. Ст. 1460.

положения рассматриваемой Конвенции отказалась, однако, в распоряжении была сделана оговорка, которой устанавливалось, что такое взаимодействие возможно и без подписания указанного документа, а также в том случае, если упомянутое спорное положение будет пересмотрено.

В свою очередь, вопрос национальной безопасности в разрезе оценки и противодействию киберпреступности в нашей стране нашёл своё отражение в Доктрине информационной безопасности РФ[1], где впервые были смоделированы представления об основных объектах возможного преступного посягательства: информация, киберпространство, информационные системы, сайт, и иное.

Указывая на основные характеризующие признаки киберпреступлений, логично признать, что основу их разновидности составляет то, является ли компьютер (или компьютерное оборудование) средством совершения противоправного посягательства, либо его объектом. В первом случае речь идет о таких правонарушениях, когда цифровое устройство используется в качестве предмета преступления, к каким смело можно отнести следующие: хищение денежных средств посредством использования специальных программ или мошеннических навыков (фишинг), к другим можно отнести те случаи, когда объектом преступного посягательства является информация либо её носитель. И в том и в другом случае важнейшим фактором, характеризующим преступление именно как киберпреступление, является фактор использования специальной компьютерной технологии. Попробуем на конкретном примере рассмотреть аспект выражения киберпреступления в реальном пространстве. В частности, на сегодняшний день основной эффект киберпреступности - финансовый. Дело в том, что киберпреступность может включать в себя множество различных видов преступной деятельности, направленной на получение прибыли. Она, в частности, включает в себя мошенничество с электронной почтой и Интернетом. Кроме того, её активное распространение неразрывно связано с мошенничеством при использовании личных данных, а также попытками украсть финансовые счета, кредитные карты или другую информацию о платёжных картах. Киберпреступники могут использовать личную информацию физического лица, а также корпоративные данные для кражи и перепродажи. Так, составом ст. 159.6 Уголовного Кодекса РФ[2] установлено, что уголовная ответственность за хищение средств по указанной статье наступает только в том случае, если указанное хищение совершено посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Другим примером реализации указанного подхода может служат преступления, совершенные путём распространения информации через сети Интернет. Так, вполне закономерно, что большинство преступлений экстремистской

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. ст. 7074.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) // СЗ РФ. 17.06.1996. № 25. ст. 2954.

направленности совершаются посредством распространения влияющей на сознание граждан информации через специально созданные ресурсы или контенты. В частности, «кибертерроризм» определяется как любая угроза причинения вреда или вымогательства через Интернет. По мере увеличения мощности компьютеров и компьютерных систем кибертерроризм использует хорошо спланированные атаки на правительственные и корпоративные компьютерные системы. Такие атаки могут быть нацелены на стратегические службы, управляемые компьютером, такие как услуги электроснабжения, водоснабжения и связи. В свою очередь, правовая оценка кибертерроризма зиждется на том, что указанное явление представляет собой «использование компьютерных технологий для запугивания или принуждения правительства, гражданского населения или любого его сегмента исключительно в политических целях»[1]. В частности, в диспозиции ст. 282 УК РФ изначально было указано на то, что деяние, совершенное с использованием цифровых технологий, относится к общественно опасным и будет служить поводом для привлечения к уголовной ответственности. В данном случае законодатель, закладывая смысл в оценку влияния средств массовой информации на сознание граждан, заведомо ставит акцент на его использовании со стороны нарушителя. Аналогичное положение дел и в любых других составах преступлений, определяемых в диспозициях норм уголовного законодательства, предусматривающих наказание за нарушение правил «антиэкстремистского» законодательства.

Таким образом, уголовная характеристика преступлений, связанных с использованием компьютерной техники, позволяет констатировать то, что их сущность замыкается на два основных фактора: использование средств компьютерной информации в качестве предмета преступления и когда объектом преступления является именно сам компьютер или его программа. И в том и в другом случае объективная сторона деяния будет характеризоваться действием, направленным на умышленную реализацию преступного умысла за счёт наличия в распоряжении субъекта знаний о функционировании компьютерной информации, её свойствах, а также непосредственного влияния на социальное пространство.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) // СЗ РФ. 17.06.1996. № 25. ст. 2954.
2. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Заключено в г. Минске 01.06.2001) // СЗ РФ. 30 марта 2009 г. № 13. Ст. 1460.

[1] Мартиросян А.Ж. Кибербезопасность и международное морское право: обзор актуальных международно-правовых проблем в области киберпреступности / А. Ж. Мартиросян // Электронное сетевое издание «Международный правовой курьер». – 2020. – № 12. – С. 41-50.

3. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. ст. 7074.
4. Распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» (утратило силу) // СЗ РФ. 21.11.05. №47. ст. 4929.
5. Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 31.03.2008. №13. ст. 1295.
6. Дзялошинский И.М. Медиа как пространство угроз: 15 лет в тени доктрины информационной безопасности1 / И.М. Дзялошинский, М.И. Дзялошинская // Коммуникации. Медиа. Дизайн. – 2016. – Т. 1. – № 1. – С. 7-33.
7. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: дисс…канд.юрид. наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Казань. 2008. 187 с.
8. Мартиросян А.Ж. Кибербезопасность и международное морское право: обзор актуальных международно-правовых проблем в области киберпреступности / А. Ж. Мартиросян // Электронное сетевое издание «Международный правовой курьер». – 2020. – № 12. – С. 41-50.
9. Терентьева Л.В. Судебная юрисдикция по трансграничным частноправовым спорам в киберпространстве: дисс…докт. юрид. наук. Специальность: 12.00.03 – гражданское право; семейное право; предпринимательское право; международное частное право. Москва, 2021. 328 с.
10. Конвенция о компьютерных преступлениях от 2001 года // [Электронный ресурс]. URL: https://rm.coe.int/1680081580 (дата обращения: 30.10.2022).

С.Ю. Скобелин

Направления деятельности лаборатории цифровых компетенций

Аннотация. Рассматривается практическая востребованность создания на базе Московской академии Следственного комитета лаборатории (криминалистического центра) цифровых компетенций. Предлагается юридическая основа ее организации, цели, задачи и принципы деятельности. Намечены основные перспективные направления работы и развития.

Ключевые слова: Киберпреступления, цифровые следы, раскрытие, расследование, навыки, компетенции, следователь, эффективность, центр цифровых компетенций.

Масштабы киберпреступлений, ранее не известные способы их совершения, изменившийся криминологический портрет лиц, совершающих такие преступления, их мотивы требуют от ведомственных образовательных учреждений правоохранительных органов инновационных подходов и расширения возможностей обучения следователей и экспертов, специализирующихся на расследовании преступлений в сфере высоких технологий, в том числе с использованием криптовалют.

В соответствии с разделом 4 Протокола поручений Председателя Следственного комитета Российской Федерации (№ поруч-45-22 от 29.12.2022) по итогам оперативного совещания по вопросам противодействия киберпреступности и применения цифровых технологий при расследовании преступлений, а также п.5.6. Приказа №19 от 30.01.2023 г. «Об организации работы по расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий», Московской академии Следственного комитета необходимо проработать вопрос создания и оборудования на базе вуза киберполигона, позволяющего моделировать различные компьютерные инциденты (в том числе киберпреступления) и следственные действия для формирования у обучающихся необходимых практических навыков для расследования подобных преступлений.

В настоящее время подготовлен проект Концепции цифровизации предварительного расследования в Следственном комитете Российской Федерации, предусматривающий широкий спектр стратегических задач и направлений работы, взаимодействия как внутриведомственных, так и межведомственных служб и подразделений, негосударственных и межгосударственных органов в целях эффективного противодействия киберпреступности.

Стратегической площадкой Следственного комитета Российской Федерации для обобщения и поиска решений перечисленных вопросов могла бы выступить лаборатория цифровых компетенций Московской академии Следственного комитета, основными направлениями деятельности которой выступили:

1) Обеспечение на основе анализа актуальных проблем правоприменительной практики и научных изысканий в области противодействия киберпреступности разработок новейших методик и приемов предупреждения, выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий;

2) Орагнизация и актуализация цифровой библиотеки по вопросам работы с цифровыми следами, тактики следственных и иных процессуальных действий, методик раскрытия и расследования киберпреступлений;

3) Внедрение мониторинговой системы поиска криминалистически значимой информации в открытых Интернет источниках;

4) Участие в формировании и ведении криминалистического учета электронных следов преступлений;

5) Оказание практической помощи территориальным следственным органам в форме повышения эффективности профессиональной деятельности сотрудников следственных и криминалистических подразделений Следственного комитета Российской Федерации на основе широкого внедрения современных высоко технологичных отечественных криминалистических средств и методов, специальной техники в раскрытии и расследовании киберпреступлений;

6) Внедрение в учебный процесс современных образцов высокотехнологичной криминалистической техники, специальных программ,

инновационных технологий методов и средств обучения, компьютеризации в целях всесторонней интенсификации и повышения качества учебного процесса (учебные фильмы, обучающие компьютерные программы, презентации, интервью и т.п.)

7) Повышение квалификации следователей и экспертов;

8) Выполнение научно-исследовательских работ по заявкам практических органов области форензики, лжефорензики, исследования цифровых следов преступной деятельности в сети Интернет и т.п.;

Опытной площадкой Лаборатории должен стать киберполигон, функциями которого являются:

1) Разработка актуальных компьютерных кейсов (следственных ситуаций), практикумов, связанных с подготовкой, совершением, сокрытием киберпреступлений (раскрытие и расследование неочевидных преступлений, связанных с посягательствами на половую неприкосновенность несовершеннолетних; доведения (склонения) их до самоубийств; вовлечения в экстремистские формирования, участие в них; организация и заказ преступлений через сеть «Интернет», организация азартных сетевых игр, распространение наркотических средств, порнографии, заведомо ложной информации и пр.)

2) Отработка практических навыков установления, изучения профиля личности преступника через открытые источники (OSINT); выявления новых эпизодов преступной деятельности правонарушителей и их соучастников путем анализа социальных сетей, мессенджеров, истории браузера и иными, в том числе программным инструментарием; поиска мест совершения преступлений и нахождения преступников по фото- видео- файлам, зонам покрытия сотовой связи, геолокации, GPS, ГЛОНАСС, сети WI-FIи пр.; получения криминалистически значимой информации через анализ логотипов авторов, никнеймов юридических и физических лиц; работы с рекламными идентификаторами; установления личности, наименования объекта, сооружения участка местности и пр. по фотографии или видеозаписи; отработки мест происшествий с датчиками радо-электронной обстановки, получения и анализа биллнговых данных и т.п.);

3) Проведение на онлайновых тренировочных площадках ролевых и деловых игр, квестов по моделированию и решений конкретных следственных задач, связанных с раскрытием и доказыванием киберпреступлений, DDoS-атак (инцидентов) на объекты критической инфраструктуры;

4) Отработка навыков качественной подготовки и проведения следственных действий (обысков, осмотров, выемок), связанных с изъятием и осмотров гаджетов участников уголовного судопроизводства;

5) Глубокое (на всех уровнях, вплоть до физического) извлечение криминалистически значимых сведений из изъятых смартфонов, планшетов, компьютеров участников, облачного хранилища, устройств, синхронизированных с изъятыми гаджетами, невидимой части сегмента) с использованием высокотехнологичной криминалистической техники (Мобильный криминалист, UFED, X-RAI, СайтСпутник, Белкасофт и т.п.);

6) Формирование способностей к скрупулезной аналитической работе, связанной с осмотрами полученных сводок и результатов, а также умений выявлять криминалистически значимую для расследования информацию, составлению информативных и понятных для суда отчетов с использованием аппаратно-программных комплексов (PC-3000 Mobile; Сегмент; Градиент, Следопыт, Лис-М и др.);

7) Выявление ложных цифровых следов (антифорензика);

8) Изучение рынка существующей и новейшей криптовалюты (Bitcoin, Ethereum и др.) с целью идентификации площадок по созданию киберкошельков, а также самих кошельков и их реквизитов;

9) Создание системы учета криптокошельков, использованных в криминальных целях, через получение информации о финансовых транзакциях, позволяющей идентифицировать цифровые финансовые активы (принадлежность кибер-кошелька к конкретной цифровой площадке: бирже, кибер-обменнику и т.п.);

10) Отработка механизма наложения ареста на цифровые активы лиц, в отношении которых ведется производство по уголовным делам, возможности наложения ареста в качестве обеспечительной меры;

11) Мониторинг «Даркнета» - т.е. «теневого» использования сети Интернет, в частности VPN-соединений, позволяющих пользователям скрывать исходный IP-адрес пользователя сети Интернет, отработка способов деанонимизации преступников;

12) Применение цифровых технологий при расследовании отдельных видов преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий (Конструктор места происшествия, автоматизированной системы обработки запросов правоохранительных органов (проект «АСОЗ») к операторам связи, администрации социальных сетей, учреждения банковской сферы и др).

13) Проведение совместных круглых столов, лекционных занятий, вебинаров, распространение видеозаписей видеолекций и практических занятий, направленных на обучение следователей в области переподготовки и расследования подобных преступлений;

14) Апробация разработанных и попытка создания собственной базы актуальных продуктов, предназначенных для форензики и расследования киберпреступлений.

Таким образом лаборатория цифровых компетенций Московской академии Следственного комитета позволит обобщать и искать решения проблем предупреждения, раскрытия и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий (в том числе криптовалюты), для работы с цифровыми следами преступной деятельности, апробации и внедрения в следственную практику новейших отечественных высокотехнологических криминалистических средств, технологий, программ и иных продуктов путем проведения научно-исследовательской, экспериментальной, лабораторной, учебной и методической работ.

Г.А. Смирнова

Тактика осмотра места происшествия с применением цифровых технологий

Аннотация. Осмотр места происшествия – одно из следственных действий, проведение которых возможно на стадии доследственной проверки в порядке ст. 144-145 УПК РФ. В настоящее время осмотр места происшествия все чаще проводится с применением цифровых устройств. Цифровые устройства дают возможность получить больше доказательственной информации. Однако при проведении осмотра места происшествия нужно придерживаться определенной тактики, для того чтобы полученная доказательственная информация не была исключена впоследствии из доказательственной базы.

Ключевые слова: следственное действие, следственный осмотр, место происшествия, цифровое устройство, следователь, криминалист.

Одним из следственных действий, проведение которых возможно на стадии проверки, проводимой в порядке ст. 144-145 УПК РФ, является следственны осмотр. К нему относят, в том числе, осмотр места происшествия.

При проведении следственного осмотра, как правило, изучается обстановка на месте, где было совершено преступление, механизм его совершения. Также в ходе осмотра места происшествия выявляются, фиксируются и изымаются следы преступника и преступления. В ходе осмотра места происшествия можно изъять предметы и документы, которые могут содержать необходимые для расследования совершенного преступления сведения, и направить их на более детальное исследование (например, назначить экспертизу и передать их вместе с постановлением о назначении экспертизы эксперту).

Проведение данного следственного действия является опциональным, т.е., если необходимость в проведении следственного осмотра отсутствует, или же если его проведение бесперспективно, от него можно отказаться.[1]

В осмотре места происшествия, как правило, принимают участие несколько сотрудников, образующих следственно-оперативную группу. В данную группу включены, как правило, оперуполномоченный уголовного розыска, следователь, эксперт-криминалист. Следователь руководит проведением следственного действия, определяет границы его проведения, поясняет, какие именно действия должны выполнить участники осмотра, составляет протокол следственного действия, в котором описывает ход и результаты его проведения.[2] Оперуполномоченный уголовного розыска оказывает содействие в проведении осмотра следователю, устанавливает очевидцев преступления, наличие на месте происшествия и поблизости от него камер видеонаблюдения. Эксперт-криминалист принимает меры к охране объектов, которые будут исследоваться в дальнейшем, изымает и упаковывает их, отбирает контрольные и

[1] Протопопов А.Л. Расследование карманных краж. СПб., 2011. С. 61.
[2] Криминалистика: учебник / под ред. В.Д. Зеленского, Г.М. Меретукова. СПб., 2015. С. 367.

сравнительные образцы, осуществляет дополнительную фиксацию следов и вещественных доказательств на месте происшествия. Эксперт-криминалист оказывает следователю содействие в более точном отображении полученной информации и данных о применении криминалистических средств и методов.[1]

Следственные действия, в том числе, осмотр места происшествия все чаще проводятся с применением цифровых технологий. При применении в ходе осмотра места происшествия различных цифровых устройств следует придерживаться определенных правил. Это необходимо для того, чтобы впоследствии дополнительные сведения, полученные с помощью данных устройств, не были исключены (в результате удовлетворения ходатайств стороны защиты) из доказательственной базы.

В частности, желательно, чтобы применение цифровых устройств осуществлялось лицом, обладающим специальными знаниями. Интересно, что в связи с большим проникновением цифровых технологий в повседневную жизнь специальные познания в этой сфере все в большей мере переходят в категорию обычных повседневных знаний. Например, осуществление фото-и видеосъемки (если речь идет о судебно-следственной фотографии) в настоящее время перешло в разряд повседневных знаний, и вполне может быть выполнено следователем с помощью фото-видеокамеры, или даже мобильного телефона. Однако применение, например, в ходе осмотра места происшествия устройства, позволяющего зафиксировать наличие на определенном участке местности базовых станций сотовой связи, лучше поручить криминалисту.

При планировании следственного действия необходимо продумать, какие цифровые устройства нужно будет применить, и заранее их подготовить. В подготовку можно включить приискание всех необходимых для их работы приспособлений, достаточную зарядку батареи. Кроме того, необходимо заранее продумать и проговорить со специалистом условия, при которых будет возможно применение данных устройств. Следует также предусмотреть ситуацию, при которой (например, в связи с изменением обстановки) применение того или иного устройства может быть затруднительно или же невозможно, и проговорить, как в данной ситуации можно получить и закрепить необходимую доказательственную информацию. Также рекомендуется изучить документы, в которых содержится информация о цифровом устройстве, которое планируется применить на месте происшествия, о принципе его работы, информации, которую можно получить с его использованием, а также о том, требуются ли какие-то документы, подтверждающие исправность данного прибора. Если речь идет о применении измерительного прибора, нужно выяснить, требуются ли документы, подтверждающие точность проводимых им измерений. Получение данной информации необходимо не только для того, чтобы максимально качественно и достаточно быстро провести следственное действие, но и для того, чтобы опровергнуть возможные доводы стороны защиты о том, что устройства, примененные в ходе осмотра места происшествия, были

[1] Комаров И.М., Антонов А.Е. Расследование преступлений на объектах железнодорожного транспорта. М., 2019. С. 146-147.

не исправны и, следовательно, с их применением была получена неверная информация. Также это важно для того, чтобы уже при работе на месте происшествия понимать, какой максимально возможный объем доказательственных сведений можно получить, какие манипуляции нужно для этого выполнить и, если возникнет необходимость, напомнить о каких-либо манипуляциях криминалисту (если последний ввиду каких-либо субъективных причин (усталость, и т.д.) решит их не выполнять).

Все цифровые устройства, которые применяются в ходе проведения следственного действия, необходимо предъявить участникам осмотра, предупредить их о применении и указать в протоколе следственного действия. В частности, во вводной части протокола осмотра нужно указать вид устройства, его модель и марку, а также отметить, кем именно данное устройство было применено. Далее, при описании самого хода осмотра места происшествия, необходимо отметить, при каких именно обстоятельствах было применено цифровое устройство, и какая информация была получена с его использованием.

Если есть основания полагать, что на месте происшествия могут быть обнаружены электронные носители информации, целесообразно привлекать к осмотру специалиста, обладающего специальными познаниями в области компьютерной техники.

Осмотр места происшествия может проводиться с участием понятых. Согласно ст. 170 УПК РФ, их участие не обязательно, но в таком случае осмотр необходимо осуществлять с применением фотосъемки или видеосъемки или звукозаписи

В том случае, если осмотр места происшествия осуществляется в присутствии понятых, они должны присутствовать на месте происшествия с момента начала проведения следственного действия, и вплоть до его завершения. Перед началом осмотра рекомендуется пояснить понятым, какие именно цифровые устройства будут использоваться на месте происшествия, для чего они необходимо. При проведении осмотра места происшествия необходимо давать пояснения относительно того, какие именно манипуляции выполняет криминалист, и какие результаты в результате этих манипуляций получены. Это необходимо, так как понятые, как правило, не обладают специальными познаниями, при этом, они должны понимать, что происходит в ходе следственного действия, за ходом которого они наблюдают. Понятые должны понимать, что проходит на месте происшествия, так как они должны, по окончании проведения следственного действия, удостоверить его ход и результаты. Это же возможно только в том случае, если понятой понимает, что именно он видит и что именно он подтверждает.[1] По окончании осмотра все участвующие лица должны расписаться в протоколе осмотра места происшествия. Это всё касается любых средств и устройств, используемых в ходе ОМП (рулетка, щуп и пр.)

[1] Данилова С.И., Муженская Н.Е. Особенности применения криминалистических средств, приемов и методов при раскрытии и расследовании квартирных краж: Методические рекомендации. М., 2009. С. 12.

Литература

1. Данилова С.И., Муженская Н.Е. Особенности применения криминалистических средств, приемов и методов при раскрытии и расследовании квартирных краж: Методические рекомендации. М.: ВНИИ МВД России, 2009. 27 с.
2. Комаров И.М., Антонов А.Е. Расследование преступлений на объектах железнодорожного транспорта. М., Юрлитинформ, 2019. 178 с.
3. Криминалистика: учебник / под ред. В.Д. Зеленского, Г.М. Меретукова. СПб., Издательство «Юридический центр», 2015. 704 с.
4. Протопопов А.Л. Расследование карманных краж. СПб.: МИЭП, 2011. 92 с.

А.Г. Соломатина

Цифровая идентификация участников уголовного судопроизводства

Аннотация. В статье рассмотрены вопросы цифровой идентификации участников уголовного судопроизводства. Изучены вопросы об особенностях и видах электронной подписи, а также о цифровых платформах, существующих в Российской Федерации, которые призваны обеспечить электронный документооборот в уголовном судопроизводстве. На ровне с электронной подписью, в статье рассмотрены иные возможности цифровой идентификации лица, в том числе – биометрической, применяемые в других отраслях государственной, банковской, таможенной деятельности. Изучен опыт Росфинмониторинга РФ, некоторых зарубежных государств. Рассмотрены уже применяемые в правоохранительной деятельности технологические решения, такие как ГАИС Сфера, ГАИС Face Pay, NtechLab.

Ключевые слова: уголовный процесс, цифровизация уголовного судопроизводства, цифровая идентификация, биометрия, биометрическая идентификация, участники уголовного судопроизводства, электронная подпись.

В настоящее время необходимость разработки технологических решений цифровой идентификации и внедрения ее для удостоверения личности участника уголовного судопроизводства ясна и не вызывает сомнения.

С 9.01.2023 года согласно ст. 474.1 УПК РФ[1] изготовление процессуальных судебных решений, за исключением тех, которые содержат информацию, составляющие охраняемую федеральным законом тайну, затрагивающие безопасность государства, права и законные интересы несовершеннолетних, решения по делам о преступлениях против половой неприкосновенности и половой свободы личности, возможно в форме электронного документа. Документ должен быть удостоверен усиленной квалифицированной электронной подписью.

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.04.2023) // // СПС Консультант-Плюс». (Дата обращения 24.04.2023 г.).

Простая электронная подпись подтверждает лишь факт формирования электронной подписи определенным лицом, имея низкую степень защиты. Как правило, она используется для подписания писем и обращений через портал Госуслуг и ее можно получить посредством кодов и паролей, а усиленную квалифицированную электронную подпись - только в аккредитованном Удостоверяющем центре.

Наиболее защищенный вид электронной подписи - усиленная квалифицированная электронная подпись, создание которой возможно в процессе криптографического преобразования информации с использованием ключа электронной подписи и позволяет идентифицировать удостоверяющее лицо.

Рассматриваемая статья ст. 474.1 УПК РФ определяет организацию информационных платформ, таких как: Единый портал, информационная система, определенная Верховным Судом РФ, Судебным департаментом при Верховном Суде РФ, или система электронного документооборота участников уголовного судопроизводства с использованием единой системы межведомственного электронного взаимодействия, посредством которых могут подаваться электронные процессуальные документы[1].

Единый портал государственных и муниципальных услуг (ЕПГУ) представляет федеральную государственную информационную систему, обеспечивающую гражданам, предпринимателям и юридическим лицам доступ к сведениям о государственных и муниципальных учреждениях и оказываемых ими электронных услугах[2].

Согласно официальному сайту Верховного Суда РФ система информационного обеспечения деятельности Верховного Суда РФ (в составе Автоматизированной информационной системы Верховного Суда РФ) включает предоставление доступа судьям и работникам аппарата Верховного Суда РФ к лентам информационного агентства и др.[3].

Единая система межведомственного электронного взаимодействия (СМЭВ) представляет собой федеральную государственную информационную систему, значение которой состоит в организации взаимодействия между информационными системами участников СМЭВ для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме[4].

---

[1] Русакова Е.П. Воздействие цифровизации на гражданское судопроизводство в России и за рубежом: опыт Китая, Индии, Сингапура, Европейского союза, США, ЮАР и некоторых других стран: автореферат дис… к.ю.н. М., 2022., 45 с.

[2] Официальный интернет-портал правовой информации. URL: https://www.gosuslugi.ru/ (Дата обращения 24.04.2023 г.).

[3]Официальный интернет-портал правовой информации. URL: http://www.vsrf.ru/about/info/systems/inf_system_vnesh_vzaim (Дата обращения 24.04.2023 г.).

[4] См.: Положение о единой системе межведомственного электронного взаимодействия (утв. постановлением Правительства РФ от 08.09.2010 № 697) // СПС Консультант-Плюс». (Дата обращения 24.04.2023г.).

Рассматриваемые законодательные изменения знаменуют собой новый этап перехода от классического уголовного процесса к цифровому, отвечающему современным реалиям трансформации общества, что позволит максимально использовать инновационные технологии в целях оптимизации уголовного судопроизводства, повышения его эффективности путем усовершенствования документооборота, сокращения процессуальных сроков, облегчения доступа граждан к правосудию.

Однако, до тех пор, пока данная норма не будет апробирована, проблемы цифровой идентификации участников уголовного-процессуального электронного документооборота, соблюдения их прав и обеспечения процессуальных гарантий, достоверности предоставляемых доказательств будут оставаться актуальными, требующими пристального внимания.

Цифровая адаптация уголовного процесса находится на старте своего развития, что требует, с одной стороны улучшения интеграции цифровой идентификации, а, с другой - обеспечение безопасности участников уголовного судопроизводства, сохранности персональных данных и охраняемой законом тайны, причем не только при производстве по уголовному делу, но и в будущем.

Для достижения обозначенной цели разработчикам технологического сопровождения данной области следует обратиться к опыту применения существующих системных решений в банковской, визовой, таможенной и других видах деятельности, в которых удостоверение личности имеет не менее важное значение. Банковские учреждения и финансовые организации внедрили наравне с процессом подачи of-line обращений технологии искусственного интеллекта, обработки естественного языка (NLP) и расширенной аналитики, для реинжиниринга процессов адаптации участников финансовых отношений. Также на примере аутентификации клиентов банков можно учесть опыт запрашивания финансовой организации у частного лица информации о традиционных схемах транзакций, адреса и внешнего вида дома проживания, традиционном местоположении мобильного устройства, с которого осуществляется большинство платежей и др.

Росфинмониторинг применяет в своей деятельности ведение делопроизводства путем персонального входа в личный кабинет и дальнейшее поизводство для участников происходит в рамках закрытого контура[1].

Помимо цифровой идентификации в виде электронной подписи в России и в мировой практике одним из популярных направлений применения искусственных нейронных сетей - распознавание голоса, лиц и жестов — признана биометрическая идентификация. В декабре 2022 года подписан Федеральный закон от 29.12.2022 № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений

[1] Тиссен О.Н., Гриненко А.В. Использование результатов деятельности Росфинмониторинга в уголовном судопроизводстве // Всероссийский криминологический журнал. 2022. Т. 16, № 4. С. 492–504.

законодательных актов Российской Федерации", регулирующий отношения, возникающие при эксплуатации, модернизации и развитии государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных"[1].

Биометрия в настоящее время фактически является неотъемлемой частью обыденной жизни – выполнение любого платежа посредством использования Face ID и Touch ID своего смартфона. Применяемые системы распознавания лиц в городском транспорте Москвы – ГАИС Сфера, для оплаты проезда в режиме реального времени без ограничений и задержек – ГАИС Face Pay воплощают в жизнь потенциал цифровой биометрической идентификации. Разработанная в России программа распознавания лиц NtechLab в моменте определяет до 50 человек в кадре, в течение трех секунд идентифицирует лица на видео, сопоставляет результаты с запросами о разыскиваемых лицах информационных систем, и в случае совпадения направляет информацию в правоохранительные органы. В других странах, например, Индии предлагаются системные решения идентификации жестов и поведенческих действий лиц.

Таким образом, на основе рассмотрения актуальных проблем цифровой идентификации участников уголовного судопроизводства при электронном документообороте следует сделать основные выводы: цифровая доступность обеспечит «безбарьерный» доступ граждан к правосудию; участники уголовного процесса заинтересованы в упрощении процессов внедрения цифровых технологий и повышения уровня безопасности сохранности их персональных данных и обеспечения прав как участников уголовного судопроизводства; внедряемые технологии не должны вести к нарушению конституционных прав граждан; для оказания положительного влияния оптимизацию уголовно-процессуального документооборота не требуется полной модернизации, т.к. следует задействовать имеющиеся достижения в области информационных и других конвергентных технологий, что позволит усовершенствовать существующую уголовно-процессуальную инфраструктуру.

Литература

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.04.2023) // // СПС Консультант-Плюс».

[1] Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СПС Консультант-Плюс». (Дата обращения 24.04.2023г.).

2. Федеральный закон "Об электронной подписи" от 06.04.2011 № 63-ФЗ // СПС Консультант-Плюс».
3. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СПС Консультант-Плюс».
4. Положение о единой системе межведомственного электронного взаимодействия (утв. постановлением Правительства РФ от 08.09.2010 № 697) // СПС Консультант-Плюс».
5. Русакова Е.П. Воздействие цифровизации на гражданское удопроизводство в России и за рубежом: опыт Китая, Индии, Сингапура, Европейского союза, США, ЮАР и некоторых других стран: автореферат дис… к.ю.н. М., 2022., 45 с.
6. Тиссен О.Н., Гриненко А.В. Использование результатов деятельности Росфинмониторинга в уголовном судопроизводстве // Всероссийский криминологический журнал. 2022. Т. 16, № 4. С. 492–504.

А.А. Соловьев

Борьба с киберпреступностью как одно из направлений политики обеспечения национальной безопасности России

Аннотация. В настоящей статье рассмотрены основные направления деятельности государства по обеспечению информационной безопасности, перечислены правовые акты, регулирующие вопросы политики государства в указанной сфере, случаи ответственности за преступления в сфере компьютерной информации, сделан вывод о значительной роли правоохранительных органов в защите и восстановлении прав граждан, пострадавших от киберпреступности

Ключевые слова: национальная безопасность, информационная безопасность, борьба с киберпреступностью, доктрина национальной безопасности, внутренние и внешние угрозы информационной безопасности, защиту информации от несанкционированного доступа

Согласно данным МВД РФ, каждое четвертое преступление в стране совершается с использованием информационных технологий, и это на сегодняшний день не удивительно – десятилетие цифровизации и перехода на электронное оказание государственных, банковских и иных видов услуг дало почву для разработки преступных схем завладения данными граждан и юридических лиц с целью их дальнейшего использования для обогащения. При этом, обязанность по защите электронной информации от несанкционированного доступа третьих лиц - обязанность не только самих владельцев такой информации, но и государства.

В этой связи, в законодательстве России раскрывается методология защиты информации, а также различные виды ответственности за правонарушения в сфере информационных технологий.

Так, в 2006 году был принят Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии со статьей 16 которого защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации. Согласно статьи 17 вышеназванного федерального закона, нарушение его требований влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Указом Президента Российской Федерации от 05.12.2016 № 646 утверждена Доктрина информационной безопасности Российской Федерации, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Фактически принятие указанного правового акта признало, что защита информации – это не просто регулируемый правом процесс или деятельность государственных и правоохранительных органов, но и вопрос национальной безопасности, к которому необходимо относиться с более пристальным вниманием, не менее чем к другим видам угроз, с которыми сталкивается в современных условиях наша страна.

Статьей 2 упомянутой Доктрины установлены основные правовые понятия, а именно: «угроза информационной безопасности Российской Федерации или информационная угроза», под которой понимается совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере, а также «информационная безопасность Российской Федерации» - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В названных определениях заложены два направления информационной безопасности - частное, касающееся интересов физических лиц и коммерческих организаций, и коллективное (государственное), затрагивающее интересы страны в целом, при этом угрозы безопасности также классифицируются на внутренние, т.е. спровоцированные внутригосударственными факторами (несовершенство отечественного программного обеспечения, санкции иностранных государств, киберпреступность), а также внешние, нацеленные на дестабилизацию работы государственных информационных систем,

инициаторами и заказчиками которых выступают иностранные государства и их граждане (наиболее частыми проявлениями являются так называемые хакерские атаки).

Помимо прочего, обозначенная Доктрина прямо устанавливает, что система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации, что обусловлено ростом количества возможных угроз.

Так, согласно статистическим сведениям МВД РФ за 2022 год[1], в целом показатели киберпреступности по сравнению с предыдущими периодами не меняются. В основном, регистрируются факты кибермошенничества. Работа органов внутренних дел ориентирована, в большей степени, на выявление, пресечение и раскрытие преступлений в обозначенной сфере.

Федеральная служба безопасности России создала Национальный координационный центр по компьютерным инцидентам (НКЦКИ), основными направлениями деятельности которого являются: координация мероприятий по реагированию на компьютерные инциденты и непосредственное участие в них; участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак; доведение до субъектов критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения; сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. Работа центра ориентирована на предупреждение и ликвидацию последствий внешних угроз информационной безопасности. Сообщения о таких угрозах возможно направить через официальный сайт НКЦКИ.

Итак, становится очевидным, что информационная безопасность государства на сегодняшний день – одно из ключевых направлений государственной политики в сфере безопасности.

По мнению В.А. Номоконова и Т.Л. Тропина, «проблема т.н. киберпреступности актуализировалась в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватили все сферы жизнедеятельности человека и государства, а глобальная сеть Интернет является одной из наиболее быстрых областей развития телекоммуникационных технологий[2]».

И, действительно, практически все сферы взаимоотношений государства и граждан перешли в цифровую среду, а чуть ранее, и система взаимодействия банковских структур со своими клиентами. На сегодняшний день, согласно открытым данным информационных систем, программу «Сбербанк Онлайн» используют 40,9 млн. человек, а на портале «Госуслуги» зарегистрировано 97,5

[1] Статистический отчет МВД РФ «Состояние преступности в Российской Федерации за январь - декабрь 2022 год» - URL: https://мвд.рф/ (дата обращения: 02.04.2023).

[2] В.А. Номоконов, Т.Л. Тропина. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. №1 (24). 2012. С.45

млн. человек. Банковские финансовые операции, оплата налогов, регистрация имущества, бизнеса, а также многие другие услуги осуществляются с мобильного телефона. Более двадцати лет в качестве средства деловой коммуникации используется электронная почта, с недавнего времени на предприятиях и во многих коммерческих компаниях, а также в некоторых государственных структурах, внедряется система электронного проектного управления. И все перечисленное, являясь программным обеспечением, подвержено киберпреступности, т.е. несанкционированному доступу третьих лиц в корыстных целях.

Возникает вопрос – каким образом обеспечить максимальную защиту информации, и какие действия в этой связи предпринимает государство.

В первую очередь защиту информации от несанкционированного доступа должны обеспечивать сами ее пользователи – каждый электронный носитель должен быть обеспечен необходимыми антивирусными продуктами, кроме того, существуют определенные правила пользования программным обеспечением и получения его исключительно из проверенных источников. Категорически запрещается передача персональных данных пользователя третьим лицам, что зачастую и является причиной совершения преступлений, особенно в сфере банковских и микрофинансовых услуг.

В то же время, зачастую несанкционированный доступ к информации происходит далеко не по вине пользователя, в каждом случае проводится проверка на предмет наличия в действиях лица, получившего такой доступ и причинившего ущерб владельцу информации, признаков состава преступления.

Уголовный кодекс Российской Федерации в главе 28 установил ответственность за преступления в сфере компьютерной информации, а именно: за неправомерный доступ к компьютерной информации, за создание, использование и распространение вредоносных компьютерных программ, за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а с 2017 года введена ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации и за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Таким образом, на сегодняшний день предупреждение преступной деятельности в сфере компьютерной информации, раскрытие преступлений и восстановление законных прав и интересов – обязанность государства. Особую роль здесь играют органных внутренних дел, прокуратуры, следственного комитета и ФСБ как гаранты исполнения положений федерального законодательства в сфере защиты информации, Доктрины информационной безопасности Российской Федерации и принимаемых в соответствии с ними нормативных правовых актов, что является одним из направлений политики обеспечения национальной безопасности России.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» // СЗ РФ, 2006, № 31 (1 ч.), ст. 3448.
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ, 2016 № 50, ст. 7074
3. В.А. Номоконов, Т.Л. Тропина. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. №1 (24). 2012. С.45-55
4. Статистический отчет МВД РФ «Состояние преступности в Российской Федерации за январь - декабрь 2022 год» - URL: https://мвд.рф/ (дата обращения: 02.04.2023)

А.А. Тимошенко

Развитие идеи быстрого права для создания условий кибербезопасности

Аннотация. Автор обращает внимание на необходимость выделения правового регулирования отдельных вопросов обеспечения кибербезопасности в отдельный институт права межотраслевого характера. Данное предложение вызвано необходимостью обеспечить оперативную реакцию права и соответственно государственных органов на изменяющиеся обстоятельства применения права в условиях глобальной цифровизации всех сторон жизни общества. Конечно же данное предложение подлежит обсуждению в самом широком аспекте особенностей его реализации, однако игнорирование потребности в его реализации является опасным для развития социума.

Ключевые слова. Кибербезопасность, защита информации, институт права, информационная безопасность, быстрое право.

Ранее нами уже предлагалось обратить внимание на вопросы развития идеи быстрого права для целей подготовки адекватной реакции на вызовы глобальной цифровизации в мире[1].

Действительно, если подходить к вопросу о кибербезопасности с точки зрения исключительно традиционных взглядов на правовое регулирование общественной жизни может возникнуть проблема в обеспечении оперативного изменения норм права для целей обеспечения данной безопасности.

Собственно безопасность в концептуальных юридических документах определяют через статическую модель, изменение которой может произойти в любое время под воздействием агрессивной внешней обстановки.

[1] Тимошенко А.А., Фейзов В.Р., Чернов И.В. Сценарный подход к исследованию направлений регулирования сферы криптовалют в Российской Федерации // Российский журнал правовых исследований. 2023. № 2 (10). С. 21 – 30; Тимошенко А.А. Совершенствование регулирования рынка криптовалют за счет идеи быстрого права // Российский журнал правовых исследований. 2022. № 1 (9). С. 93 - 98.

В соответствии с п. 5 Стратегии национальной безопасности Российской Федерации[1] (далее – Стратегия) такая безопасность определена через использование законодательной конструкции, предполагающей достижение в результате эффективной деятельности государственных органов состояния «защищенности национальных интересов» Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны.

Следует отметить, что названный документ ключевым образом определяет приоритеты всей государственной деятельности в области безопасности, в том числе, и информационной.

В дополнение к нему действуют Доктрина информационной безопасности Российской Федерации[2], а также Стратегия развития информационного общества в Российской Федерации на 2017 0- 2013 годы[3].

Практически во всех документах предлагается принять меры для своевременного предотвращения воздействия различного рода угроз на безопасность сложной системы, в качестве которой выступает государство в лице его органов, организации, а также многонациональный народ Российской Федерации.

Кибербезопасность предполагает защиту от специального рода цифровых угроз, который могут заключаться в специальных атаках злоумышленников на компьютеры, их сети, сервера, мобильные устройства, электронные системы, базы данных и отдельные их виды.

В ряде случаев без правового регулирования отдельных областей использования данных технических устройств и их систем не обойтись. При этом, как мы уже отметили, такое регулирование должно осуществляться в оперативном режиме.

Так, например, при майнинге криптовалют как правило используются специальные устройства - ASIC майнеры.

Допустим, для обеспечения национальной безопасности государство решит запретить их оборот в Российской Федерации под страхом привлечения к уголовной ответственности импортеров, а также продавцов и покупателей. Для этих целей необходимо установить запрет на ввоз их на таможенную территорию страны, для чего следует внести изменения акты Коллегии Евразийской экономической комиссии, досконально соблюсти требования ст. 7 Таможенного кодекса Евразийского экономического союза. Также необходимо предусмотреть

---

[1] Утверждена Указом Президента Российской Федерации от 02.07.2021 № 400 // СПС «КонсультантПлюс».

[2] Утверждена Указом Президента Российской Федерации от 05.12.2016 № 646 // СПС «КонсультантПлюс».

[3] Утверждена Указом Президента Российской Федерации от 09.05.2017 № 203 // СПС «КонсультантПлюс».

ответственность за оборот товаров с родовыми признаками, подпадающими под устройства для майнинга в Уголовном кодексе Российской Федерации.

На выполнение указанных действий может потребоваться значительное время. К примеру, в 2019 году было подсчитано, что в среднем на принятие законопроекта, внесенного Президентом Российской Федерации может понадобиться в среднем 74,2 дня, Правительством Российской Федерации – более 172 дней, а депутатом Государственной Думы Федерального Собрания Российской Федерации – более 217 дней[1].

Наглядно необходимость ускорения данных процессов продемонстрировала ситуация с обеспечением адекватного ответа на экономические санкции недружественных Российской Федерации государств.

Для этих целей в соответствии со статьей 4 Федерального закона от 30.12.2006 № 281-ФЗ «О специальных экономических мерах»[2] Президенту Российской Федерации предоставлены исключительные права по введению различного рода ограничений на субъектов хозяйственных отношений для защиты национальных интересов. В рамках данных полномочий уже вступили в законную силу значительное число актов, значительно корректирующих сложившиеся правоотношения.

Мы предлагаем предусмотреть аналогичные процедуры д для целей регулирования мероприятий, направленных на обеспечение кибербезопасности. В качестве регулятора могла бы выступить межведомственная комиссия, решения которой можно рассматривать в качестве бланкетных норм для целей применения уголовного закона, а равно любого другого законодательного акта, в диспозициях своих норм предусматривающего обращение к решениям такого органа.

Очень важно добиваться всестороннего рассмотрения вопросов введения различного рода запретов и ограничений на рынке информационных товаров, работ и услуг, в связи с чем они не должны определяться позицией одного единственного органа исполнительной власти, к примеру, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Для иллюстрации эффективного применения таких механизмов можно рассмотреть деятельность Экспертного совета по существенным рыночным отклонениям, созданного при Банке России в соответствии с Приказом данного органа от 22.03.2016 № ОД-951[3].

В силу некоторой закрытости создаваемого межотраслевого института права необходимо дополнительно предусмотреть:

- систему обжалования решений межведомственного органа;
- дополнительные гарантии реализации права каждого на эффективную правовую защиту;

---

[1] Борзенкова Е. Со скоростью президента: путь законопроекта в России // Портал правовой информации «право.ru» [электронный ресурс]. Режим доступа: https://pravo.ru/story/212484/ (дата обращения: 12.05.2023).

[2] СПС «КонсультантПлюс».

[3] СПС «КонсультантПлюс».

- максимально автоматизировать поиск возможных угроз кибербезопасности за счет внедрения технологий искусственного интеллекта.

Выполнение этих и других подобных условий позволит существенно оптимизировать процедуры государственного вмешательства в стихийно складывающиеся отношения на цифровых рынках. Широкое обсуждение подобных проблем в экспертном сообществе будет только способствовать качественному повышению уровня безопасности в обществе.

Литература

1. Борзенкова Е. Со скоростью президента: путь законопроекта в России // Портал правовой информации «право.ru» [электронный ресурс]. Режим доступа: https://pravo.ru/story/212484/ (дата обращения: 12.05.2023).
2. Тимошенко А.А. Совершенствование регулирования рынка криптовалют за счет идеи быстрого права // Российский журнал правовых исследований. 2022. № 1 (9). С. 93 - 98.
3. Тимошенко А.А., Фейзов В.Р., Чернов И.В. Сценарный подход к исследованию направлений регулирования сферы криптовалют в Российской Федерации // Российский журнал правовых исследований. 2023. № 2 (10). С. 21 – 30.

Н.В. Уханова

К вопросу об изъятии и осмотре персонального компьютера, цифровой информации до и после возбуждения уголовного дела

Аннотация. Рассматриваются киберпреступления, при расследовании которых изъятию и осмотру подвергаются цифровые следы, содержащиеся в киберпространстве, в том числе, в персональных компьютерах и телефонах. Отмечаются особенности осмотра разных видов цифровых следов. На основе анализа научной литературы и судебно-следственной практики выделяются принципы работы с цифровыми следами.

Ключевые слова: киберпреступления, виды цифровых следов, осмотр компьютера, осмотр цифровых следов, судебное решение на осмотр.

Большинство авторов относят к киберпреступлениям широкий спектр составов преступлений. Это не только преступления в сфере компьютерной информации (глава 28), но и многие другие, совершаемые в киберпространстве, преступные деяния: мошенничество, кража, незаконный оборот запрещенных предметов (наркотиков, оружия, поддельных денег), склонение к самоубийству, вымогательство и иные[1]. Существует тенденция к увеличению количества

[1] Лыженкова А.Н., Шарыпова Т.Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности // Инновации, наука, образование. 2021. № 26. С. 900-904; Кочкина Э.Л. Определение понятия

киберпреступлений в финансовой сфере, причем последние носят организованный характер[1].

Выборочный анализ 50 приговоров и иных процессуальных документов, опубликованных на портале судов общей юрисдикции города Москвы в 2022 году, показал, что в большинстве случаев объектами изъятия и осмотра в связи с выявлением и расследованием различных киберпреступлений являются мобильные телефоны и смартфоны. Именно они чаще всего используются при совершении следующих преступлений:

- незаконный сбыт наркотических средств (ст. 228.1 УК РФ);
- кража с банковского счета (п. «г» ч. 3 ст. 158 УК РФ);
- различные виды мошенничества (ст. ст. 159, 159.3, 159.6 УК РФ);
- неправомерный доступ в компьютерной информации (ст. 272 УК РФ);
- нарушение тайны переписки и телефонных переговоров (ст. 138 УК РФ);
- неправомерный оборот средств платежей (ст. 187 УК РФ);

В зависимости от вида преступления, телефоны могут быть изъяты как до возбуждения уголовного дела (например, в ходе личного досмотра – при выявлении незаконного сбыта наркотических средств, осмотра места происшествия), так и после возбуждения уголовного дела (при обыске в жилище, личном обыске и т.д.).

Персональные компьютеры используются при совершении таких преступлений как подделка документов (ст. 327 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ (ст. 273 УК РФ). При этом при расследовании преступлений в ходе обысков изымаются, а затем осматриваются и признаются вещественными доказательствами, как правило, системные блоки.

Практика показывает, что в случае использования компьютеров в качестве средств совершения преступлений используются также дополнительные средства – переходники, флеш-накопители и те же телефоны.

Например, С. копировал со служебного компьютера на категорированный флеш-накопитель незаконно выгруженную из баз данных служебную информацию, а затем с флеш-накопителя, используя переходник, переносил ее на свой мобильный телефон, после чего посредством интернет-мессенджеров «WhatsAp» (Ватцап) и «Telegram» (Телеграм), установленных на его мобильном устройстве, передавал неустановленному лицу, действовавшему от имени детективного агентства, получая за это плату[2].

Как в случае с телефонами, так и с системными блоками главным объектом осмотра, имеющим доказательственное значение, является цифровая информация.

«киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162-169.

[1] Исмаилов Э.Ф. Киберпреступления в банковской сфере // Моя профессиональная карьера. 2019. № 6. Т. 1. С. 221.

[2] Приговор Преображенского районного суда г. Москвы по уголовному делу № 1-363/22 от 14.04.2022 г. [Электронный ресурс] // Официальный портал судов общей юрисдикции г. Москвы. URL: https://mos-gorsud.ru/.

Так, при расследовании киберпреступлений в сфере незаконного оборота наркотических средств объектами поиска в киберпространстве будут являться цифровые фотографии закладок, переписка соучастников преступления, а также электронные платежные инструменты, которые, как свидетельствует А.В. Пахарев, представлены многообразными формами и относятся как к легальной финансовой системе, так и к ее альтернативным видам[1].

При подделке документов объектом осмотра являются, в частности, файлы с электронными заготовками документов, при неправомерном доступе к компьютерной информации – программное обеспечение.

В процессе современного незаконного оборота наркотических средств, оружия, поддельных денег широкое распространение получили шифрование и криптовалюты, которые имеют особые цифровые следы и создают дополнительные трудности для расследования. Анализ транзакций с криптовалютами, в том числе с усиленной анонимностью, возможен с использованием специальных программных продуктов.

Осмотр предметов – электронных носителей информации может осуществляться с участием потерпевших, свидетелей, а также подозреваемых и обвиняемых, сотрудничающих со следствием.

Например, Н. в ходе осмотра предоставил органам следствия пароли от технических средств, в рамках осмотра активно пояснял внутреннее устройство программного обеспечения технических средств для целей раскрытия своей деятельности; предоставил органам следствия доступ к своим криптовалютным активам[2].

Одной из особенностей совершения киберпреступлений является возможность их совершения практически из любого места, при наличии доступа к Интернету. Поэтому объектом следственного интереса часто является не материальный предмет (компьютер), а именно цифровая информация, хранящаяся, во многих случаях, на удаленных серверах, в том числе, расположенных за рубежом. Например, потерпевший может находиться в одном государстве; лицо, совершающее преступление – в другом, а система используемых в преступной деятельности электронных денег – в третьем.

Исходя из этого, следует констатировать, что такие следственные действия как обыск, выемка, осмотр места происшествия (предмета) имеют неадаптированную к современным условиям законодательную регламентацию. Это отмечают многие авторы, например, С.Б. Россинский[3].

---

[1] Пахарев А.В. Проблемные вопросы в выявлении и раскрытии киберпреступлений в сфере незаконного оборота наркотиков, как элемента, как элемента экономической безопасности // Актуальные проблемы теории и практики оперативно-розыскной деятельности. СПб, 2019. С. 225.

[2] Постановление суда апелляционной инстанции по уголовному делу № 10-2974/22 от 16.02.2022 г. [Электронный ресурс] // Официальный портал судов общей юрисдикции г. Москвы. URL: https://mos-gorsud.ru/.

[3] Цит. по: Каримов Б.А. Особенности развития уголовно-процессуальных норм, регламентирующих изъятие и осмотр носителей цифровой информации // Международный научный журнал «Вестник науки». 2022. № 11 (56). Т. 1. С. 148-149.

Необходимо, чтобы в соответствующих статьях Уголовно-процессуального кодекса Российской Федерации шла речь не только о предметах и документах, имеющих значение для дела, но и об информации (цифровой информации), хранящейся в киберпространстве.

По нашему мнению, в определенных случаях для осмотра телефона или компьютера может потребоваться судебное решение (определение Конституционного Суда Российской Федерации от 24.06.2021 года № 1364-О). Предварительный судебный контроль в виде получения следователем судебного решения на осмотр электронных носителей информации необходим тогда, когда доступ следователя к охраняемой законом информации оказывается вне ведения ее обладателя[1]. Например, когда факт изъятия и последующего осмотра компьютера остается неизвестным для его владельца[2].

Анализ научной литературы и судебно-следственной практики позволяет выделить следующие принципы работы с цифровыми следами:

---

[1] Определение Конституционного Суда РФ от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации» [Электронный ресурс] // Законы, кодексы и нормативно-правовые акты Российской Федерации. URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-24062021-n-1364-o/.

[2] Учитывая дискуссионный характер мнения автора по этому вопросу, и в связи с тем, что в целевую аудиторию настоящего издания входят также практические работники СКР, редколлегия полагает целесообразным отметить следующее: Конституционный Суд РФ в указанном определении указывает на необходимость получения следственными органами судебного решения при подготовке и проведении одного их трех следственных действий, специально предназначенных для извлечения информации о переписке, телефонных переговорах, почтовых, телеграфных и иных сообщений, связанных с ограничением конституционных прав граждан (это предусмотрено в ст.ст.185, 186 и 186.1 УПК РФ), когда ограничение неприкосновенности сведений осуществляется вне ведения участника переговоров, который не осведомлен о контроле за его переговорами и сообщениями, а потому ограничен в возможности своевременно оспорить правомерность соответствующих действий, а также когда для доступа к содержанию переговоров, сообщений используются технические средства и возможности оператора связи (в том числе полученные от него ключи для дешифровки и т.п.), т.е. когда оператор связи является участником правоотношений.

УПК РФ не предусматривает получение судебного решения на осмотр предмета - изъятой в ходе обыска (личного обыска) или осмотра места происшествия компьютерной техники, в т.ч. смартфонов и содержащейся в их памяти информации (даже конфеденциальной) независимо от того известно ли об этом владельцу данной техники (он может быть и не установлен). При этом не возбраняется применять высокотехнологичные средства восстановления удаленной информации, определения геопозиции гаджета и т.п. Это подтверждается отечественной следственной и судебной практикой.

Как неоднократно отмечал Конституционный Суд Российской Федерации (определения от 25 января 2018 года № 189-О; от 17 июля 2018 года № 1955-О; от 28 ноября 2019 года № 3205-О; от 24.06.2021 № 1364-О), проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения {примеч. ред.}.

– недопустимость использования «открытых» сетей (Wi-Fi) при осмотре удаленной информации[1];

– недопустимость поиска файлов, копирование и иные действия (в том числе включение компьютерной техники) без участия специалиста;

– корректное завершение работы, отключение роутера, модема;

– недопущение дистанционного воздействия (удаления информации), а также контакта изъятой компьютерной техники с источниками магнитного излучения во время транспортировки и хранения (можно, например, поместить компюьтер в сумку Фарадея);

– незамедлительность осмотра компьютера с участием специалиста, особенно в тех случаях, когда отсутствует зарядное устройство;

– обязательность фотофиксации внешнего вида, внутреннего содержания (то есть, цифровых следов), а также обстановки, окружающей компьютер[2].

Литература

1. Исмаилов Э.Ф. Киберпреступления в банковской сфере // Моя профессиональная карьера. 2019. № 6. Т. 1. С. 216-237.
2. Каримов Б.А. Особенности развития уголовно-процессуальных норм, регламентирующих изъятие и осмотр носителей цифровой информации // Международный научный журнал «Вестник науки». 2022. № 11 (56). Т. 1. С. 148-151.
3. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162-169.
4. Лыженкова А.Н., Шарыпова Т.Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности // Инновации, наука, образование. 2021. № 26. С. 900-904;
5. Мосина С.В., Иванов В.Ю. Некоторые особенности работы с электронно-цифровыми следами при расследовании склонения несовершеннолетнего к самоубийству, совершенного в сети Интернет // Вестник Могилевского института МВД. 2020. № 2. С. 73-77.
6. Пахарев А.В. Проблемные вопросы в выявлении и раскрытии киберпреступлений в сфере незаконного оборота наркотиков, как элемента, как элемента экономической безопасности // Актуальные проблемы теории и практики оперативно-розыскной деятельности. СПб, 2019. С. 221-227.
7. Законы, кодексы и нормативно-правовые акты Российской Федерации. URL: https://legalacts.ru

[1] Исмаилов Э.Ф. Киберпреступления в банковской сфере // Моя профессиональная карьера. 2019. № 6. Т. 1. С. 235.

[2] Мосина С.В., Иванов В.Ю. Некоторые особенности работы с электронно-цифровыми следами при расследовании склонения несовершеннолетнего к самоубийству, совершенного в сети Интернет // Вестник Могилевского института МВД. 2020. № 2. С. 75-76.

8. Официальный портал судов общей юрисдикции г. Москвы. URL: https://mos-gorsud.ru/.

М.В. Феоктистов

Система и виды киберпреступлений в новых Уголовных кодексах Армении и Киргизии второй генерации

Аннотация. В статье рассмотрена система компьютерных преступлений в новом уголовном законодательстве Армении и Киргизии, ее сравнение с национальной системой и возможностью использования опыта наших соседей при реформировании российского уголовного права.

Ключевые слова: киберпреступление, компьютерное преступление, уголовное право, Россия, Армения, Киргизия.

Еще недавно уголовное законодательство бывших союзных советских республик напоминало братьев-близнецов, созданных как под копирку. Однако, после распада СССР и образования на его основе отдельных самостоятельных и независимых государств их законодательство постепенно начало отличаться от ранее заложенных исторических лекал.

В отличие от УК РСФСР 1960 г.[1] УК Армении, принятый 7 марта 1961 г.[2] просуществовал значительно дольше и был заменен УК Армении от 29 апреля 2003 года[3]. Уголовное законодательство Киргизии, наоборот, уже переживает третью генерацию. Действующий УК Киргизии, сменил на своем посту УК, принятый 2 февраля 2017 г. Пока в России ведутся дебаты о целесообразности или нецелесообразности принятия нового УК РФ[4] или его полностью обновленной редакции[5], законодатели соседних государств опередили своего российского коллегу и осуществили уже вторую (а в Киргизии и третью), после распада СССР, кодификацию уголовного законодательства.

---

[1] Уголовный кодекс РСФСР от 27 октября 1960 г. (ред. от 30 июля 1996 г.) // https://www.consultant.ru/document/cons_doc_LAW_2950/ (дата обращения 05.02.23).

[2] Уголовный кодекс Армянской ССР от 7 марта 1961 г. Ереван, 1961.

[3] Уголовный кодекс Республики Армении: Закон Республики Армении № ЗР-528 от 29 апреля 2003 г. // http://www.parliament.am/legislation.php?sel=show&ID=1349&lang= rus (дата обращения 05.02.23).

[4] См., например: Уголовный кодекс хотят заново реформировать // https://www.ugolkod.ru/new-uk-rf (дата обращения 05.02.23).

[5] См., например, Орешкин М.И. К вопросу о необходимости разработки и принятия государственной концепции новой редакции Уголовного кодекса Российской Федерации // Сибирский юридический вестник. 2018. № 4; URL: https://cyberleninka.ru/article/n/k-voprosu-o-neobhodimosti-razrabotki-i-prinyatiya-gosudarstvennoy-kontseptsii-novoy-redaktsii-ugolovnogo-kodeksa-rossiyskoy-federatsii (дата обращения: 05.02.23); Стариков Н.С. Нужен ли России новый Уголовный кодекс? https://nstarikov.ru/nuzhen-li-rossii-novyj-ugolovnoj-kodeks-92388 (дата обращения 05.02.23); Головко Л. Нормы УК и принятие новых кодексов // https://zasudili.ru/news/normy-uk-i-prinyatie-novykh-kodeksov/ (дата обращения 05.02.23).

Новый УК Армении[1] был принят Национальным Собранием 5 мая 2021 г., подписан Президентом 26 мая 2021 г., введен в действие с 1 июля 2022 г.[2] Отдельные положения УК (в части уголовной ответственности юридических лиц, наказания в виде ограничение свободы, содержания в дисциплинарном батальоне) вступают позже). Одновременно с УК РА введены в действие новые Уголовно-процессуальный[3] и Уголовно-исполнительный кодексы[4].

Новый УК Киргизии[5] был принят Жогорку Кенешем 22 сентября 2021 г., подписан Президентом 28 октября 2021 г., введен по истечении 15 дней с момента опубликования[6]. Одновременно с УК КР введен в действие новый Уголовно-процессуальный кодекс, а также внесены изменения в Уголовно-исполнительный кодекс 2017 г.[7]

Несмотря на столь юный возраст оба УК уже претерпели ни одно изменение. В УК Армении такие изменения были внесены спустя месяц после принятия[8]. Всего в РА принято 7 законов о внесении изменений в УК, а в Киргизии — 5, что вероятно свидетельствует о возможных ошибках, допущенных еще на стадии разработки проекта Кодекса и его принятия. Однако, на наш взгляд, предпочтительнее своевременное устранение допущенных противоречий, законодательного брака, нежели его сохранение в угоду обеспечения неприкасаемости текста недавно принятого акта.

Компьютерные преступления включены в раздел 12 УК Армении «Преступления против общественной безопасности». В УК КР они образуют раздел VIII «Преступления против общественной безопасности и общественного порядка», т.е. по родовым объектам эти преступления совпадают в УК РА, КР и РФ.

Глава 38 УК РА именуется «Преступления против безопасности компьютерной системы и компьютерной информации».

---

[1] Уголовный кодекс Республики Армении: Закон Республики Армении № ЗР-199 от 27 мая 2021 года // https://base.spinform.ru/show_doc.fwx?rgn=144695 (дата обращения 05.02.23).

[2] О введении в действие Уголовного кодекса Республики Армении: Закон Республики Армении № ЗР-144 от 18 июня 2022 г. // https://base.spinform.ru/show_doc.fwx?rgn=143424 (дата обращения 05.02.23).

[3] Уголовно-процессуальный кодекс Республики Армении: Закон Республики Армении № ЗР-306 от 27 июля 2021 г. // https://base.spinform.ru/show_doc.fwx?rgn=143021 (дата обращения 05.02.23).

[4] Бадалян Н. Армения полностью меняет Уголовно-исполнительный кодекс // https://arminfo.info/full_news.php?id=69439 (дата обращения 05 февраля 2023 г.).

[5] Уголовный кодекс Кыргызской Республики: Закон Республики Кыргызстан № 127 от 28 октября 2021 г. // http://cbd.minjust.gov.kg/act/view/ru-ru/112309?cl=ru-ru (дата обращения 05.02.23).

[6] О введении в действие Уголовного кодекса Кыргызской Республики, Уголовно-процессуального кодекса Кыргызской Республики, Кодекса Кыргызской Республики о правонарушениях и внесении изменений в некоторые законодательные акты Кыргызской Республики: Закон Кыргызской Республики № 126 от 28 октября 2021 г. // http://cbd.minjust.gov.kg/act/view/ru-ru/112305?cl=ru-ru (дата обращения 05.02.23).

7 Там же.

8 См.: О внесении изменения в Уголовный кодекс Республики Армении: Закон Республики Армении от 17 июня 2021 г. №ЗР-259 // https://base.spinform.ru/ show_doc.fwx?rgn = 133921 (дата обращения 05.02.23).

В Киргизском УК глава 40 названа «Преступления против кибер-безопасности».

Таким образом в отличие от российского законодателя оба государства акцентируют внимание на охраняемых общественных отношениях, на которые посягает виновный (безопасность компьютерной системы, компьютерной информации, кибербезопасности), а не на сфере компьютерной информации, в которой возможно совершение любых, в том числе и не имеющих никакого отношения к киберпространству, преступлений.

Также как и в России у наших коллег предусмотрена уголовная ответственность за Неправомерный доступ к компьютерной информации (ст. 272 УК РФ); Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). При этом соответствующие статьи УК Армении именуются: Проникновение в компьютер, компьютерную систему или компьютерную сеть (ст. 359); Незаконный оборот специальных программных или инструментальных средств (ст. 363); Нарушение правил или требований эксплуатации компьютера, компьютерной системы или компьютерной сети (ст. 365), а статьи УК КР — Несанкционированный доступ к компьютерной информации и электронным документам, в компьютерную систему или сеть электросвязи (ст. 319) и Создание вредоносных программных продуктов (ст. 320). УК КР не предусматривает отдельной статьи, аналогичной ст. 274 УК РФ, однако, ч. 3 ст. 319 УК КР повышает уголовную ответственность за несанкционированный доступ к компьютерной информации и электронным документам, в компьютерную систему или сеть электросвязи, совершенное с целью умышленного уничтожения, изменения, блокирования, приведения в непригодное состояние компьютерной информации или электронного документа либо вывода из строя, разрушения информационных систем или сети электросвязи. Здесь удачно в качестве предмета преступления называется в том числе и электронный документ.

В отличие от УК РФ, устанавливающего уголовную ответственность за Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1) и Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274^2), его зарубежные аналоги таких статей не содержат, однако, п. 3 ч. 4 ст. 319, п. 3 ч. 2 ст. 320 УК КР предусматривают в качестве квалифицирующего признака совершение преступления в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре.

Среди, деяний, неизвестных российскому УК, армянский законодатель криминализирует такие действия, как: Изменение компьютерного сведения (ст. 360), Незаконное извлечение компьютерных сведений (ст. 362), Компьютерный подлог (ст. 364), а также компьютерный саботаж (ст. 361).

Последнее деяние известно не только армянскому, но и киргизскому уголовному законодательству (ст. 321 — Кибер-саботаж).

УК Киргизии содержит и довольно интересную норму, отсутствующую как в УК Армении, так и в УК РФ, которая устанавливает уголовную ответственность за Массовое распространение электронных сообщений (ст. 322), осуществленное без предварительного согласия адресатов, приведшее к нарушению или прекращению работы программных продуктов, телекоммуникационных систем, оборудования и абонентских терминалов. Общественная опасность такого деяния достаточно очевидна, ведь порою неоднократные обращения с запросами к серверу, носящими массовый и циклический характер, приводят к тому, что оборудование испытывает перегрузки, преждевременно изнашивается и выходит из строя, работа сайта или сервиса блокируется. Достаточно вспомнить как такими атаками блокировались сервисы Центральной избирательной комиссии РФ в дни досрочного голосования. Поэтому такая норма может быть воспринята и отечественным законодательством.

Другим образцом для подражания может стать и норма о компьютерном саботаже, который выражается в уничтожении, повреждении, искажении или блокировании (изоляции) сведения, хранящегося в компьютере, компьютерной системе, компьютерной сети или в другом компьютерном оборудовании, без разрешения, предусмотренного законом или договором, или на ином правомерном основании.

Интерес, в плане возможной рецепции, может представлять и ст. 364 УК Армении, преследующая за компьютерный подлог, выражающийся в незаконном вводе, незаконном изменении, стирании компьютерного сведения или блокировании (изоляции) доступности этого сведения в целях появления юридических последствий, которые повлекли создание недостоверного сведения. Целесообразность криминализации таких действий обусловлена существенным ростом в настоящее время компьютерных технологий, их использованием для доступа граждан к получению государственных услуг, официальной информации, распоряжения и управления персональными данными и т.п.

Все УК не предусматривают совершение преступления с использованием средств компьютерной техники в качестве обстоятельства, отягчающего наказание, однако, совершение преступления посредством использования сетей телекоммуникации, в том числе сети Интернет; с публичной демонстрацией в сети Интернет в УК РА и УК РК выступает конструктивным признаком в 1 основном составе преступления, квалифицирующим признаком I степени в 17 составах преступлений в УК Армении и в 6 составах УК Киргизии и в 1 квалифицирующим признаком II степени (УК Армении).

И, наконец, в ст. 257 УК РА предусмотрена уголовная ответственность за компьютерное хищение, которое включено в систему преступлений против собственности и определяется законодателем, как хищение чужого имущества, совершенное путем ввода, изменения, уничтожения, перекрытия (изолирования) компьютерных данных без разрешения, предусмотренного законом или договором, или по иному правомерному основанию, или путем воздействия на

работу компьютера, компьютерной системы или компьютерной сети иным способом. Думается, что целесообразность включения в УК такой нормы давно назрела и может быть взята за основу. Такое решение более предпочтительно, чем имеющаяся в УК РФ ст. 159[5] «Мошенничество в сфере компьютерной информации», тем более, что компьютерная информация не может быть обманута. По сути дела, использование для хищения компьютера есть не что иное, как один из новых способов хищения, а именно способ является основным критерием выделения форм хищения и такое решение будет лежать в русле существующей системы хищений. В УК КР нет специальной нормы, посвященной компьютерному хищению, однако, в некоторых случаях наряду с квалифицирующим признаком «кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков мошенничества)» (п. 5 ч. 3 ст. 205 УК КР) говорится о «краже с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков мошенничества)» (п. 6 ч. 3 ст. 205).

Подводя итог нашему исследованию, можем отметить, что при сохранении некоторых традиционных подходов к системе компьютерных преступлений законодатели соседних государств внесли и существенные коррективы. Одни из принятых решений могут быть заимствованы в ходе дальнейшей реформы российского уголовного права (а также иных государств), а эффективность других может быть проверена только временем.

Э.Б. Хатов

Использование информационно-аналитических платформ анализа транзакций цифровой валюты при подготовке будущих следователей

Аннотация. В статье рассматриваются некоторые проблемы повышения качества подготовки будущих следователей Следственного комитета в условиях цифровизации преступности и следственной деятельности. Одним из путей их решения автор предлагает использование возможностей информационно-аналитических платформ анализа транзакций цифровой валюты.

Ключевые слова: киберпреступность, следователь, цифровизация, криптовалюта, анализ, платформа.

Реалии современного состояния преступности, в структуре которой последние годы фиксируется стабильно высокий уровень преступлений, совершенных с использованием высоких технологий[1], наглядно демонстрируют выраженную потребность не только в широкой цифровизации следственной деятельности в целом[2], но и в следователях, обладающих достаточными цифровыми компетенциями.

[1] Официальный сайт МВД РФ https://xn--b1aew.xn--p1ai/reports/item/35396677/

[2] В настоящее время Следственным комитетом Российской Федерации с участием ведомственных академий ведется работа над разработкой Концепции цифровизации следственной деятельности.

Для удовлетворения указанной потребности в Следственном Комитете Российской Федерации приняты соответствующие организационные меры по подготовке и повышению квалификации следственных кадров. Так, в соответствии с решением Председателя Следственного комитета Российской Федерации А.И. Бастрыкина от 17.04.2023 в текущем году стартует набор обучающихся по направлению подготовки 40.04.01 «Юриспруденция» по новой специализации (направленности подготовки) «Расследование преступлений, совершенных с использованием информационных технологий». Помимо этого, кардинально обновлены программы обучения студентов, организован научный кружок «Киберследователь», который послужил основой формирования кадрового резерва из числа обучающихся, проявивших способности к научно-технической деятельности и активному использованию цифровых технологий. Немаловажную роль в решении поставленных задач играют учрежденные по инициативе Председателя Следственного комитета Российской Федерации А.И. Бастрыкина специализированные кафедры в Московской и Санкт-Петербургской ведомственных академиях.

В рамках углубленного изучения современных возможностей расследования киберпреступлений, развития цифровых компетенций обучающиеся под руководством квалифицированных преподавателей приобретают необходимые следователю знания, навыки и умения в сфере цифровых технологий, принимая также участие в научных исследованиях прикладного характера. Так, разработанный в стенах Академии проект «Виртуальный помощник следователя – «ПоСледователь», целью которого является усовершенствование процесса расследования путем модернизации механической составляющей деятельности следователя, использования в процессе составления процессуальных документов возможностей искусственного интеллекта, занял в июне 2023 г. 3 место на конкурсе проектов хакатон «Искусственный интеллект для анализа больших данных», организованном ГИАЦ МВД России среди ведомственных ВУЗов правоохранительных органов. Указанная разработка рассматривается нами как очередной шаг к прогнозируемым ведомственным аналитическим программам, которыми можно будет управлять в ближайшем будущем просто голосовыми командами, так называемых электронных помощников (электронных ассистентов).[1]

Во взаимодействии со специализированным отделом по расследованию киберпреступлений и преступлений в сфере высоких технологий Главного следственного управления Следственного комитета Российской Федерации на кафедре информационных технологий и организации расследования киберпреступлений тестировались аналогичные обозреватели, разработанные негосударственными структурами - информационные платформы – такие как

[1] Хатов, Э. Б. Анализ преступности: перспективы цифровизации / Э. Б. Хатов // I Стояновские чтения. Российские следственные органы: прошлое, настоящее, будущее : Материалы научно-практической конференции. К 200-летию со дня рождения Николая Ивановича Стояновского и 10-летию образования Следственного комитета Российской Федерации , Москва, 15 апреля 2021 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2021. – С. 144. – EDN JBYFWK.

«Шард» и Crypto.thibm, с помощью которых можно не только проанализировать в истории подозрительные трансакции условно-анонимных криптовалют и визуализировать их, но активизировать функцию мониторинга (отслеживания) для контроля вывода средств.

Учитывая, что все большее число экономических преступлений связано с использованием криптовалют[1], представляется, что современный следователь должен обладать также навыками использования различных информационно-аналитических платформ-обозревателей. К ним можно отнести известный и разработанный Росфинмониторингом обозреватель криптовалют «Прозрачный блокчейн 2». В отличие от первой, новая версия, которая сейчас в стадии внедрения, может анализировать трансакции более чем 20 криптовалют.

Указанные платформы облегчают применение следователями методов гугл-доркинга, прямой корреляции для поиска уже идентифицированных криптокошельков, их адресов уже привязанных к различным сервисам и открытым публичным базам данных, методы скоринга, по жалобам и негативным отзывам на их пользователей, по несанкционированным утечкам информации, что нередко позволяет получить никнеймы и другие идентифицирующие данные на интересующих лиц.

Актуальность вопроса объясняется тем, что несмотря на утвержденную Правительством Российской Федерации 08.02.2022 Концепцию законодательного регламентирования механизмов организации оборота цифровых валют, проблема правового регулирования вопроса *деанонимизации киберкошельков* в современных условиях постоянного роста их применения в криминальной сфере по прежнему остается одной из ключевых.

В этой связи протестированные и получившие положительное заключение кафедры указанные информационно-аналитические платформы могут быть использованы в процессе изучения дисциплин: «Цифровые следы преступлений против личности», «Расследование киберпреступлений» и ряда других. При наличии учетных записей пользователи из числа обучающихся могут непосредственно осваивать возможности указанных платформ по анализу трансакций криптовалют на практических и лабораторных занятиях в компьютерных классах (киберполигоне). Следует отметить, что кафедрой при поддержке руководства Академии достигнуты принципиальные договоренности с правообладателями по использованию указанных информационно-аналитических платформ в тестовом режиме в учебных целях, что позволит повысить качество и прикладной характер обучения.

Таким образом, развитие цифровых компетенций будущих следователей по использованию информационно-аналитических платформ для идентификации участников интересующих следствие подозрительных (криминальных) трансакций, в том числе трансграничных, представляется по сути необходимым

[1] См.: Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). С. 101–108; Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография / под ред. Е.В. Емельяновой и О.С. Бутенко. – СПб: Санкт-Петербургская академия СК России, 2022.и др.

элементом обучения современных следователей Следственного комитета Российской Федерации.

Литература

1. Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). С. 101–108;
2. Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография / под ред. Е.В. Емельяновой и О.С. Бутенко. – СПб: Санкт-Петербургская академия СК России.
3. Хатов Э. Б. Анализ преступности: перспективы цифровизации // I Стояновские чтения. Российские следственные органы: прошлое, настоящее, будущее : Материалы научно-практической конференции. К 200-летию со дня рождения Николая Ивановича Стояновского и 10-летию образования Следственного комитета Российской Федерации , Москва, 15 апреля 2021 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2021. – С. 141-145. – EDN JBYFWK.

Б.Е. Чич

К вопросу об особенностях обжалования следователем решений прокурора (на примере уголовных дел о некоторых преступлениях)

Аннотация. В статье анализируются принимаемые прокурором решения о возвращении уголовных дел следователю, об отмене постановления следователя о возбуждении уголовных дел о некоторых преступлениях, в том числе о киберпреступлениях. Рассматриваются случаи, когда установление специального способа совершения преступления с использованием информационных и телекоммуникационных технологий на этапе проверке сообщения о преступлении является обязательным. Указываются пределы достаточности установления в стадии возбуждения уголовного дела данных о способе совершения преступлений. Приводится правоприменительная практика по обжалованию следователем решений прокурора по указанным уголовным делам и сообщениям о преступлениях.

Ключевые слова: законность, право на обжалование, прокурор, следователь, процессуальная самостоятельность, киберпреступление, способ совершения преступления, возбуждение уголовного дела, возвращение уголовного дела следователю.

Основанием отмены прокурором решений следователя являются ошибки, допущенные на различных этапах досудебного производства. Зачастую обжалуемые решения касаются оценки достаточности собранных доказательств для реализации положений статьи 215 УПК РФ или достаточности данных для принятия решения о возбуждении уголовного дела. При отмене постановления

следователя об отказе в возбуждении уголовного дела прокурором не редко указывается на недостаточность проведенных процессуальных и следственных действий, направленных на подтверждение оснований, предусмотренных ч. 1 ст. 24 УПК РФ.

Вместе с тем, не всегда и не все принимаемые прокурором решения являются законными и обоснованными, в связи с чем они требуют обжалования. Решение следователя обжаловать решение прокурора направлено на реализацию назначения уголовного судопроизводства (ст. 6 УПК РФ), соблюдение принципа законности и выработку наиболее оптимального пути предотвращения и разрешения возможных конфликтов в уголовно-процессуальной деятельности. Следует признать, что и прокурором, и лицом, осуществляющим проверку по сообщению о преступлении и предварительное расследование могут допускаться ошибки ввиду невозможности исключения человеческого фактора и необходимости владения специальными знаниями. По мнению Н.В. Османовой, на практике порой могут встречаться одиозные решения как со стороны прокурора, вернувшего уголовное дело в порядке, предусмотренном п. 2 ч. 1 ст. 221 УПК РФ, так и со стороны прокурора, не удовлетворяющего жалобу следователя и поддерживающего позицию нижестоящего прокурора [1, 33].

Рассмотрим особенности обжалования следователем решений прокурора на примере уголовных дел о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий.

По уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий, большое значение имеет установление способа совершения преступления. Поэтому при получении в ходе проверки сообщения о преступлении сведений о невозможности установления специального способа совершения противоправного уголовно-наказуемого деяния с использованием сети Интернет и отсутствии обстоятельств, исключающих производство по уголовному делу, принимается решение о возбуждении уголовного дела по основному составу преступления.

В случае, если в диспозиции статьи УК РФ в качестве способа совершения преступления указывается использование сети Интернет или информационно-телекоммуникационных технологий, возбуждение уголовного дела допускается только при наличии достоверной и достаточной информации об указанном в соответствующей норме способе совершения преступления. На это указывает и конструкция квалифицированных составов ряда преступлений. Возбуждение уголовного дела по признакам таких преступлений допускается только в случае наличия информации о соответствующем способе совершения преступления. Отсутствие в диспозиции статьи «специального» способа указывает на то, что доказывание в стадии возбуждения уголовного дела обязательным не является.

В подтверждение указанных доводов обратимся к правоприменительной практике. Так, в отношении С. возбуждено уголовное дело по признакам преступления, предусмотренного п. «б» ч. 4 ст. 132 УК РФ [2]. Согласно позиции следователя в ходе осмотра квартиры потерпевшего установлена комната, в которой стоит компьютер, с помощью которого осуществлялся выход в телекоммуникационную сеть «Интернет». По мнению прокурора в материалах

доследственной проверки отсутствовала информация о месте совершения преступления, а также не проведена лингвистическая экспертиза переписки между подозреваемым С. и потерпевшим Б. Указанное явилось основанием отмены прокурором постановления следователя о возбуждении уголовного дела. Не согласившись с решением прокурора, следователь обжаловал его, указав в обоснование своей позиции, что наличие объяснения Б. и переписки между С. и Б. являются достаточными для возбуждения уголовного дела, а отсутствие лингвистической экспертизы не препятствует принятию законного решения. Вышестоящий прокурор поддержал позицию следователя.

В настоящее время на стадии возбуждения уголовного дела в целях установления оснований для принятия процессуального решения по сообщению может применяться практически весь спектр процессуальных действий, предусмотренных ч. 1 ст. 144 УПК РФ. Вместе с тем, все еще остаются процессуальные и следственные действия, провести которые фактически невозможно на этапе производства проверки сообщения о преступлении.

Указанное подтверждается правоприменительной практикой. Так, прокурором отменено постановление следователя о возбуждении уголовного дела по факту смерти П. по ч. 1 ст. 105 УК РФ [3]. В обосновании своей позиции прокурор указал, что постановление следователя является преждевременным и необоснованным, поскольку в ходе доследственной проверки каких-либо данных о том, что смерть П. носит насильственный характер не установлено. В момент обнаружения трупа окна и двери квартиры были закрыты, при этом входная дверь квартиры была закрыта на замок изнутри, порядок в квартире не нарушен. Следователь обжаловал решение прокурора, указав, что точная причина смерти П. не установлена, а предварительная причина смерти в виде асфиксии проведенными исследованиями не подтверждена, судебно-медицинское исследование трупа не завершено. Для установления возможности получения телесных повреждений, асфиксии при падении с положения стоя и под весом собственного тела, явившейся причиной смерти, необходимо проведение комплексной судебно-медицинской экспертизы, производство которой в сроки, предусмотренные ст. 144 УПК РФ, не представляется возможным. Таким образом, отменяя постановление о возбуждении уголовного дела, прокурор ограничил следственный орган в исполнении государственной функции по осуществлению уголовного преследования, в ходе которого полноценно могут быть рассмотрены вопросы по установлению события преступления, виновности либо невиновности лиц. В рамках же доследственной проверки возможности для установления объективной истины исчерпаны и соответственно только после возбуждения уголовного дела, по результатам установления круга общения П. посредством изучения детализаций телефонных переговоров и переписки в сети «Интернет» при её наличии, допросов свидетелей на предмет установления возможных лиц, которые могли желать П. смерти, проведения очных ставок, судебных экспертиз, возможно установление всех обстоятельств произошедшего. В данном случае только совокупность собранных в ходе предварительного следствия доказательств позволит сделать

вывод о наличии или отсутствии состава преступления. Вышестоящий прокурор поддержал позицию следователя.

Практика обжалования следователем решений прокурора не всегда носит положительный характер, и удовлетворение находят не все жалобы следователя. Возбужденное в отношении Т. уголовное дело по признакам преступления, предусмотренного ч. 1 ст. 282 УК РФ [4], было возвращено прокурором следователю для производства дополнительного следствия в связи с ненадлежащим осмотром информации, размещенной в сети «Интернет», повлекшем отсутствие в материалах дела сведений о точном времени совершения преступления. По уголовному делу установлено, что Т. разместил в сети «Интернет» аудиозапись экстремистского характера, при осмотре которой следователем не указано время ее создания и размещения, а одного лишь факта размещения оказалось недостаточным, поскольку на момент совершения преступления возраст Т. мог и не достигнуть возраста уголовной ответственности. Доводы следователя о невозможности по техническим причинам установить точное время, а также показания самого Т. о том, что он выложил аудиозапись экстремистского характера после того, как ему исполнилось 16 лет, показались вышестоящему прокурору не убедительными. В удовлетворении жалобы следователю отказано.

Следует учитывать, что информация (сведения) о совершении преступления, связанного с использованием информационно-телекоммуникационных технологий и сети «Интернет» даже после ее удаления может быть восстановлена и изъята в установленном законом порядке. Поэтому необходимо отметить обязательность (по уголовным делам о киберпреступлениях) привлечения специалиста к производству следственных действий, направленных на поиск информации и предметов, по изъятию предметов и их осмотру.

Изложенное в очередной раз подтверждает, что в современных условиях развития технических средств важным элементом обеспечения прав участников уголовного судопроизводства является постоянное повышение уровня подготовки следователей, руководителей следственных органов и прокурорских работников, совершенствование их навыков работы с информационными и телекоммуникационными технологиями, электронными носителями информации, ее изъятием, осмотром и хранением, а также направленность субъектов уголовного преследования на строгое исполнение требований закона и реализацию назначения уголовного судопроизводства.

Литература

1. *Османова Н.В.* Право следователя на отстаивание интересов следствия в уголовном судопроизводстве // Российский следователь. 2019. № 5. С. 32-36.
2. Уголовное дело № 11702030006000041 // Архив следственного управления Следственного комитета Российской Федерации по Краснодарскому краю.
3. Уголовное дело № 11702920006000207 // Архив следственного управления Следственного комитета Российской Федерации по Республике Татарстан.

4. Уголовное дело № 2016/838 // Архив следственного управления Следственного комитета Российской Федерации по Томской области.

Л.С. Шеховцова

Роль судебно-лингвистической экспертизы при расследовании преступлений, совершаемых с использованием сети Интернет

Аннотация. В статье рассматривается криминалистическое значение судебно-лингвистической экспертизы для расследования преступлений, совершаемых с использования сети Интернет. Особенности объектов исследования, диалоговая форма коммуникации определяют специфику судебно-лингвистической экспертизы. По некоторым категориям уголовных дел, в частности возбужденных по факту совершения преступлений экстремистского характера, оскорбления, вымогательства установление события преступления, а также наличия в действиях лица признаков состава преступления требует производства исследования смыслового содержания текста.

Ключевые слова: лингвистическая экспертиза, текст, смысловое содержание, расследование, сеть Интернет

Исследование смыслового содержания текста значимо для расследования разных категорий преступлений, в том числе, организации деятельности экстремистской организации, публичных призывов к осуществлению экстремистской деятельности, публичного оправдания терроризма; склонения к совершению самоубийства; незаконного сбыта наркотических средств; вымогательства; угрозы убийством[1] и др.

Такие преступления все чаще совершаются с использованием сети Интернет, что определяет специфику судебно-лингвистической экспертизы, назначаемой по уголовным делам.

Анализ интернет-переписки или звукозаписи переговоров может помочь решить задачу определения ролей и содержание конкретных действий, совершаемых участниками преступных групп. Это приобретает особое значение в ситуации, когда смысловое содержание текста в сети законспирировано или неочевидно для участников уголовного судопроизводства по иным причинам.

Так, например, в ходе расследования незаконного сбыта наркотического средства была проведена судебно-лингвистическая экспертиза интернет-переписки подозреваемых. В заключении эксперт указал, что в предоставленных материалах речь идёт о совместной работе, связанной с криминальными способами обогащения, с подпольным производством и нелегальной реализацией чего-либо, о трудоустройстве «кладменом», к профессиональным

[1]Назарова Т.В., Громова А.В. Перспективы развития и востребованность фоноскопических, лингвистических и автороведческих экспертиз при раскрытии и расследовании киберпреступлений // Криминалистика в условиях развития информационного общества. М., 2018, С 206–210.

обязанностям которого относятся развешивание и упаковка неких объектов, а также их размещение в определенных местах. В тексте переписок имеются признаки маскировки содержательных элементов текста, обозначающих объекты, действия, которые осуществляются «курьером», «минёром» в сфере деятельности, связанной с криминальными способами обогащения, с подпольным производством и нелегальной реализацией чего-либо[1]. Выводы эксперта были положены следователем в основу обвинительного заключения при определении ролей участников преступной группы.

В сети Интернет смысл текста кроме слов может передаваться также с помощью невербальных средств коммуникации: небуквенных символов, графических изображений, аудио и видеофайлов. Так, например, типичными средствами коммуникации при выражении угрозы являются символы, передающие в сжатом виде информацию для идентификации опасности: изображение черепа с костями, огня, молнии, оружия, а также прочие графические символы, которые используются для передачи эмоций испуга и страха, тревожного настроения.

Судебно-лингвистическая оценка смысла текста, обнаруженного в сети Интернет, имеет специфику. Часто такое исследование не ограничивается необходимостью применения специальных филологических знаний, а требует привлечения иных специалистов. Судебно-лингвистическая экспертиза традиционно производиться комплексно с судебно-компьютерной экспертизой (например, если исследованию подлежит размещенный на веб-сайте текст), с судебно-фоноскопической экспертизой (например, при проведении акустического анализа речевых сигналов, при нарушении звукопроизношения, наличии диалектических и акцентных и иных особенностей), с судебно-психологической экспертизой и другими.

Таким образом заключение судебно-лингвистической экспертизы является источником доказательственной информации при расследовании преступлений, совершаемых с использованием сети Интернет. В ряде случаев доказать событие преступления и наличие в действиях лица состава преступления, например, оскорбления, доведения до самоубийства, вымогательства затруднительно без заключения судебно-лингвистической экспертизы.

Наиболее часто такая экспертиза используется в качестве процессуального средства проверки и уточнения собранных по делу доказательств: установление темы разговора и предмета высказываний, а также определенные символов, слов и словосочетаний, имеющих экстремистскую окраску или характерных для выражения угрозы, оскорбления и других противоправных или связанных с ними действий.

[1] Приговор Волгоградского гарнизонного военного суда Волгоградской области № 1-35/2020 от 27 мая 2020 г.URL: https://sudact.ru/regular/doc/kYMPainB9gZH.

Литература

1. Назарова Т.В., Громова А.В. Перспективы развития и востребованность фоноскопических, лингвистических и автороведческих экспертиз при раскрытии и расследовании киберпреступлений // Криминалистика в условиях развития информационного общества. М., 2018, С 206–210.
2. Приговор Волгоградского гарнизонного военного суда Волгоградской области № 1-35/2020 от 27 мая 2020 г.URL: https://sudact.ru/regular/doc/kYMPainB9gZH.

В.И. Шиян

Современные тенденции киберпреступности

Аннотация. В статье представлены основные современные тенденции киберпреступности. Обращено внимание на последовательный рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации и лиц, их совершивших. Определены региональные особенности.

Ключевые слова: киберпреступность, киберпреступления, информационно-телекоммуникационные технологии, компьютерная информация, региональный аспект, современные тенденции.

Современный период мирового развития характеризуется быстрым развитием информационно-коммуникационных технологий, что повышает вероятность возникновения киберугроз для всех сфер общественной жизни[1]. IT-технологи используют для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности[2].

С началом специальной военной операции увеличилось количество компьютерных атак на российские информационные ресурсы; большая часть таких атак осуществляется с территорий иностранных государств. Так, по данным «Лаборатории Касперского» в марте 2022 года число DDoS-атак на российские организации выросло в восемь раз по сравнению с тем же месяцем

[1] См.: Борисов А.В. Классификация угроз транспортной безопасности // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 4(26). – С. 43-46; Борисов А.В. Угрозы транспортной безопасности России // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 2(24). – С. 76-79; Гончарова М.В., Шиян В.И. Состояние и тенденции современной киберпреступности// Вестник Академии Следственного комитета Российской Федерации. 2021. № 1 (27). С. 53-56; Афанасьев П.Б. Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 10-14.

[2] См.: Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

2021 года. Прогрессирует и продолжительность атак: в феврале-марте 2022 года они в среднем длились 29,5 часов, в то время как в 2021 году – не более 12 минут[1].

По сравнению с 2021 годом в 2022 году ущерб только от киберпреступлений, выявленных органами внутренних дел, увеличился более чем на 20% и составил 91 941 183 тыс. руб.

В рамках данной статьи под киберпреступностью будем понимать совокупность преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, и лиц, их совершивших на определенной территории за определенный период времени.

Учитывая, что в формах официальной статистической отчетности ГИАЦ МВД России, сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий стали выделяться только с 2018 года, за основу возьмем период с 2018 по 2022 годы.

В течение последних пяти лет исследуемому виду преступлений свойственна тенденция последовательного роста, которая фиксировалась, как правило, на фоне общего снижения преступности (см. табл.).

Таблица

Динамика киберпреступлений в 2018–2022 годах

Показатели	**Годы**				
	2018	**2019**	**2020**	**2021**	**2022**
Всего зарегистрированных преступлений	1 991 532	2 024 337	2 044 221	2 004 404	1 966 795
Киберпреступления	174 674	294 409	510 396	517 722	522 065
Доля киберпреступлений в структуре преступности, %	8,8	14,5	25,0	25,8	26,5
Выявлено лиц, совершивших киберпреступления	24 002	44 158	65 665	95370	98 252

Так, в 2022 году количество зарегистрированных преступлений по сравнению с 2018 годом сократилось на 1,2%. В тоже время аналогичный показатель киберпреступлений увеличился на 198,9%. Количество лиц, выявленных за совершение киберпреступлений также существенно возросло (+309,3%).

Тенденция роста характерна и для доли киберпреступлений в структуре преступности. Если в 2018 году это значение составляло 8,8%, то в 2022 году

[1] См.: Десять самых громких кибератак XXI века. URL: https://www.kaspersky.ru/resource-center/threats (дата обращения 26.03.2023).

достигло 26,5%. Таким образом, в настоящее время практически каждое третье преступление совершается с использованием IT-технологий.

По итогам 2022 года, как и ранее[1] лидерами криминальной статистики по количеству зарегистрированных киберпреступлений продолжают оставаться города федерального значения – Москва (50 503) и Санкт-Петербург (20 663). Высокие значения данного показателя зафиксированы в Краснодарском крае (22 603), Республике Татарстан (17 993), Челябинской области (17 281), Московской области (15 061) и Ростовской области (13 642).

Наибольшие темпы прироста киберпреступлений в 2022 году по сравнению с 2021 годом наблюдались в Республике Северная Осетия – Алания (+47,8%), Тверской области (+40,1%), Рязанской области (+26,3%), Республике Крым (+22,4%), Московской (+19,1%) области, Карачаево-Черкесской Республике (+18,9%). Вместе с тем аналогичный общероссийский показатель незначительный – 0,8%.

В пяти регионах зафиксированы наибольшие темпы снижения киберпреступлений – Ненецком АО (–28,0%), Чеченской Республике (–22,2%), Республике Калмыкия (–22,4%), Республике Хакасия (–19,1%) и Республике Тыва (–16,8%).

По справедливому замечанию А.Ж. Саркисян и Г.Ф. Коимшиди «заметное снижение темпов роста таких преступлений обусловлено усилением профилактической деятельности правоохранительных органов, средств массовой информации и служб безопасности ведущих банков страны»[2]. В этой связи весьма продуктивным является решение Банка России, в соответствии с которым граждане получили возможность самостоятельно устанавливать запреты и ограничения на онлайн-операции по своим счетам.

Необходимо отметить, что абсолютное большинство зарегистрированных киберпреступлений (более 98%) выявляется органами внутренних дел. Повысился уровень раскрываемости киберпреступлений. В 2022 году он составил 27,8 %. В качестве сравнения отметим, что в 2021 году это значение достигало только отметки 23,4%.

Несмотря на то, что в структуре киберпреступности 52,1% составляют тяжкие и особо тяжкие преступления, их число уменьшилось на 5,6%. Сократилось количество киберпреступлений, предусмотренных статьями 110^1 УК РФ (–55,6%), 138 УК РФ (–19,2%), 138^1 УК РФ (–15,0%), 146 УК РФ (–24,1%), 158 УК РФ (–27,6%), 159^3 УК РФ (–29,0%), 159^6 УК РФ (–22,5%), 183 УК РФ (–41,5%), 234 УК РФ (–17,8%), 242^2 УК РФ (–41,3%), 273 УК РФ (–36,9), а также, совершенных при помощи средств мобильной связи (–2,1 %), расчетных (пластиковых) карт (–23,2 %).

В немалой степени указанные тенденции обусловлены эффективной деятельностью Управления по организации борьбы с противоправным

[1] См.: Саркисян А.Ж., Коимшиди Г.Ф. Динамика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации // Расследование преступлений: проблемы и пути их решения. 2022. № 1(35). С. 71-76.

[2] Саркисян А.Ж., Коимшиди Г.Ф. Указ. соч. С. 72.

использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации (УБК МВД России), которое было создано в соответствии с Указом Президента Российской Федерации от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты Президента Российской Федерации». В числе первостепенных задач УБК МВД России в исследуемой сфере – организация предупреждения, выявления, пресечения и раскрытия преступлений, совершаемых с использованием (в сфере) информационно-коммуникационных технологий, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших; организация пресечения распространения в информационно-телекоммуникационной сети Интернет информации, создающей угрозу причинения вреда жизни, здоровью и имуществу граждан; организация международного взаимодействия и др.

В качестве следующей тенденции следует назвать активизацию деятельности организованных групп и преступных сообществ (преступных организаций) в киберпространстве. Наиболее существенными индикаторами выступают транснациональный характер противоправной деятельности, широкое использование современных достижений науки, техники, информационно-телекоммуникационных технологий для легализации (отмывания) денежных средств, в сфере незаконного оборота наркотиков и оружия, создание в сети Интернет порносайтов.

Глобализация информационных процессов обусловила появление новых форм терроризма и экстремизма – кибертерроризма и киберэкстремизма. Например, более половины преступлений экстремистской направленности (52,3 %) совершается с использованием IT-технологий, несмотря на ежедневный мониторинг сети Интернет и блокировку сайтов, признанных экстремистскими. Так, по состоянию на 19 октября 2022 года МВД России совместно с Роскомнадзором ограничен доступ к более 150 тыс. Интернет-ресурсам, содержащим призывы к массовым беспорядкам и иные сведения, направленные на дестабилизацию российского общества[1].

В структуре организованной преступности фиксируется прирост преступлений в сфере компьютерной информации (+212,2% в 2022 году), сохраняется тенденция по вовлечению в организованную преступную деятельность высококвалифицированных IT-специалистов.

Учитывая основные современные тенденции киберпреступности, до настоящего времени сохраняется потребность в повышении эффективности мер противодействия киберпреступности, активизации совместных комплексных профилактических мероприятий и специальных операций правоохранительных органов России и зарубежных стран.

[1] Выступление В.А. Колокольцева на заседании Государственной Думы Федерального Собрания Российской Федерации в рамках «правительственного часа» [Электронный ресурс]. URL: https://мвд.рф/document/33200763 (дата обращения: 26.03.2023).

Литература

1. Афанасьев П.Б. Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // В сб.: Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. Всероссийская научно-практическая конференция. М., 2021. С. 10-14.
2. Борисов А.В. Классификация угроз транспортной безопасности // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 4(26). – С. 43-46.
3. Борисов А.В. Угрозы транспортной безопасности России // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 2(24). – С. 76-79.
4. Гончарова М.В., Шиян В.И. Состояние и тенденции современной киберпреступности// Вестник Академии Следственного комитета Российской Федерации. 2021. № 1 (27). С. 53-56.
5. Саркисян А.Ж., Коимшиди Г.Ф. Динамика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации // Расследование преступлений: проблемы и пути их решения. 2022. № 1(35). С. 71-76.

А.Д. Яким

ChatGPT и информационные технологии в аспекте киберпреступности

Аннотация. В статье приведен правовой обзор на актуальные возможности искусственного интеллекта, ChatGPT. Определяются основные направления технологий будущего. Внимание уделяется использованию искусственного интеллекта в киберпреступлениях.

Ключевые слова: ChatGPTB, расследование преступлений, машинное обучение, алгоритмы.

Искусственный интеллект (далее ИИ), киберпространство, ChatGPTB (от англ. Generative Pre-trained Transformer «генеративный предварительно обученный трансформер» — чат-бот с искусственным интеллектом, разработанный компанией OpenAI и способный работать в диалоговом режиме, поддерживающий запросы на естественных языках) – данные термины, на сегодняшний день, входят в нашу жизнь с явлениями цифровизации. Актуальны они и в криминальной среде, ведь используются возможности инноваций для совершения преступных деяний. Меняются не только способы и средства совершения преступлений, но и характеристика личности преступника. В научной среде под термином «преступник» понимается — субъект преступления, носитель наиболее общих, устойчивых, существенных социально-

психологических черт с присущими ему антиобщественным поведением, вариантом поведения[1].

Преступления искусственного интеллекта – новое направление для изучения в науке, если ChatGPT может совершать преступные деяния, то возможно стоит задуматься о понимании субъекта преступления. Рассмотрим подробнее. Официальное определение ИИ в стратегических документах Российской Федерации утверждено от 10 октября 2019 года №490 «Национальная стратегия искусственного интеллекта на период до 2030 г.»[2] в которой определяются цели и основные задачи ИИ в России: искусственный интеллект-комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатом интеллектуальной деятельности человека. В стратегии прописаны перспективные методы использования ИИ, набор данных, архитектура вычислительной системы. Свойство ИИ – эболаративность, то есть обучаемость, даже без использования открытой библиотеки ИИ, которая включает в себя набор алгоритмов, предназначенных для разработки технологических решений на его основе, это несомненно вызывает интерес правоохранительных органов.

Криминологическая «Теория дифференциальной ассоциации», выдвинутая Эдвином Сатерлендом, основной постулат которой гласит: преступное поведение является результатом социального обучения, позволяет сделать вывод, что если человек может научиться девиантному поведению в социуме, становясь преступником, то и ИИ аналогичным образом может стать потенциальным преступником. Данное явление становится возможным с помощью обучения его определенным командам, созданием специального алгоритма, который способен вывести из строя заданные параметры, либо же ИИ сам придет к тому, что сможет обладать способностью думать, принимать решения. Данный сигнал может стать намеренным, либо с намеренным причинением вреда с помощью ИИ. Еще некоторое время назад, ученым казалось, что машина никогда не сможет заменить человека, а сейчас детерминация технотронной преступности влияет на развивающиеся системы ИИ. По мнению А.А. Бессонова[3,4] - цифровизация в деятельности по расследованию преступлений востребованность методов работы с большими данными, алгоритмов искусственного интеллекта, различных информационно-аналитических комплексов и систем поддержки принятия решений.

---

[1] Криминология. Учебник / Под ред., Н.Ф. Кузнецовой и Г.М. Миньковского. М., 1998.

[2]Указ Президента РФ О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. №490 // Собрание законодательства Российской Федерации. - 2019.-№41, ст.5700.

[3]Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. – Москва: Проспект, 2021. -816 с.

[4] Бессонов А.А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. №1 (35). С.1.

В свою очередь, В.С.Овчинский справедливо отмечает: «Существует ИИ трех видов - самый простой – применимый обычные программы, алгоритмы, которые работают на основе больших данных, средний ИИ используют на производствах, а сильный ИИ – сверхразум, это ИИ, который превзойдет к 2040 году все человечество» Базирующаяся в Сан-Франциско компания Open AI выпустила несколько версий языковой модели GPT, которая обучается на текстах из интернета и может генерировать осмысленные ответы на вопросы. GPT-3 может создавать связный текст. Наибольшей критике подвергался тот факт, что модель не понимает контекста, а просто пытается предсказывать текст слово за словом. ChatGPT работает на новой версии модели — GPT-3.5. Она лучше справляется с контекстом благодаря тому, что запоминает подробности беседы. В отличие от многих нейросетевых чат-ботов, ChatGPT запоминает детали разговора и может строить ответы, основываясь на информации, которую ему уже сообщил пользователь. Последняя на сегодняшний день версия GPT-4 мощнее GPT-3.5[1]. GigaChat – новая русскоязычная версия, созданная разработчиками SberDevices способна решать интеллектуальные задачи, например отвечать на фактологические вопросы, и поддерживать беседу, обладает навыком создания изображений.

В 2011 году учёные из Техасского университета проводили опыты над нейронной сетью Discern. По их задумке, программа должна была изучать языки. Загрузив в неё множество данных, исследователи решили имитировать душевную болезнь, наделив искусственный интеллект шизофренией. То есть, намеренно заставили его сойти с ума. Не в силах совладать с анализом большого объёма данных, Discern говорил о себе в третьем лице и путал времена. Discern выражался обрывками фраз и слов, а также выдавал результат, не соответствующий реальной действительности, заявил, что в здании заложена бомба и он приготовил учёным террористический акт. В 2018 году группа исследователей из Массачусетского технологического института «с нуля» создала первого в мире ИИ-психопата. Назвали его Норманом — в честь героя хичкоковского триллера «Психо». Обучение происходило за счет кадров убийств, взятых из сети-интернет. После этого машинный разум не мог воспринимать мир привычным образом. Он видел в различных (вполне мирных) силуэтах, описаниях, картинах исключительно сцены насилия. Учёные из Массачусетса пришли к выводу: при необходимости машину с помощью алгоритма можно запрограммировать под любое восприятие, мировоззрение, в зависимости от направленности действий программирующего.

По мнению португальского эксперта по нейронауке Закари Мейнена, в будущем ИИ научится испытывать депрессию и галлюцинации. Да и прочие эмоции, в том числе негативные — их будут вызывать цифровые аналоги нейромедиаторов. Подобными исследованиями сейчас занимается вычислительная психиатрия — новая наука в области искусственного интеллекта.

[1] Ларина Е.С., Овчинский В.С. ChatGPT: мировой переполох// Завтра.ру. URL: ChatGPT: мировой переполох (zavtra.ru) Дата обращения: 22.05.2023.

Какие психические расстройства могут лежать в основе желания причинить смертельный вред другому человеку? И может ли обладать психическими особенностями машина?

Многие ученые придерживаются мнения о том, что ИИ имеет возможности:

– антропоморфно разумных мыслительных и когнитивных действий, таких как распознавание образов, символьных систем и языков, рефлексия, рассуждение, моделирование, образное (смыслопорождающее и смысловоспринимающее) мышление, анализ и оценка;

– самореферентности, саморегулирования, самоадаптирования под изменяющиеся условия, самоограничения и при этом поддерживать себя в гомеостаз[1]

Проведенные за последние десятилетия исследования показали, что не только ИИ способен поменять право, но в свою очередь право воздействует на ИИ, поэтому юридические исследования продолжаются в направлении решения проблемы урегулирования отношений, в которых искусственный интеллект задействован.

Следовательно, вопрос о правовой регламентации ответственности за нештатную работу киборгизированных устройств будет признана за субъектом, устанавливающим программное обеспечение, а также обучение ИИ алгоритмам. Стоит отметить, что вопрос об ответственности поднимался уже несколько лет назад[2]. Практика правоприменения не стоит на месте и в ближайшем будущем увидим первые судебные прецеденты, касающиеся ответственности создателей алгоритмов кибергозированных устройств.

Литература

1. Указ Президента РФ О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. №490 // Собрание законодательства Российской Федерации. - 2019.-№41, ст.5700.
2. Криминология. Учебник / Под ред., Н.Ф. Кузнецовой и Г.М. Миньковского. М., 1998.С.12.
3. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография. – Москва: Проспект, 2021. -816 с.

[1] Мохат П.М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. 2018. №6. URL: https://cyberleninka.ru/article/n/k-voprosu-o-spetsifike-pravovogo-regulirovaniya-iskusstvennogo-intellekta-i-o-nekotoryh-pravovyh-problemah-ego-primeneniya-v-otdelnyh Дата обращения: 25.05.2023..

[2] Федоров А.В. О некоторых тенденциях развития уголовно-правовой антикоррупционной политики в Российской Федерации в части, касающейся установления уголовной ответственности юридических лиц // Антиномии. 2014. №3. URL: https://cyberleninka.ru/article/n/o-nekotoryh-tendentsiyah-razvitiya-ugolovno-pravovoy-antikorruptsionnoy-politiki-v-rossiyskoy-federatsii-v-chasti-kasayuscheysya Дата обращения: 28.05.2023 С.3..

4. Бессонов А.А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. №1 (35).
5. Ларина Е.С., Овчинский В.С. ChatGPT: мировой переполох// Завтра.ру. URL: ChatGPT: мировой переполох (zavtra.ru)Дата обращения: 22.05.2023
6. Морхат П.М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. 2018. №6. URL: https://cyberleninka.ru/article/n/k-voprosu-o-spetsifike-pravovogo-regulirovaniya-iskusstvennogo-intellekta-i-o-nekotoryh-pravovyh-problemah-ego-primeneniya-v-otdelnyh Дата обращения: 25.05.2023.
7. Федоров А.В. О некоторых тенденциях развития уголовно-правовой антикоррупционной политики в Российской Федерации в части, касающейся установления уголовной ответственности юридических лиц // Антиномии. 2014. №3. URL: https://cyberleninka.ru/article/n/o-nekotoryh-tendentsiyah-razvitiya-ugolovno-pravovoy-antikorruptsionnoy-politiki-v-rossiyskoy-federatsii-v-chasti-kasayuscheysya Дата обращения: 28.05.2023.

Сведения об авторах

Бессонов Алексей Александрович – ректор ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», доктор юридических наук, доцент, Почётный работник Следственного комитета при прокуратуре Российской Федерации, полковник юстиции.

Архипова Ирина Александровна – заместитель начальника кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент, полковник полиции.

Агаян Виолетта Арсеновна – старший преподаватель Ростовского института (филиала) ВГУЮ (РПА Минюста России), член Экспертного совета по законотворчеству МП Государственной Думы ФС РФ.

Афанасьев Павел Борисович – доцент кафедры «Уголовное право, уголовный процесс и правоохранительная деятельность» Юридического института Российского университета транспорта (МИИТ), кандидат юридических наук.

Афанасьева Ольга Романовна – профессор кафедры «Уголовное право, уголовный процесс и правоохранительная деятельность» Юридического института Российского университета транспорта (МИИТ), доктор юридических наук, доцент.

Бешукова Зарема Муратовна – профессор кафедры уголовного права и уголовного процесса Адыгейского государственного университета, доктор юридических наук, доцент.

Бычков Василий Васильевич – декан факультета повышения квалификации Московской академии Следственного комитета, кандидат юридических наук, доцент, Почетный сотрудник Следственного комитета Российской Федерации, полковник юстиции.

Валов Сергей Владимирович – старший научный сотрудник научно-исследовательского отдела факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета, кандидат юридических наук, доцент.

Вихляев Александр Александрович – преподаватель кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я. Кикотя, майор полиции.

Гарафутдинова Флюра Муллахматовны - старший преподаватель РТУ МИЭА.

Гончаров Дмитрий Константинович – старший оперуполномоченный Отдела экономической безопасности и противодействия коррупции УМВД России по г. Керчи, майор полиции.

Голубовский Владимир Юрьевич – ведущий научный сотрудник отдела по совершенствованию нормативно-правового регулирования деятельности центра изучения проблем управления и организации исполнения наказаний в уголовно-исполнительной системе ФКУ НИИ ФСИН России, доктор юридических наук, профессор, почетный работник высшего

профессионального образования, почетный сотрудник МВД России генерал – майор в отставке.

Гущев Максим Евгеньевич – заведующий кафедрой криминалистики Нижегородского филиала ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», кандидат юридических наук, доцент, подполковник юстиции.

Журбенко Алексей Михайлович – доцент кафедры криминалистики Белгородский юридический институт МВД России имени И.Д. Путилина, кандидат экономических наук, капитан полиции.

Зайцева Елена Александровна - профессор кафедры уголовного процесса учебно-научного комплекса по предварительному следствию в органах внутренних дел Волгоградской академии МВД России, заслуженный работник высшей школы РФ, доктор юридических наук, профессор.

Зиганшин Марсель Нурсилевич – старший преподаватель кафедры криминалистики Уфимский юридический институт МВД России подполковник полиции.

Калашников Виктор Сергеевич – доцент кафедры уголовного процесса и криминалистики Кемеровского государственного университета, кандидат юридических наук.

Кардашевская Марина Владимировна – профессор кафедры предварительного расследования Московской академии СК России, доктор юридических наук, профессор.

Киселёв Евгений Александрович – доцент кафедры криминалистики Хабаровского филиала ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», кандидат юридических наук, доцент, полковник юстиции.

Клещенко Юрий Григорьевич – доцент кафедры права Гуманитарно-социального института, научный сотрудник Института международного права и экономики имени А.С. Грибоедова, кандидат экономических наук.

Кондратьев Юрий Анатольевич – доцент кафедры уголовного права и криминологии, кандидат юридических наук ВГУЮ (РПА) Минюста России); доцент.

Красненко Юрий Владимирович – преподаватель кафедры уголовного процесса Белгородского юридического института МВД России имени И.Д. Путилина, майор полиции.

Кунц Елена Владимировна – ведущий научный сотрудник отдела разработки методологий исполнения наказаний, связанных с лишением свободы, изучения пенитенциарной преступности центра исследования проблем обеспечения безопасности в учреждениях уголовно-исполнительной системы ФКУ НИИ ФСИН России, доктор юридических наук, профессор, почетный работник высшего профессионального образования.

Лебедева Анна Андреевна – доцент кафедры криминалистики Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент, подполковник юстиции.

Литвишко Петр Андреевич – заместитель начальника Главного управления международно-правового сотрудничества Генеральной прокуратуры РФ – начальник управления правовой помощи и правоохранительного содействия, кандидат юридических наук, государственный советник юстиции 3 класса.

Логинов Евгений Александрович – профессор кафедры публичного права Московского государственного института международных отношений (университет) Министерства иностранных дел Российской Федерации (МГИМО), доктор юридических наук, профессор.

Любавский Алексей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета Российской Федерации, кандидат технических наук.

Лысенко Евгений Сергеевич – кандидат юридических наук, доцент заведующий кафедрой информационных технологий и организации расследования киберпреступлений Санкт-Петербургской академии Следственного комитета.

Макарова Оксана Валерьевна – ведущий научный сотрудник центра уголовного, уголовно-процессуального законодательства и судебной практики Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, кандидат юридических наук.

Максимов Константин Викторович – доцент кафедры оперативно-разыскной деятельности органов внутренних дел Уфимского юридического института МВД России, кандидат исторических наук, подполковник полиции.

Матвеева Евгения Александровна – бакалавр права, соискатель магистерской степени МГИМО МИД России.

Муллагалеева Лилия Рамилевна – следователь по особо важным делам отделения по расследованию киберпреступлений и преступлений в сфере высоких технологий третьего следственного управления (с дислокацией в городе Нижний Новгород) Главного следственного управления Следственного комитета Российской Федерации, кандидат юридических наук, майор юстиции.

Муратова Надежда Георгиевна – доктор юридических наук, профессор, заслуженный юрист Республики Татарстан, профессор кафедры уголовного процесса и криминалистики Казанского (Приволжского) федерального университета, юрист второго класса.

Нургалеев Нияз Рифович – начальник отдела по противодействию наркоугрозе в сети Интернет и организованной преступной деятельности Управления по контролю за оборотом наркотиков МВД по Республике Башкортостан, подполковник полиции.

Озеров Игорь Николаевич – заведующий кафедрой судебно-экспертной и оперативно-розыскной деятельности. Московская академия Следственного комитета Российской Федерации.

Османова Надежда Валерьевна – декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета, кандидат юридических наук, доцент, подполковник юстиции.

Павловская Надежда Владимировна – заведующий лабораторией криминологического обеспечения прокурорской деятельности Научно-исследовательского института Университета прокуратуры Российской Федерации, кандидат юридических наук.

Петраков Сергей Викторович – заведующий кафедрой управления следственной деятельности (Высшие академические курсы) факультета повышения квалификации Санкт-Петербургской академии Следственного комитета, кандидат юридических наук, доцент, полковник юстиции.

Попов Алексей Михайлович – декан факультета подготовки следователей Московской академии следственного комитета Российской Федерации, полковник юстиции, кандидат юридических наук, доцент.

Побегайло Анастасия Эдуардовна – доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, кандидат юридических наук, советник юстиции.

Посельская Людмила Николаевна – кандидат юридических наук, доцент, Московский университет МВД России имени В.Я. Кикотя, доцент кафедры криминалистики.

Прорвич Владимир Антонович – профессор кафедры уголовного процесса Московской академии Следственного комитета России, доктор юридических наук, доктор технических наук, профессор, Почетный профессор Московской академии Следственного комитета России.

Рахманова Екатерина Николаевна – заведующая кафедрой уголовного права Северо-Западного филиала ФГБОУВО «РГУП», доктор юридических наук, доцент.

Савченко Майя Михайловна – доцент кафедры «Экономическая безопасность», ФБГОУ ВО Калининградский государственный технический университет, кандидат экономических наук, доцент.

Саркисян Армен Жораевич – руководитель редакционно-издательского и информационно-библиотечного отдела Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент, майор юстиции.

Семенов Евгений Юрьевич – кандидат юридических наук, доцент профессор кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России имени В.В. Лукьянова.

Серебренникова Анна Валерьевна – профессор кафедры уголовного права и криминологии Юридического факультета МГУ им. М.В. Ломоносова, доктор юридических наук, доцент.

Скобелин Сергей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», кандидат юридических наук, доцент, полковник юстиции.

Смирнова Галина Андреевна – аспирант кафедры публичного и уголовного права Гуманитарного института АНО ВО «Российский новый университет», главный специалист Отдела административной и уголовной практики Дирекции по безопасности АО «Мосэнергосбыт».

Соломатина Анна Георгиевна – доцент кафедры уголовного процесса Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент, полковник полиции.

Соловьев Александр Александрович – и.о. заведующего кафедрой Правовых дисциплин Астраханского филиала Российской Академии Народного Хозяйства и Государственной Службы (РАНХиГС), кандидат юридических наук.

Тимошенко Андрей Анатольевич – заведующий кафедрой международного сотрудничества в сфере прокурорской деятельности, обеспечения представительства и защиты интересов Российской Федерации в межгосударственных органах, иностранных и международных (межгосударственных) судах, иностранных и международных третейских судах (арбитражах)Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

Уханова Надежда Владимировна – доцент кафедры предварительного расследования Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент, полковник полиции.

Феоктистов Максим Викторович — доцент кафедры уголовного права и криминологии Всероссийского государственного университета юстиции (РПА Минюста России), доцент кафедры юриспруденции Российского университета кооперации, Заслуженный юрист Кубани, кандидат юридических наук, доцент.

Хатов Эдуард Борисович – заведующий кафедрой информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета Российской Федерации, к.ю.н., доцент полковник юстиции.

Чич Бислан Еристемович – старший следователь-криминалист отдела криминалистики следственного управления Следственного комитета Российской Федерации по Республике Адыгея.

Шеховцова Любовь Сергеевна – старший преподаватель кафедры криминалистики Московского Университета МВД России имени В.Я. Кикотя, кандидат юридических наук, подполковник полиции.

Шестак Виктор Анатольевич – профессор кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД России, доктор юридических наук, доцент.

Шиян Валентина Ивановна – доцент кафедры «Уголовное право, уголовный процесс и правоохранительная деятельность» Юридического института Российского университета транспорта, кандидат юридических наук, доцент.

Шурухнов Владимир Александрович – доцент кафедры судебно-экспертной и оперативно-розыскной деятельности Московской академии Следственного комитета Российской Федерации, полковник юстиции, кандидат юридических наук, доцент.

Яким Алина Дмитриевна – ассистент кафедры информационных технологий и организации расследования киберпреступлений ФГКОУ ВО "Московская академия Следственного комитета Российской Федерации".

Содержание

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Материалы международной научно-практической конференции

(Москва, 28 апреля 2023 года)

Подписано в печать 06.10.2023

Формат 60х90 1/16
Усл. печ. л. 15,87
Тираж 100 экз.
Печать офсетная
Заказ № 408

Отпечатано в типографии Московской академии Следственного комитета Российской Федерации, ул. Врубеля, д. 12