СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯСЛЕДСТВЕННОГО КОМИТЕТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ И ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Материалы международной научно-практической конференции

(Санкт-Петербург-Москва, 2-3 декабря 2021 года)

Москва, 2022

УДК 343.2
ББК 67.408
П 83

П 83 **Противодействие киберпреступлениям и преступлениям в сфере высоких технологий**: материалы международной научно-практической конференции (Санкт-Петербург-Москва, 2-3 декабря 2021 года) М. Московская академия Следственного комитета Российской Федерации, 2022. – 201 с.

УДК 343.2
ББК 67.408

Сборник сформирован по материалам, представленным на международную научно-практическую конференцию, проведенную одновременно в Санкт-Петербургской и Московской академиях СК России 2-3 декабря 2021 года. В конференции приняли участие представители центрального аппарата СК России, Общественной палаты России, ведущих вузов страны, а также сотрудники более 40 следственных управлений СК России, обучающиеся академий и иные заинтересованные лица. Сборник представляет интерес для юристов – учёных и практиков. Редакционная коллегия обращает внимание на то, что научные подходы и идеи, и взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

Международная научно-практическая конференция
«Противодействие киберпреступлениям
и преступлениям в сфере высоких технологий»
(2-3 декабря 2021 года)

Международная научно-практическая конференция «Противодействие киберпреступлениям и преступлениям в сфере высоких технологий» состоялась на базе Санкт-Петербургской и Московской академий Следственного комитета 2-3 декабря 2021 года.

С учетом выполнения санитарно-эпидемиологических требований форум проводился в гибридном формате.

Рис.1 Санкт-Петербургская академия СК России

В конференции приняли участие представители центрального аппарата СК России, Общественной палаты России, Академии управления МВД России, Санкт-Петербургского государственного университета, Российского университета дружбы народов, Центра исследования проблем правосудия РГУП, МГЮА, Всероссийского научно-исследовательского института МВД России, международно-правового факультета МГИМО МИД России и других ведущих вузов страны. Участниками работы круглого стола и пленарного заседания были также сотрудники более 40 следственных управлений СК России, обучающиеся академий и иные заинтересованные лица.

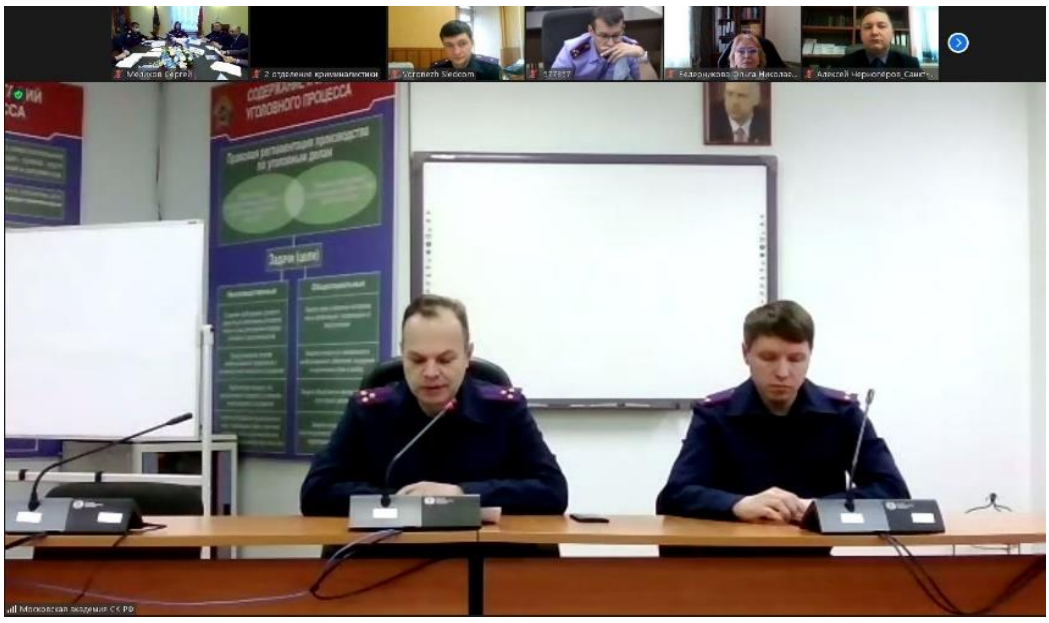


Рис. 2 Московская академия СК России

С приветственным словом к участникам конференции обратились и.о. ректора Санкт-Петербургской академии Елена Владимировна Емельянова, и.о. ректора Московской академии Алексей Геннадьевич Головач и руководитель управления воспитательной работы Следственного комитета Герой России Сергей Васильевич Петров, которые отметили безусловную актуальность тематики и ее важность для практических работников следственных органов. Кроме того, было озвучено письменное приветствие от имени руководства Российского общества «Знание», в котором подчеркнута возможность использования материалов форума в просветительской деятельности.

Заседание круглого стола было посвящено вопросам информационной безопасности детей. Участники мероприятия затронули такие важные и актуальные темы, как защита прав несовершеннолетних в цифровой среде, геймификация как инструмент вовлечения в деструктивные сообщества.

Выступающими приведен анализ отдельных проблем расследования киберпреступлений, озвучены пути их решения. Отдельными предметами дискуссии стали вопросы статуса цифровых свидетельств преступлений в онлайн-пространстве, выявления и блокировки запрещённой информации как средства профилактики преступлений, применения программно-аппаратных средств защиты информации, соблюдения прав человека при цифровизации и ряд других.

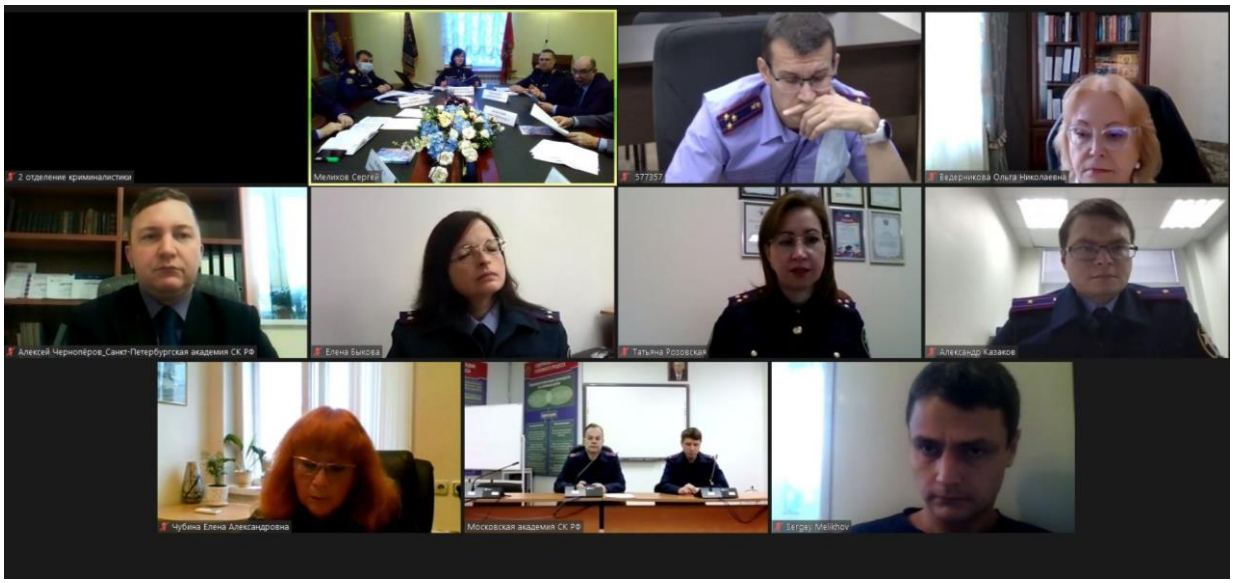


Рис. 3. Работа секции в гибридном формате

Перед официальным открытием конференции, 02 декабря 2021 года на прошла молодежная секция «Использование специальных знаний при расследовании киберпреступлений и преступлений в сфере высоких технологий», в которой приняли участие обучающиеся (студенты, магистранты, курсанты) образовательных организаций высшего образования Российской Федерации, а также научно-практический круглый стол для сотрудников следственных подразделений «Использование электронно-цифровой информации в

доказывании по делам о киберпреступлениях и преступлениях в сфере высоких технологий».

В работе молодежной секции приняли участие более 140 обучающихся из образовательных организаций Следственного комитета России, МВД России, Минобороны России, Балтийского федерального университета имени Иммануила Канта, Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Санкт-Петербургского государственного университета, Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева, Финансового университета при Правительстве Российской Федерации, Московского государственного института международных отношений (университет) Министерства иностранных дел Российской Федерации, Юридического института Российского университета дружбы народов.

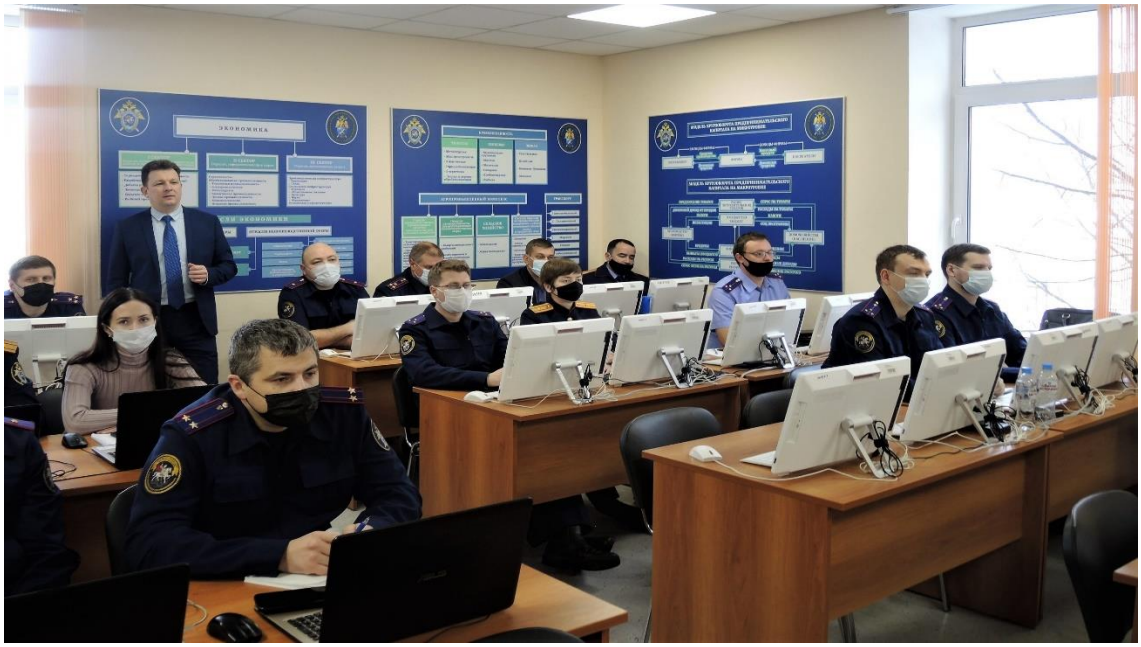


Рис. 4. Работа конференции

В своих докладах выступающие затронули актуальные проблемы расследования киберпреступлений и преступлений в сфере высоких технологий, вопросы их профилактики, а также причинно-следственные аспекты существования и роста рассматриваемой группы противоправных явлений. По окончании работы секции ее участники констатировали, что мероприятие оказалось полезным и продуктивным, а также выразили готовность к дальнейшему сотрудничеству в научной сфере.

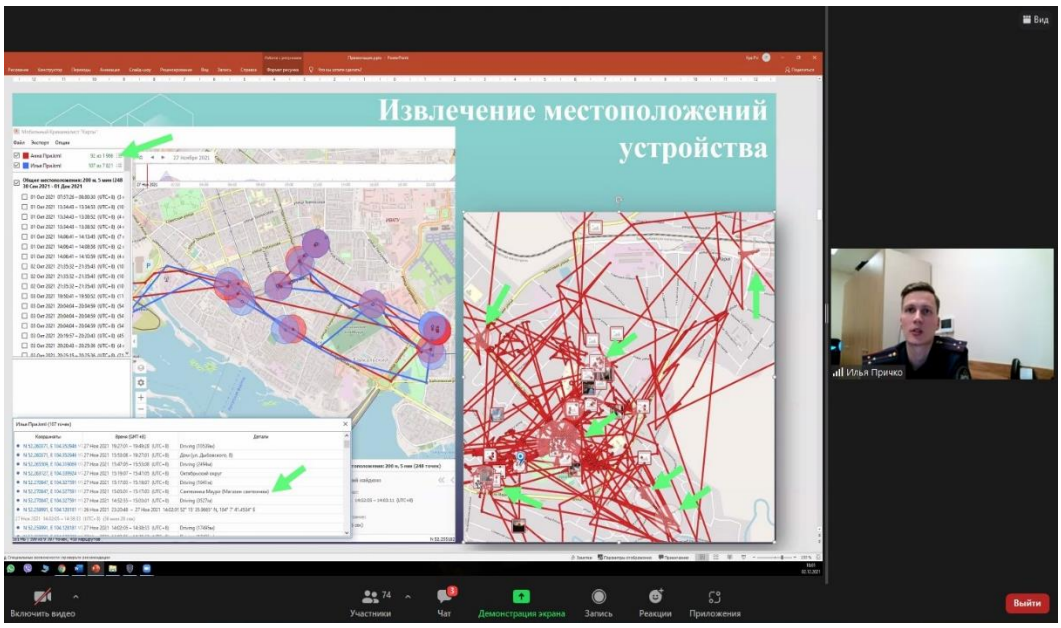


Рис. 5. Работа конференции

Работа научно-практического круглого стола, проводимая среди сотрудников следственных подразделений «Использование электронно-цифровой информации в доказывании по делам о киберпреступлениях и преступлениях в сфере высоких технологий», осветила вопросы сбора и анализа доказательственной информации из открытых источников; организации и проведения судебных компьютерно-технических и информационно-аналитических экспертиз; доказательственного значения электронно-цифровой информации; использования информации, полученной от операторов сотовой связи.

Оргкомитет конференции

Е.В. Баркалова

Актуальные вопросы уголовного преследования по делам о преступлениях, совершенных в отношении несовершеннолетних с использованием информационно-коммуникационных технологий

Осуществление уголовного преследования как на досудебных стадиях уголовного судопроизводства, так и при поддержании государственного обвинения в суде по делам о преступлениях в отношении несовершеннолетних с использованием информационно-коммуникационных технологий имеет определенные особенности, вызванные спецификой процессуального статуса потерпевшего, а следовательно законодательными ограничениями и комплексом тактических рекомендаций по производству следственных и иных процессуальных действием с его участием, а также особенностями способа совершения преступления – использование современных технических средств, из-за которых место нахождения потерпевшего и обвиняемого не совпадают и возникают проблемы с идентификацией виновного лица. При этом можно предотвратить ряд негативных для государственного обвинителя судебных ситуаций, включая попытки стороны защиты дезавуировать доказательства по уголовному делу, в случае соблюдения требований уголовно-процессуального законодательства, прогнозирования версий стороны защиты и своевременного сбора доказательств для их опровержения.

Наиболее распространенными преступными посягательствами в рассматриваемой сфере в отношении несовершеннолетних являются развратные действия и доведение до самоубийства или склонение к самоубийству. Высокая степень общественной опасности заключается в том, что совершение преступлений против половой свободы и половой неприкосновенности в отношении несовершеннолетних вызывает нездоровый интерес к половым отношениям, и в дальнейшем виновные совершают половые преступления в отношении несовершеннолетних не дистанционно, а с непосредственным контактом, договариваясь о встречах через социальные сети и мессенджеры. Вторая группа преступных посягательств не менее общественно опасна, поскольку круг охватываемой аудитории потенциальных потерпевших весьма обширен, и несвоевременное выявление законными представителями и сотрудниками образовательных учреждений таких контактов может привести как минимум к психологической травме, как максимум попытке совершения самоубийства или самоубийству.

В круг обстоятельств, подлежащих доказыванию согласно статье 73 Уголовно-процессуального кодекса РФ, включаются причины и условия, способствовавшие совершению преступления. В связи с этим сразу после выявления преступных посягательств в отношении несовершеннолетних необходимо проводить анализ деятельности различных органов и организаций в сфере образования, здравоохранения, организации досуга несовершеннолетних, поддержки семьи, материнства и детства, охраны безопасности и общественного порядка и выявлять недостатки и упущения в работе указанных органов, которые

не позволили своевременно определить наличие криминогенной ситуации в конкретной семье, образовательном учреждении, а также принимать меры реагирования в отношении контролирующих органов на самых ранних стадиях уголовного судопроизводства. Данное требование не всегда выполняется или в ряде случаев выполняется формально.

При производстве следственных действий с участием несовершеннолетних необходимо обеспечивать участие законных представителей и педагогов (психологов). При этом возникают вопросы относительно надлежащего выполнения своих функций законными представителями и своевременного реагирования следователями в случае оказания ими противодействия (неявки для участия в следственных действиях, попыток сорвать их производство, отрицательное отношение к применяемым следователем средств фиксации следственных действий, ко всем кандидатурам участников, склонение несовершеннолетнего к даче определенных показаний или отказу от их дачи вообще). В качестве таких случаев можно рассматривать отказ в применении видеозаписи при производстве следственных действий. Видеофиксация позволит в дальнейшем не вызывать в суд для допроса несовершеннолетнего потерпевшего во избежание его травмирования. Однако, на практике многие следователи отрицательно относятся к видеофиксации, поскольку опасаются возможных нарушений процессуальных требований по применению видеосъемки и полноты фиксации показаний несовершеннолетних, а также в целях экономии времени. В связи с этим допрос несовершеннолетних должен проводиться подробно по заранее составленному плану с подбором необходимого круга участников. В случае возражения законным представителем против применения видеосъемки полагаем возможным ставить вопрос о его отстранении от участия в деле и замене на другого.

В ряде случаев возникает вопрос о надлежащей кандидатуре педагога (психолога) при подборе участников следственных действий. На практике в качестве педагога (психолога) привлекают штатного психолога из образовательного учреждения начального или среднего уровня или сотрудника органов опеки и попечительства с профильным образованием, однако не во всех муниципалитетах есть такие специалисты. Наличие диплома о профильном высшем образовании не является гарантией получения достоверных и последовательных показаний несовершеннолетнего в ходе допроса, но в условиях дефицита специалистов не всегда его кандидатуре с точки зрения опыта работы и наличия определенных профессиональных качеств уделяется столь пристальное внимание. Установление психологического контакта с несовершеннолетним, помощь в формулировке вопросов, психологическая подготовка к допросу и участию в других следственных действиях несовершеннолетнего – это лишь часть задач, возложенных на педагога (психолога) как на досудебных стадиях уголовного судопроизводства, так и в ходе рассмотрения уголовного дела судом.

Особое значение приобретает заключение комплексной психолого-психиатрической экспертизы несовершеннолетнего потерпевшего, поскольку ее проведение позволяет ответить на вопросы о психологическом состоянии и

особенностях ребенка, выражающихся в наличии психических расстройств, фобий, соответствия уровня психического и интеллектуального развития возрасту, наличии определенных личностных качеств, склонности к чрезмерному фантазированию, патологической склонности ко лжи и др. Ответы на последние из указанных вопросов следует оценивать критически с учетом склонности всех детей до 14-летнего возраста к фантазированию, зачастую отождествления себя с мультипликационными героями, сказочными персонажами, получением зачастую нефильтрованной информации из Интернета относительно способов преступлений, поведения участников уголовного процесса и пр. Так, по одному из уголовных дел о преступлениях, предусмотренных ч. 1 ст. 132 УК РФ, в заключении комплексной психолого-психиатрической экспертизы в отношении несовершеннолетнего потерпевшего было указано, что вербальная информация согласуется с невербальными действиями мальчика, что свидетельствует о правдивости сообщенных им сведений относительно действий сексуального характера отчима несовершеннолетнего в отношении него.

По уголовным делам о склонении к самоубийству и доведении до самоубийства психолого-психиатрическая экспертиза потерпевшего, в том числе посмертная, позволит установить характер и степень негативного воздействия информационного контента на ребенка, побудивших его к суицидным попыткам, а также исследовать в целом особенности психического состояния ребенка. При этом оценку самому содержанию информации, направляемой несовершеннолетнему, следователь будет давать с учетом заключений других специалистов, например, психолингвистов, или экспертов в области видеофоноскопии в зависимости от формы предоставленного материала.

Современные технические возможности позволяют сделать привязку к определенному месту гаджета, который использовался для выхода на связь потерпевшего и виновного, однако установить, что конкретное лицо его использовало и вело переписку с ребенком, отправляя ему запрещенный контент, вызывает определенные сложности на практике. Особенно часто возникают проблемы, если это обстоятельство не проверено следователем в виду того, что обвиняемый признает вину в совершенном преступлении, однако на стадии судебного следствия отказывается от ранее данных показаний, выдвигая новое алиби.

Так, осужденный ранее за совершение преступлений против половой свободы и половой неприкосновенности, отбывая наказание в местах лишения свободы, отправлял несовершеннолетним девочками фотографии обнаженных мужских половых органов, просив их также сделать собственные интимные фотографии и направить ему. При рассмотрении судом уголовного дела подсудимый выдвинул версию о том, что мобильным телефоном пользовался его сокамерник, который ко времени судебного следствия уже скончался. Стороне обвинения пришлось представлять документы и ходатайствовать о вызове в суд для допроса сотрудников исправительного учреждения с целью установления периода совместного пребывания в камере этих осужденных, его сверкой с датами

переписки с несовершеннолетними, установлением вопроса о продолжении переписки после смерти сокамерника подсудимого.

Определенные сложности вызывает также опровержение версии обвиняемого о том, что он не был осведомлен о несовершеннолетнем возрасте потерпевшего ввиду дистанционного характера общения и указании в социальных сетях недостоверных сведений о себе, размещении чужих фотографий или их отсутствии, использовании программ-редакторов фотоснимков. Наличие в персональном аккаунте потерпевшего сведений о месте его обучения, фотоснимков потерпевшего, их получение обвиняемым, исходя из которых очевиден несовершеннолетний возраст потерпевшего, позволяют опровергнуть рассматриваемую версию, если потерпевший и обвиняемый познакомились через интернет-ресурсы.

Полнота, эффективность и законность проведенных следственных и иных процессуальных действий, прогнозирование и своевременная проверка версий стороны защиты, учет правовых, организационных и тактических особенностей производства следственных действий с учетом процессуального статуса несовершеннолетнего, законодательных ограничений и возрастных особенностей позволят осуществлять своевременное и эффективное противодействие рассматриваемым преступлениям.

Д.В. Белых-Силаев, Д.В. Деулин

Инструментально-психофизиологические методы выявления киберпреступлений, совершаемых с помощью социальной инженерии

Аннотация. Статья посвящена рассмотрению отдельных проблем социальной инженерии как совокупности подходов в прикладных социальных науках, ориентированных на изменение поведения и установок людей, разрешение социальных проблем. Дискутируется взгляд на социальную инженерию как на технологию не только правомерного, но и противоправного поведения. Обсуждаются возможности полиграфа для противодействия противоправному технологий социальной инженерии.

***Ключевые слова*:** инструментально-психофизиологические методы; полиграф; анализатор стресса по голосу; термография; термоэнцефалоскопии; айтрекинг; социальная инженерия; социальная установка (аттитюд); мошенничество; киберпреступность.

В настоящее время социальная инженерия рассматривается как совокупность подходов в прикладных социальных науках, ориентированных на изменение поведения и установок людей, разрешение социальных проблем, адаптацию социальных институтов к изменяющимся условиям и сохранение социальной стабильности[1]. Вместе с тем, отдельные методы социальной инженерии могут быть использованы не на общественное благо, а в угоду частным интересам. Так, в сфере высоких технологий методы социальной инженерии могут быть использованы для незаконного доступа к информации или системам хранения

[1] Электронный ресурс: URL: https://dic.academic.ru.

информации без использования технических средств. Сами инструменты социальной инженерии могут быть направлены на изменение поведения человека, его привычного паттерна поведения путем введения в заблуждения или предоставление неточных сведений.

Социальная инженерия сегодня выступает как особый вид мошенничества с привлечением современных технологий. Прообраз социальной инженерии можно обнаружить в рекламе. Там цель – убедить любыми способами человека в необходимости приобретения рекламируемой продукции, в обосновании чего-либо. Примером может быть применения софистики. Всем известный античный софизм: «*У тебя есть то, что ты не терял, ты не терял рога, значит у тебя есть рога*»[1]. В рекламе можно встретить «незавершенный» софизм. Например, для обоснования показа рекламы в московском метрополитене можно перед входом в Интернет прочитать надпись «*Пока вы смотрите рекламу – в мире рождается 356 котят*». Создается бессознательная установка на одобрение просмотра рекламы, ведь в результате рождаются котята. Цель таких софизмов – ввести в заблуждение слушателя, вызвать положительные эмоции.

Мы продемонстрировали пример непреступного использования социальной инженерии, направленный не на приобретении информации, а наоборот, на предоставление ненужной информации с целями продвижения продукции и услуг. Существуют более агрессивные формы социальной инженерии, которые воплощаются в современном информационном пространстве. Так, с помощью методов социальной инженерии можно совершать уголовно-наказуемые деяния: «бесконтактные убийства» (синий кит) – поиск психологической информации о пользователях сети с целью довести их до самоубийства. Это могут быть иные преступления, с помощью общения в информационном пространстве приобретая «ключи доступа» к аккаунтам банковских карт, злоумышленники совершают хищение денежных средств. Высокие технологии и методы социальной инженерии становятся удобным универсальным орудием преступления. Но компьютерные технологии и методы социальной инженерии представляют опасность только при совмещении их с преступным умыслом.

В целях разоблачения злоумышленников, можно использовать современную инструментально-психологическую методологию выявления скрываемой информации. Воздействуя на преступника психологическими стимулами и регистрируя деятельность его физиологических систем, можно анализировать достоверность информации, тем самым определять его предрасположенность к реализации преступного умысла.

Важно отметить, что в настоящее время среди наиболее надежных инструментальных методов выявления скрываемой информации остается полиграф. Однако, развитие науки и техники не оставляет сомнений в том, что в скором будущем будут совершенствоваться технические возможности аппаратных средств диагностики лжи. Кроме того, будут создаваться инновационные методы, основанные на сканирование участков головного мозга

[1] Брутян Г. Паралогизм, софизм и парадокс // Вопросы философии. 1959. № 1. С. 56-66.

с целью фиксации очагов возбуждения в ответ на предъявление значимых стимулов.

Сегодня одной из разновидностей психофизиологического метода выявления лжи является «анализатор стресса по голосу». Данный метод основан на том, что происходит регистрация изменений динамики речевого сигнала в ответ на предъявленные в ходе процедуры стимулов. Обработка происходит с помощью специальной компьютерной программы. Суть метода заключается в выявление латентных акустических характеристик голова, которые обусловлены стрессовой реакцией организма. В основе этого механизма находятся результаты исследований физиолога Липпольда, который установил, что в состоянии полного расслабления и покоя скелетные мышцы испытывают миографический тремор (микровибрацию). В состоянии психофизиологического возбуждения этот тремор ослабевает или исчезает совсем.[1]

Вместе с тем, в научных публикациях имеется существенная критика данного метода. Так американский специалист П.Экман в своей книге рассказывает о «машинах», способных якобы с высокой точностью определять ложь по голосу. Однако в работе акцентируется внимание на недостаточной обоснованности соотношения лжи и стресса. В инструкциях к этим приборам есть предупреждение пользователей о рисках пропуска лжецов, не испытывающих отрицательных эмоций, и наоборот – «*неправильно истолковать поведение правдивых людей, которые чем-то расстроены*»[2].

Как отмечают Оглоблин С.И. и Молчанов А.Ю. сама процедура обнаружения ложных сведений с опорой на голосовой анализатор стресса принципиально не отличается от процедуры классической детекции с использованием полиграфных устройств[3]. Авторы, обосновывая низкую достоверность результатов такого обследования, указывают, прежде всего, на использование недостаточного количества показателей одного канала. Это увеличивает субъективность результатов исследования, снижает их точность[4].

Холодный Ю.А., рассматривая основные методы «криминалистической полиграфологии», указывает на акустический метод, реализуемый с помощью так называемых анализаторов стресса по голосу, ориентированного на диагностику идеальных следов события путем оценки амплитудно-частотных характеристик голоса человека, а также психолингвистический метод, реализуемый в тех же целях путем контроля и оценки темпоральных (временных), лексических и синтаксических характеристик речи человека[5].

---

[1] Пеленицын А.Б., Степанов А.А. Детекторы лжи по голосу [Электронный ресурс] код доступа: http://poligraf.sp.ru

[2] Экман П. Психология лжи. Обмани меня, если сможешь. И: Питер, 2010. - 304 с.

[3] Оглоблин С.И., Молчанов А.Ю. Инструментальная «детекция лжи». – Ярославль: Нюанс, 2004. 147 с.

[4] Там же. С. 149.

[5] Холодный Ю.И. Криминалистическая полиграфология и ее применение в правоохранительной практике // Информационный бюллетень № 21 по материалам криминалистических чтений «Запросы практики – движущая сила развития криминалистики и судебной экспертизы». М.: Академия управления МВД России, 2003. С. 14-19.

Разновидностью инструментальных средств выявления скрываемой информации является энцефалографический и магнито-энцефалографический методы исследования мозговой активности. В некоторых исследованиях приводятся убедительные данные об эффективности одного из данных методов. Так, в исследованиях способов повышения контроля работы операторов сложных промышленных систем и установок, а также в целях совершенствования проверки квалификации персонала при приеме на работу новых сотрудников применялся метод анализа энцефалограммы испытуемого. Изучение так называемой «вызванной активности» головного мозга на сложный визуально-когнитивный стимул с целью использования этого эффекта в целях выявление ложных сведений позволяет говорить о принципиально новых прогрессивных методах в этой области[1].

На протяжении ряда лет исследуются возможности разных альтернативных методов инструментальной диагностики ложных сведений. В некоторых статьях приводятся доводы в пользу возможной эффективности рассматриваемых альтернативных способов. Таким образом, все методы сводятся к группе направлений:

- анализ вызванных потенциалов мозга, изображений, полученных методом ядерного магнитного резонанса;
- измерение стресса в голосе;
- термография (измерение температуры участков тела);
- динамическое измерение диаметра зрачка глаза (айтрекинг).

Интересным является метод термического анализа поверхности кожи. Разработаны специальные технические приборы, которые используются для оценки изменений кровоснабжения отдельных участков поверхности лица. Главной целью использования тепловизоров является обнаружение кратковременных изменений кровотока, обусловленных активностью симпатической нервной системы[2].

Также относительно новым направлением исследования выявления ложных сведений является измерение зрачковой реакции. Прежние визуальные наблюдения показали, что в процессе лжи действительно наблюдаются изменения размера зрачка[3]. В некоторых работах, авторы отмечают, что, в частности было показано, что зрачковая реакция возникает при ответах на все вопросы, относящиеся к преступлению, однако она более выражена при ложных ответах на них[4].

В ряде работ в качестве наиболее перспективного метода отмечается метод термоэнцефалоскопии (метод, анализирующий активность коры головного мозга

---

[1] Коршаков А.В., Шатерников В.Е. Идентификация и определение достоверности принятых решений по вызванной энцефалографической активности // Промышленные АСУ и контроллеры. № 8. – 2013. – с.20-25; Белых-Силаев Д.В. Психофизиологические методы детекции лжи // Юридическая психология. № 2. – М., 2017. С. 31-35.

[2] Дженнифер Вендемия. Детекция лжи // «Polygraph». – 2003. № 32 (2). – с. 97-106. Электронный ресурс, код доступа: http://www.poligraftest.ru.

[3] Навваро Д., Карлинс М. Я вижу, о чем вы думаете – Минск: «Попурри», 2009. 336 с.

[4] Там же. С. 97-106.

посредством регистрации локальных изменений температур), разработанный в Институте высшей нервной деятельности и нейрофизиологии РАН и в Институте радиоэлектроники (Шевелев И. А.) в 80-х годах прошлого века[1].

Такое изобилие инструментальных технических средств обнаружения скрываемой информации позволяет комплексно подходить к проблеме оценки и верификации скрываемой информации в рамках противодействия преступлений в сфере высоких технологий, совершаемых с применением методов социальной инженерии.

Литература

1. Белых-Силаев Д.В. Психофизиологические методы детекции лжи // Юридическая психология. № 2. – М., 2017. С. 31-35.
2. Брутян Г. Паралогизм, софизм и парадокс // Вопросы философии. - 1959.- № 1. С. 56-66.
3. Дженнифер Вендемия. Детекция лжи // «Polygraph». – 2003. № 32 (2). – с. 97-106 [Электронный ресурс] код доступа: http://www.poligraftest.ru.
4. Коршаков А.В., Шатерников В.Е. Идентификация и определение достоверности принятых решений по вызванной энцефалографической активности // Промышленные АСУ и контроллеры. № 8. – 2013. С. 20-25.
5. Навваро Д., Карлинс М. Я вижу, о чем вы думаете – Минск: «Попурри», 2009. 336 с.
6. Оглоблин С.И., Молчанов А.Ю. Инструментальная «детекция лжи». – Ярославль: Нюанс, 2004. - 417 с.
7. Пеленицын А.Б., Степанов А.А. Детекторы лжи по голосу [Электронный ресурс] код доступа: http://poligraf.sp.ru.
8. Холодный Ю.И. Криминалистическая полиграфология и ее применение в правоохранительной практике // Информационный бюллетень № 21 по материалам криминалистических чтений «Запросы практики – движущая сила развития криминалистики и судебной экспертизы». М.: Академия управления МВД России, 2003. С. 14-19.
9. Экман П. Психология лжи. Обмани меня, если сможешь. И: Питер, 2010. - 304 с.

С.Н. Боков, М.И. Жданов

Психологическое онлайн-тестирование и проблемы защиты персональных данных

Аннотация. В статье рассмотрены риски использования результатов психологической онлайн-диагностики в качестве инструмента для несанкционированного воздействия на испытуемых. Показано, что каждая

[1] Оглоблин С.И., Молчанов А.Ю. Инструментальная «детекция лжи». – Ярославль: Нюанс, 2004. 417 с.

психодиагностическая методика может иметь двойное применение – как для оказания направленной психотерапевтической (медико-психологической) помощи обследуемому, так и для применения к нему несанкционированного, зачастую скрытого, деструктивного психологического воздействия. Указывается на необходимость разработки чёткого законодательного регулирования психологической онлайн-диагностики.

Ключевые слова: психология; право; государственная безопасность; психологическое тестирование; психологическое онлайн-тестирование; персональные данные; защита персональных данных; информационно-психологическое воздействие; информационные войны.

В последние десятилетия широкое распространение получило психологическое онлайн-тестирование. На многочисленных сайтах предлагается возможность пройти диагностику самого широкого спектра индивидуально-психологических и социально-психологических особенностей личности: профориентационных; интеллектуальных; особенностей мышления; особенностей памяти; особенностей темперамента и характера; семейных взаимоотношений; особенностей сексуального поведения; особенностей межличностных отношений; суицидального риска и многого другого.

На ряде сайтов для прохождения тестирования предлагается ввести некоторые личные данные испытуемого – пол, возраст (иногда дату рождения), образование, причём не всегда для тех методик, для которых такие данные имеют значение при выборе варианта методики и обработки результатов.

Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных», под персональными данными понимается любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).[1] Закон, определяя понятие биометрических персональных данных и специальных категорий персональных данных, прямого понятия психологических персональных данных не содержит[2], однако с определёнными основаниями к психологическим персональным данным могут быть отнесены упоминаемые в части 1 статьи 10 сведения о состоянии здоровья и интимной жизни.

На заседании Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека член Совета И. Борисов обратил внимание Президента на необходимость регулирования использования видеотрафика, который идёт с избирательных участков. В частности, он указал, что практически миллион просмотров были инициированы с IP-адресов из-за рубежа. «Вопрос: для чего такое количество интересантов смотрит наши выборы и проводит видеозапись фактически образа человека и как он дальше будет использоваться с учётом тех технологий, которые сегодня существуют?

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Ст. 3. – URL: http://ivo.garant.ru/#/document/12148567/paragraph/14:0. Дата обращения 12.12.2021.

[2] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Ст. ст. 10, 11. URL: http://ivo.garant.ru/#/document/12148567/paragraph/77:0, http://ivo.garant.ru/#/document/12148567/paragraph/89:0. Дата обращения 12.12.2021.

То есть лично я озабочен тем, что образы моих сограждан оказываются в чужих руках, и непонятно, как и для каких целей они там будут находиться».[1]

Отвечая ему, Президент Российской Федерации В. В. Путин сказал: «По поводу того, что образы наших граждан, избирателей собираются кем-то и как-то используются… Образы-то ладно, а вы знаете, что биологический материал собирается по всей стране, причём по разным этносам и людям, проживающим в разных географических точках Российской Федерации? Вот вопрос: вот это зачем делают?

Делают целенаправленно и профессионально. Мы – такой объект очень большого интереса. Поэтому и в первой части того, что я сказал, всё это взаимосвязано. Нам нужно, конечно, без всяких страхов к этому относиться. Они пускай делают, что они хотят, а мы должны делать то, что мы должны, и с учётом ваших замечаний будем выстраивать эту работу».[2]

Результаты проведённых психодиагностических обследований представляют собой ценный материал, позволяющий получить сведения об индивидуально-психологических особенностях испытуемого (и группы испытуемых), а также для разработки мероприятий психологического воздействия на него (соответственно – группу испытуемых), включая дистанционное информационное воздействие. В свою очередь это может представлять реальную угрозу безопасности страны, так как полученные при проведении психодиагностических обследований групп населения данные могут быть положены в основу отдельных технологий информационной войны. Подобные аспекты использования результатов психодиагностических обследований фактически пока ещё не привлекают к себе должного внимания соответствующих специалистов.

Между тем каждая валидизированная, надёжная и стандартизированная психодиагностическая методика позволяет получать такие сведения.

Например, Шкалы интеллекта Векслера (для взрослых и детей) позволяют получить широкий спектр информации об общей осведомлённости, понятливости, способности осуществления базовых мыслительных операций, ряде нейропсихологических особенностей и др.

Методика диагностики социального интеллекта позволяет оценивать способность испытуемых быстро, практически автоматически, воспринимать, понимать и правильно оценивать поведение окружающих и на этой основе выстраивать своё собственное, наиболее адаптивное в данной ситуации поведение.

Опросник враждебности Басса-Дарки диагностирует различные разновидности агрессивного поведения (предрасположенность испытуемого к физической агрессии, косвенной агрессии, вербальной агрессии, раздражительности, негативизму, обидчивости, подозрительности, возникновению чувства вины.

[1] URL: http://www.kremlin.ru/events/president/transcripts/55947. Дата обращения 19.12.2021.
[2] URL: http://www.kremlin.ru/events/president/transcripts/55947. Дата обращения 19.12.2021.

Опросник приспособляемости Белла выявляет особенности семейной приспособляемости, приспособляемости к болезням и травмам, уживчивость, враждебность, эмоциональную уравновешенность и др.

Личностный опросник Дженкинса, выявляя склонность в реализации так называемого поведения типа А, даёт возможность определять предрасположенность к развитию сердечно-сосудистых заболеваний.

Опросник Плучека-Келлермана-Конте «Индекс жизненного стиля» диагностирует состояние механизмов психологической защиты личности (вытеснения, отрицания, замещения, компенсации, реактивных образований, проекции, интеллектуализации (рационализации) и регрессии).

Методика диагностики интерперсональных отношений Т. Лири выявляет свойственные испытуемому типы межличностных отношений: властного-лидирующего, независимого-доминирующего, прямолинейного-агрессивного, недоверчивого-скептического, покорного-застенчивого, зависимого-послушного, сотрудничающего-конвенциального или ответственного-великодушного.

Изучение локуса контроля личности (уровня субъективного контроля) позволяет диагностировать психологическую основу любой ответственности: принимает ли обследуемый на себя ответственность за различные происходящие в ним в жизни события (то есть человек принимает на себя ответственность) либо же он считает, что всё происходящее с ни от него фактически не зависит, а зависит от других людей, обстоятельств, судьбы и т. д. (то есть имеется перекладывание ответственности на других, сам человек ответственность на себя не принимает).

Один из самых фундаментальных и часто используемых личностных опросников – MMPI (СМИЛ, ММИЛ, СМОЛ) – даёт развёрнутую картину эмоционально-мотивационных особенностей личности. С его помощью определяются такие базовые параметры, как соматизация тревоги (сверхконтроль), тревога/тревожность (пессимистичность), вытеснение тревоги (эмоциональная лабильность), социальная конфликтность (импульсивность), преобладание у испытуемого интересов, традиционно приписываемых мужчинам или женщинам(мужественность-женственность), подозрительность в межличностных взаимодействиях (ригидность), сенситивность в межличностных отношениях, социальная аутизация (индивидуалистичность) и социальная активность (оптимистичность). Кроме того, использование многочисленных дополнительных шкал позволяет выявлять, в частности, способность к обучению, склонность к алкоголизации, антисоциальные тенденции, лидерские качества, альтруизм, наличие идей преследования, самоудовлетворённость, толерантность и мн. др.

Опросник терминальных ценностей (И. Г. Сенин) позволяет диагностировать жизненные цели (терминальные ценности) испытуемого, такие, как собственный престиж, высокое материальное положение, креативность, активные социальные контакты, развитие себя, достижения, духовное удовлетворение, сохранение собственной индивидуальности).

Из приведённого, далеко не полного, перечня используемых в настоящее время психодиагностических методик отчётливо видно, сколь широкий спектр индивидуальных особенностей личности можно выявить при их применении. Получая результаты таких исследований, соотнесённые по отдельным группам населения, возникает риск использования их для разработки методик информационно-психологического воздействия на эти группы, что может угрожать государственной безопасности. Всё это настоятельно диктует необходимость чёткого правового регулирования психологического онлайн-тестирования.

Л.В. Голоскоков

Об элементах доктрины борьбы с киберпреступностью

Аннотация. В статье рассмотрено состояние дел в сфере разработки элементов доктрины борьбы с киберпреступностью. Показано, что поскольку пока в России нет общей доктрины, частная доктрина, например в уголовном праве, не сможет обеспечить эффективную правоохрану, борьбу с преступностью или профилактику преступности в полной мере, а также дать ответ на вопрос, что является в государстве приоритетным, первичным, а что второстепенным в деле борьбы с преступностью нового вида – киберпреступностью. Предлагается начать работать над комплексом доктринальных идей на всех уровнях.

Ключевые слова: право, уголовное право, латентность, доктрина, киберпреступность.

Как известно, преступность в цифровой среде имеет латентность, которая оценивается разными авторами на уровне 95-99%, но мы полагаем, что и такие цифры не отражают реальной картины, потому что надёжных инструментов оценки латентности в этой сфере не существует, а те методы, которые выдаются за такой инструмент, представляют собой лишь частичный механизм прорисовки картины в этой сфере. Специалисты пишут, что «по одним оценкам, соотношение зарегистрированных и латентных преступлений варьируется в пределах от 1:3 до 1:5; другие эксперты говорят о соотношении 1:100 и даже большем. Применительно к наиболее опасному проявлению коррупции – взяточничеству давалась экспертная оценка, согласно которой выявляется менее 1% этих преступлений»[1].

Для противодействия киберпреступности А.А. Бессонов предлагает использовать цифровую криминалистическую модель преступления, которая должна представлять собой криминалистическую характеристику в машиночитаемой форме, в которой сведения о криминалистически значимых признаках и их закономерных связях между собой выражены в виде математических категорий, уравнений и/или неравенств, и обозначает ряд

[1] Государственная система предупреждения преступлений и иных правонарушений, место в ней органов внутренних дел: курс лекций / [Е.Ю. Титушкина и др.]. Москва: Академия управления МВД России, 2021. С. 29.

требований общего характера к таким моделям: «1) максимальная лаконичность в её математическом описании; 2) адекватность, состоящая в наиболее точном воспроизводстве конкретного вида преступлений как объекта-оригинала, причём в режиме реального времени»[1] и др.

Мы можем согласиться с такой постановкой вопроса и не согласиться одновременно, и в этом сложность рассматриваемой задачи. Объясняем, почему. Максимальная лаконичность в её математическом описании, конечно, в идеале нужна, но второй же пункт требований противоречит первому, потому что достижение адекватности, состоящей в наиболее точном воспроизводстве конкретного вида преступлений как объекта-оригинала будет требовать всё более полного описания, которое неизбежно будет расходиться с лаконичностью. Лаконичность здесь будет всегда неизбежно противостоять наиболее точному воспроизводству, которое будет требовать всё новых деталей и, возможно, сопутствующего ему математического обеспечения, а если ещё учесть совершенно правильное требование о том, что всё это должно происходить в реальном времени, то – тем более.

Как мы видим, вроде бы простейшие правильные рассуждения мгновенно наталкиваются на возникающие барьеры, которые не позволяют нарисовать идеальную конструкцию, не имеющую внутренних изъянов и противоречий. Это говорит, во-первых, об исключительной сложности поставленной задачи, во-вторых, о том, что любые модели в праве начинают строиться не с фундамента, а где-то чуть выше. Но при отсутствии фундамента любые построения моделей или их частей будут страдать неполноценностью.

Характерной чертой нового мышления специалистов в области уголовного-правовых наук является такое правильное направление, как использование междисциплинарного подхода, включающего в себя криминалистику, психологию, методы математики, статистики, машинного обучения и распознавания образов, а также использование ряда методов: кластерный анализ и анализ выбросов, нейронные сети, регрессионный анализ, Байесовская классификация, метод деревьев решений, анализ временных рядов и другие[2]. Снова ничего невозможно возразить против правильности такого мышления. Однако и здесь отсутствует фундамент, и его отсутствие проявляется в том, что нет ответа (понятно, что в исследовании А.А. Бессонова была совершенно другая задача), на вопрос, а для чего это всё нужно в конечном итоге, во имея какой идеи.

Нам мгновенно дадут ответ, и он будет правильным (см. название статьи А.А. Бессонова) – противодействие киберпреступности. Но это ответ правильный, но не абсолютно правильный. В рамках конкретной научной статьи о киберпреступности – правильный, а в рамках глобальной доктрины государства – не полностью правильный, ибо учитывает только ущерб от

[1] Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Сетевое издание «Академическая мысль». 2020. № 4 (13) С. 60.

[2] Там же. С. 60-61.

общественно опасных деяний по преступлениям, перечисленным в УК РФ. Однако существуют деяния, представляющие на один-два порядка большую опасность для государства по величине наносимого ущерба, и которые тоже осуществляются с помощью компьютеров, банковских сетей, то есть с помощью всяких кибернетических устройств, систем и механизмов, но эти деяния не криминализированы и статей в УК РФ по ним нет. Соответственно, здесь нет киберпреступности в её уголовно-правовом понимании, но есть ущерб в сотни раз превосходящий ущерб от киберпреступлений, хотя последний мы точно не знаем в связи с высокой и тоже неизвестной латентностью. Тем не менее, утверждать о том, что не криминализированные деяния, о которых пойдёт речь, наносят ущерб существенно больший, чем все киберпреступления вместе взятые, можно.

Рассмотрим, как говорят в правительстве и парламенте любой страны при принятии нового закона, цену вопроса – за что сражаются все правоохранительные органы. Специалисты МВД приводят такую статистику: «в России за 2019 г. выявлено преступлений с использованием IT-технологий – 294 409 (+68,5 %)»[1]. Это количество преступлений. Ущерб дадим только общий – от всех существующих преступлений, поскольку по ним существует какая-то статистика, причём, официально исходящая от России. В «Отчёте о взаимной оценке» 2019 года FATF приводятся данные о сумме ущерба по всем существующим преступлениям в России, включая и киберпреступления: «По оценкам властей, в 2014–2018 годах ежегодный ущерб, нанесённый преступлениями, расследованными в рамках всех уголовных дел, в среднем составлял примерно 220 миллиардов рублей»[2].

При среднем курсе доллара в 2014 году 38 руб. за доллар ущерб от всех преступлений в сумме 220 миллиардов рублей, если его выразить в долларах, составлял примерно 5,8 млрд долларов, значит, в 2014 году вся правоохранительная система России выявила преступлений на 5,8 млрд долларов, а за рубеж в 2014 году ушло в виде вывоза капитала совершенно легально 151 млрд долларов[3]. В другие годы вывоз капитала был меньше, однако нас интересует вопрос, который вытекает из приведённых цифр – почему за вывезенный капитал, превышающий весь ущерб от всех преступлений в 2014 году в 26 раз (151/5,8=26), причём, вывезенный именно через электронные банковские сети и совершенно легально, никакой ответственности по УК РФ не предусмотрено, и это в условиях, когда Россия все тридцать лет ищет по всему миру инвестиции, в то же время перекачивая через банковские сети и

[1] Государственная система предупреждения преступлений и иных правонарушений, место в ней органов внутренних дел: курс лекций / [Е.Ю. Титушкина и др.]. Москва: Академия управления МВД России, 2021. С. 43.

[2] FATF (2016), Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris. URL: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-russian-federation-2019.html, С. 19, (дата обращения 29.03.2021).

[3] См.: Аганбегян А.Г. О необходимости новой социально-экономической политики // Среднерусский вестник общественных наук. 2020. Том 15. № 3. С. 20–21.

киберсистемы огромные капиталы нашим так называемым «партнёрам», которые в последнее время только и обсуждают возможную войну с Россией.

На этот вопрос и должна ответить доктрина России, которой пока нет, но без которой столь глобальные вопросы не будут решены, а без их решения попытки решить второстепенные вопросы всегда обречены на провал, даже если они звучат как весьма важные, типа «кибернетических преступлений». Эти главные вопросы не решает доктрина уголовного права и уголовный кодекс. Наоборот, кодекс уводит нас от решения таких глобальных задач, потому что наиболее опасные деяния оказываются не криминализированы и подвергать их криминализации законодатель за 30 лет не решился.

Доктрина должна ответить на эти вопросы и расставить приоритеты, в данном случае хотя бы из чисто количественных соображений (сумм ущерба), которые будут сами по себе, без всяких других обоснований правильными.

Есть и другие обоснования, лежащие в сферах науки, культуры, образования, медицины, пенсионной сферы и других сфер, куда могли бы быть направлены уходящие за рубеж капиталы. Свои граждане лишены достаточного уровня медицинского и пенсионного обслуживания, а страны – наши военные противники – получают от России огромные финансы и при этом угрожают ей санкциями и войной. Вот где корень проблемы, а не только в том, как найти в России преступника в сферах киберпреступности или любой другой сфере. Дело ещё и в том, что найденные и возвращённые в бюджет страны деньги от любых преступлений снова попадают в общий финансовый оборот страны и оттуда снова рано или поздно уходят за рубеж в виде вывоза капитала. И это при том, что, разумеется, борьба с преступлениями в сфере киберпреступности нужна так же, как со всеми другими преступлениями. Вот такие сложные связи.

Поэтому сначала нужно взяться за решение главной проблемы. Она хорошо известна депутатам и правительству. О вывозе капитала пишет *Российская газета*: «Мишустин привёл статистику за 2019 год, согласно которой объёмы дивидендов, которые вывели за рубеж российские компании, составили 4,4 трлн рублей. «Только системная работа поможет предотвратить этот вывод», – резюмировал он, призвав депутатов к совместной работе»[1].

Когда такая системная работа начнётся, не ясно, а пока Уголовный кодекс РФ остаётся в своём старом состоянии неведения о длящейся тридцать лет крупнейшей финансовой катастрофе России. Соответственно, учёные должны искать ответы прежде всего на главные вопросы, и понимать, что, например, в Республике Казахстан события января 2022 года были инспирированы не столько какими-то террористами, которых найти и показать так и не смогли, а прежде всего экономическими условиями народа в стране, где происходят точно такие же процессы, как на всём пространстве СНГ, и наблюдается тот же самый

[1] Замахина Т. Мишустин ответил на вопрос Володина о борьбе с выводом средств за рубеж // Российская газета. 12.05.2021 12:16. Рубрика: Власть, URL: https://rg.ru/2021/05/12/mishustin-otvetil-na-vopros-volodina-o-borbe-s-vyvodom-sredstv-za-rubezh.html (дата обращения 01.11.2021).

вывоз капитала из этих стран, который выше иных видов ущербов от преступности, в том числе и от киберпреступлений.

А что же доктрина, которая составляет предмет нашего исследования? Е.А. Русскевич пишет, что «доктрина уголовного права, пожалуй, так и не смогла решить проблему разработки модели системного обновления отечественного уголовного законодательства в условиях информационного общества, не сформулировала общих правил и не предложила чётких критериев его осуществления. Во многом именно по этой причине соответствующие решения законодателя воспринимаются специалистами не как последовательный курс по «оцифровке» отечественного уголовного законодательства, а как спонтанный ответ на актуальные потребности правоприменения, реакция на так называемый «криминализационный повод»[1].

Можно отчасти согласиться с этим выводом, за исключением того, что сама по себе «оцифровка» законодательства без доктрины ни к чему хорошему не приведёт, но мы при этом должны помнить, что доктрина уголовного права, как и Концепция развития гражданского законодательства Российской Федерации должны коррелировать с доктриной общей, стоящей над всеми отраслями права, и такая доктрина должна быть одна и отвечать на фундаментальные вопросы жизни государства и общества. Такой доктрины нет. Причём, мы не зацикливаемся на формальном названии и не утверждаем, что это должна быть доктрина по названию соответствующего документа. Название документа может быть и стратегия, и доктрина, в советское время такие идеи были в составе программы партии и в «Моральном кодексе строителя коммунизма», важно, чтобы в нём были ответы на фундаментальные вопросы государства: куда идём, что строим, во имя чего работаем и живём, каковы наши ценности, за которые будет готов идти умирать наш гражданин, отстаивая их перед лицом внешней угрозы и т.д. Такого документа нет, и пока его нет, частные доктрины и концепции развития отдельных отраслей права не будут способны решать свои вопросы.

Таким образом, Россия нуждается в разработке сначала общих доктринальных положений, и только затем она может перейти к частным, в числе которых будут и доктринальные положения уголовного права. Общие моменты таких положений начали прорабатываться, в частности, это духовные ценности, которые недавно впервые в официальном документе были чётко изложены: «К традиционным российским духовно-нравственным ценностям относятся, прежде всего, жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России. Традиционные

[1] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2022. С. 135-136.

российские духовно-нравственные ценности объединяют нашу многонациональную и многоконфессиональную страну»[1].

Попытки развить ценностную основу продолжаются, например, в виде опубликованного Министерством культуры проекта Указа Президента Российской Федерации «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»[2]. Однако, поскольку это пока проект, судить о его действенности рано.

Создание идейной платформы государства идёт сложно и медленно, и пока оно не состоится, в области уголовного права будут продолжать иметь место только отдельные и разрозненные направления борьбы с теми или иными видами преступлений, причём, без цельной уголовно-правовой политики, без проработанных элементов доктрины борьбы с киберпреступностью, которые должны вытекать из главной доктрины. При таком положении дел эффективная борьба с киберпреступностью будет осложнена именно на концептуальном уровне, а не на уровне права, уголовного права или криминалистики. Необходимо начинать работать над комплексом доктринальных идей на всех уровнях, начиная с разработки общей доктрины, заканчивая переходом к разработке частных доктрин отраслей права.

Такая работа не начата, поскольку все правоохранительные органы ушли в научное исследование частностей, они исследуют проблемы: борьбы с киберпреступностью, борьбы и экстремизмом, борьбы с терроризмом, борьбы с экономическими преступлениями и т.д. Общую и глобальную задачу поставил Президент Российской Федерации В.В. Путин: «Хочу особо подчеркнуть важность профилактической составляющей в работе Следственного комитета. Прошу уделять самое серьёзное внимание не только выявлению, но и устранению условий, способствующих совершению преступлений, вести эту работу системно, в координации с другими ведомствами, органами исполнительной и законодательной власти»[3].

Это и есть высокий концептуальный и доктринальный уровень, но работа на этом уровне не началась потому (но это только одна из причин), что, как мы полагаем, у правоохранительных органов – ни у какого из них, ни у них всех совместно нет достаточных научных ресурсов для решения такой задачи, и поэтому они будут продолжать решать свои сугубо частные, ведомственные и узкие задачи, которые звучат для любого органа одинаково: нужно, чтобы научные исследования данного правоохранительного органа отвечали интересам этого органа. А общая доктрина должна отвечать интересам всего государства, а не отдельного её органа. Пока имеет место такое узковедомственное понимание предназначения науки, выход из данного замкнутого круга на более высокий уровень исследований не произойдёт.

---

[1] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.

[2] Электронный ресурс: URL: https://regulation.gov.ru/projects#npa=123967.

[3] Путин В. В. Обращение по случаю 10-летия Следственного комитета. 15 января 2021 года 09:00, URL: http://www.kremlin.ru/events/president/news/64892 (дата обращения 30.01.2022).

Д.К. Гончаров

Криминалистические особенности выявления, раскрытия и расследования незаконной организации и проведения азартных игр с использованием информационно-телекоммуникационных сетей

Аннотация. В статье рассмотрены вопросы развития информационных технологий и, как следствие, кибреперступности. Проведен анализ специфических признаков преступлений, совершаемых в сфере компьютерных технологий. Рассмотрены особенности организации проведения азартных игр с использованием возможностей информационно-телекоммуникационных устройств. Обращено внимание на специфику получения и исследования следов преступлений данной категории. Предложены некоторые криминалистические рекомендации при расследовании фактов незаконной организации и проведения азартны игр.

Ключевые слова: информационные технологии, киберпреступность, азартные игры, выявление, расследование, криминалистическое обеспечение, электронно-цифровые следы, изъятие игорного оборудования.

В настоящее время применение информационных технологий охватило все сферы жизни современного общества. Повсеместная компьютеризация оказывает положительное влияние на жизнь каждого человека, создает комфортные условия для решения многих социально-бытовых вопросов, и в то же время обуславливает значительный рост киберпреступности. Практически каждое четвертое преступление совершается с использованием IT-технологий[1].

Преступления, совершаемые с использованием информационных технологий, имеют существенную специфику. Преступники, используя технические новшества в сфере высоких компьютерных технологий, получают возможность посягать на наиболее значимые общественные отношения в сфере прав и интересов граждан, общества и государства. Сложность выявления преступлений в сфере информационных технологий, а также возможность их совершения в сети Интернет, увеличивают степень общественной опасности киберпреступлений в разы.

Использование технических возможностей современного компьютерного оборудования дает возможность преступникам дистанционно управлять действиями соучастников, тем самым снижая риски быть обнаруженными.

В преступных группах, совершающих преступления посредством информационно-телекоммуникационных сетей, организатор и исполнитель могут не знать друг друга и никогда не встречаться, что увеличивает степень латентности таких преступлений[2].

---

[1] Официальный сайт МВД России. URL: https: //xn-b1aew.xn-p1ai/reports/item/27024130/ (дата обращения 13.12.2021).

[2] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч.1. – 208 с.

Одним из видов преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, является незаконная организация и проведение азартных игр. Существующие ограничения в сфере игорного бизнеса, введенные Федеральным законом 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», зачастую нарушаются организаторами игорных заведений, с целью получения колоссальной прибыли[1]. В соответствии с требованиями ст. 171.2 УК РФ уголовная ответственность предусмотрена за организацию и (или) проведение игр с использованием игрового оборудования вне игорной зоны либо с использованием информационно-телекоммуникационных сетей, в т. ч. сети Интернет, средств связи, в т.ч. подвижной, либо без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне, сопряженное с извлечением дохода в крупном и особо крупном размере, либо совершенные организованной группой[2].

Организаторы незаконных азартных игр, с целью ухода от уголовной ответственности и придания проводимым азартным играм вида легальной деятельности, маскируют их под Интернет кафе, компьютерные клубы и иные заведения.

Примером может служить сеть незаконных игорных заведений, осуществлявших свою деятельность на территории Республики Крым и г. Севастополя, организаторы которых арендовали помещения, располагавшиеся в местах скопления людей, в районе автовокзалов и рынков, устанавливали на входе в помещения постеры с надписью «WebMoney, кибероплата», а в указанных помещениях проводили азартные игры с использованием сети Интернет.

В криминалистической науке вопросам выявления, раскрытия и расследования преступлений, совершаемых в сфере незаконной деятельности по организации и проведению азартных игр, посвящены исследования А.А. Литвина, Н.В. Машинской, О.В. Усенко, О.Ю. Антонова, А.Г. Себякина, О.П. Науменко.

При этом специальные научные исследования, посвященные методике выявления, раскрытия и расследования незаконной организации и проведения азартных игр с использованием информационно-телекоммуникационных сетей,

---

[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/d6fb3580fbd6ef3e662688c02af241894aa7f3a6/ (дата обращения 10.12.2021).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 01.07.2021). [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/b20820739fab5a2c2645f2c2dba2d73e9025f6e4/ (дата обращения 11.12.2021).

отсутствуют, что приводит к возникающим трудностям организационно-правового и криминалистического обеспечения противодействия данной категории преступлений[1].

Выявление незаконной организации и проведения азартных игр начинается с получения оперативной информации, а также анализа оперативной обстановки.

К признакам проведения азартных игр можно отнести следующие факты:

увеличение электронных переводов денежных средств с одного счета на другой счет в отдельно взятом месте, что подтверждает данные биллинга сотовой связи и банков, обслуживающих счета; жалобы граждан в административные органы, а также органы правопорядка на регулярное появление в определенных местах подозрительных людей, шум, драки, замусоренную придомовую территорию; данные Интернет-провайдеров о выходе в игровые сайты сети Интернет с определенных точек доступа; информация, полученная от микрофинансовых организаций об увеличении количества оформленных потребительских займов в определенном районе; увеличение количества регулярных вызовов такси в ночное время на один и тот же адрес.

При проведении азартных игр зачастую используется обычное компьютерное оборудование, которое путем выхода в сеть Интернет подключается к удаленным игровым серверам, которые, как правило, расположены далеко за пределами Российской Федерации. Установить местоположение таких серверов в большинстве случаев невозможно по техническим причинам. Как правило, организаторы незаконных игорных заведений предусматривают возможность экстренного отключения игорного оборудования, работающего в удаленном доступе, от сети электропитания, в случае появления сотрудников правоохранительных органов. Основная часть электронно-цифровых следов[2] (программ и модулятора случайных цифровых комбинаций) при этом не сохраняется на жестких дисках компьютеров, что создает трудности отнесения данного оборудования к игровому, а проводимые игры к азартным при последующем проведении судебных компьютерно-технических экспертиз.

Поэтому, с целью максимального сохранения электронно-цифровых следов, рекомендуется фиксировать процесс проведения азартных игр оперативно-розыскными методами, в момент функционирования игорного оборудования в игровом зале. Также, на стадии доследственной проверки необходимо принять все возможные меры оперативного характера к установлению как личности организатора и круга лиц, участвующих в незаконной игорной деятельности[3], так и возможного местонахождения удаленных северов, используемых при проведении азартных игр.

---

[1] Литвин А.А. Расследование преступлений, связанных с незаконной организацией азартных игр // Законность. 2010. № 5. С. 60-62.

[2] Тишутина И.В. Цифровые следы в преодолении противодействия расследованию преступлений в сфере экономической деятельности // Цифровой след как объект судебной экспертизы. Мат. Междунар. науч-практ. конф. М.: МГЮУ имени О.Е. Кутафина. 2020. С. 231.

[3] Машинская Н.В. Проблемы выявления и эффективного расследования незаконных организации и проведения азартных игр // Раскрытие и расследование преступлений. // Общество и право 2020 № 3(73) (с. 53-58).

Развитие информационных технологий и современных средств связи позволяет злоумышленникам дистанционно руководить игровым процессом, а также осуществлять контроль за работниками игорного заведения. Зачастую организаторы игорной деятельности создают группы в таких сервисах мгновенных сообщений, как WhatsApp, Viber, Telegram, в которые включают всех сотрудников игорного заведения, для мгновенной координации их действий.

Так, например, организатор одного из игорных заведений, осуществлявших деятельность на территории г. Керчи Республики Крым, находясь в г. Владимир, осуществлял контроль и руководство участниками преступной группы посредством сообщений в сервисе мгновенных сообщений Viber, а видеокамеры, установленные внутри игрового зала, были дистанционно выведены на экран его смартфона[1].

В большинстве случаев при проведении судебной компьютерно-технической экспертизы средств связи, используемых для обеспечения доступа к информации информационно-телекоммуникационных сетей[2], экспертам удается получить информацию о подобного рода переписке, даже если она удалена из памяти смартфона.

Осмотр места происшествия, в ходе которого осуществляется изъятие игорного оборудования, средств связи, электронных носителей информации в незаконных игорных заведениях, необходимо проводить с участием специалиста в области компьютерных технологий[3]. Привлечение специалиста обусловлено необходимостью установления и фиксации электронно-цифровых следов, подтверждающих факты проведения азартных игр, осмотра и фиксации установленных компьютерных программ и игровых приложений, фиксации сведений о выходе в сеть Интернет и подключении к игровым серверам, а также получения статистических данных, позволяющих определить размер извлеченного дохода.

Для установления и фиксации следов преступлений в сфере незаконной организации и проведения азартных игр, рекомендуется проводить осмотр и изъятие игорного оборудования, подключенного к сети, во время непосредственного проведения азартных игр. С этой целью, до проведения осмотра необходимо получить схему помещения, расположения игорного оборудования, сети электропитания и предусмотреть возможное

---

[1] Официальный сайт Керченского городского суда Республики Крым. URL: https://kerch--krm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=76 831253 &delo_id=1540006&new=0&text_number=1(дата обращения 14.12.2021).

[2] Приказ Мининформсвязи РФ от 11.12.2006 № 166 «Об утверждении Правил применения средств связи, используемых для обеспечения доступа к информации информационно-телекоммуникационных сетей, передачи сообщений электронной почтой и факсимильных сообщений». [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64994/ 54bdbc1d7dff4a23b8da71f82a156d20636fb2a5/ (дата обращения 16.12.2021).

[3] Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: автореф. дис. ... канд. юрид. наук. – Москва, 2021. – 26 с.

местоположение участников игорного процесса во время проведения осмотра. При планировании тактических комбинаций и определения функций каждого участника следственного действия, необходимо предусмотреть возможность ограничения подвижности присутствующих работников игрового зала и игроков во время проведения осмотра, в целях исключения возможного отключения игрового оборудования от сети электропитания.

Также, вместе с проведением осмотра места происшествия, целесообразно одновременно провести личный досмотр и обыски у всех участников преступной группы, осуществляющих проведение азартных игр. В ходе проведения указанных следственных действий рекомендуется изымать средства подвижной радиотелефонной связи с доступом в сеть Интернет и иные информационно-коммуникационные устройства, включая планшетные компьютеры, которые имеют возможность подключения к сети Интернет[1], для последующего назначения судебной компьютерно-технической экспертизы.

Таким образом, анализируя теоритические исследования и практическое состояние выявления, раскрытия и расследования преступлений в сфере незаконной организации и проведения азартных игр, в том числе с использованием информационно-телекоммуникационных сетей, можем сделать вывод о том, что информационные технологии и преступность в данной сфере развиваются гораздо быстрее, чем нормативно-правовые акты, направленные на борьбу с киберпреступностью. В связи с чем, данное направление работы требует комплексного монографического исследования, с предложением криминалистических рекомендаций противодействия незаконной организации и проведения азартных игр.

Литература

1. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А.В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч.1. – 208 с.
2. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет. автореф. дис. ... канд. юрид. наук. – Москва, 2019. – 25 с.
3. Литвин А.А. Расследование преступлений, связанных с незаконной организацией азартных игр // Законность. 2010. № 5. С. 60-62.
4. Машинская Н.В. Проблемы выявления и эффективного расследования незаконных организации и проведения азартных игр // Раскрытие и расследование преступлений. // Общество и право 2020 № 3(73) (с. 53-58).
5. Официальный сайт Керченского городского суда Республики Крым. URL: https://kerch--krm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_

[1] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет. автореф. дис. ... канд. юрид. наук. – Москва, 2019. – 25 с.

op=doc&number=76 831253 &delo_id=1540006&new=0&text_number=1 (дата обращения 14.12.2021).
6. Официальный сайт МВД России. URL: https: //xn-b1aew.xn-p1ai/reports/item/27024130/ (дата обращения 13.12.2021).
7. Приказ Мининформсвязи РФ от 11.12.2006 № 166 «Об утверждении Правил применения средств связи, используемых для обеспечения доступа к информации информационно-телекоммуникационных сетей, передачи сообщений электронной почтой и факсимильных сообщений». [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64994/ 54bdbc1d7dff4a23b8da 71f82a156d20636fb2a5/ (дата обращения 16.12.2021).
8. Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: автореф. дис. ... канд. юрид. наук. – Москва, 2021. – 26 с.
9. Тишутина И.В. Цифровые следы в преодолении противодействия расследованию преступлений в сфере экономической деятельности // Цифровой след как объект судебной экспертизы. Мат. Междунар. науч-практ. конф. М.: МГЮУ имени О.Е. Кутафина. 2020. С. 231.
10. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 01.07.2021). [Электронный ресурс] // Доступ из справочно-правовой системы «Консультант Плюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_10699/b20820739fab5a2c2645 f2c2dba2d73e9025f6e4/ (дата обращения 11.12.2021).
11. 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/d6fb3580fbd6ef3e662688c02af241894aa7f3a6/ (дата обращения 10.12.2021).

А.А. Житков

Трансформация уголовного права в цифровое пространство

Аннотация. В статье представлен авторский взгляд на актуальную в уголовно-правовой науке проблему. Проанализированы основные тенденции, связанные с цифровизацией уголовного права по наиболее обсуждаемым направлениям, приведены позиции исследователей в этой области. Определены признаки, указывающие на невозможность отнесения искусственного интеллекта к самостоятельному субъекту преступления. Изложена личная позиция автора относительно использования искусственного интеллекта в процессе квалификации преступлений и принятии процессуальных решений.

Ключевые слова: цифровые технологии, уголовное право, квалификация преступлений, искусственный интеллект, цифровизация, субъект преступления.

Преобразующий эффект цифровых и коммуникационных технологий, оказываемый на современное общество, все сильнее привлекает внимание исследователей-правоведов по всему миру. С момента появления рабочих станций для персональных компьютеров в начале 1980-х гг., запуска глобальной сети Интернет в 1991 году до настоящего времени проведено множество исследований в том числе и в области уголовного права, в которых отмечается, что цифровизация является катализатором трансграничной преступной деятельности[1].

С другой стороны, развитие цифровых технологий помогает эффективно противодействовать преступности. Бесспорно, что компьютеризация рабочих мест сотрудников правоохранительных органов, цифровизация различных процессов, автоматизация баз данных положительно влияет на оперативность раскрытия, расследования преступлений и рассмотрения дел в суде. Цифровизация давно вошла и закрепилась в процесс уголовного судопроизводства. При всех «за» и «против» цифрового пространства в уголовном судопроизводстве уйти от него уже невозможно.

В настоящее время в научной среде наметился спор о возможности использования искусственного интеллекта при квалификации деяния, а также в доказывании вины, вынесении приговора или принятии иных процессуальных решений. Другой вектор – это рассмотрение искусственного интеллекта как самостоятельного субъекта преступления.

Ученые признают искусственный интеллект сложной, искусственно созданной программно-аппаратной системой, способной воспринимать и анализировать информацию, а также к самообучению[2]. Достаточно серьезное внимание в юридической науке уделяется вопросу рисков и неопределенностей, связанных с использованием искусственного интеллекта[3]. Отдельные исследователи считают, что уже сейчас искусственный интеллект находится на таком уровне, что в России необходимо принять специальный кодифицированный акт в области робототехники[4].

По нашему мнению, в настоящее время рассмотрение искусственного интеллекта в качестве субъекта преступления может повлечь за собой только негативные последствия, поскольку злоумышленники будут использовать

---

[1] Афанасьев А.Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 32.

[2]Камышанский В.П., Корецкий А.В. Понятие и правовой статус носителя искусственного интеллекта // Власть Закона. 2019. № 1 (37). С. 43.

[3]Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22. № 1. С.102.

[4]Архипов В.В., Наумов В.Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИРАН. 2017. № 6. С.53.

роботов в своих преступных целях, оставаясь при этом безнаказанными. Однако, если физический носитель искусственного интеллекта будет полностью независим от человека в своих действиях и решениях, приобретет способность к осмыслению своего поведения, оценке его возможных последствий, можно будет рассуждать об уголовной ответственности такого субъекта. Но на современном этапе развития техники в этой области, нельзя искусственный интеллект идентифицировать без участия человека, поскольку он не может существовать без участия человека:

Во-первых, по своей сути искусственный интеллект это созданная человеком компьютерная программа, как и его физический носитель.

Во-вторых, в эпоху стремительного развития компьютерной, цифровой техники компьютерная программа «искусственный интеллект» через непродолжительное время может морально устареть, ресурсы памяти ее физического носителя будут исчерпаны, и она потеряет способность к самообразованию. А физический ее носитель также без обслуживания человеком может прийти в физическую негодность. Кроме того, источник энергии (аккумулятор, солнечные батареи, иной источник питания) для обеспечения бесперебойной работы искусственного интеллекта и его физического носителя требует постоянного участия человека. Искусственный интеллект и его физический носитель не способны воспроизводить себе подобные устройства.

В-третьих, искусственный интеллект не обладает разумом, чувствами, эмоциями.

Последние признаки придают физическому лицу свойство субъекта преступления. При этом, говоря о преступлении, мы понимаем его как деяние, то есть волевой и осознанный акт поведения. Машина с искусственным интеллектом такими свойствами не обладает.

Кроме того, в уголовном праве достаточно много оценочных норм, которые требуют в конкретной ситуации принятие нестандартного решения (обоснованный риск, крайняя необходимость, выполнение или невыполнение приказа или распоряжения). Интуиция, «шестое чувство» не свойственно искусственному интеллекту.

На наш взгляд, в настоящее время искусственный интеллект нельзя рассматривать как самостоятельный субъект преступления, так как без участия человека его деятельность невозможна, поэтому ответственность за вред, причиненный искусственным интеллектом, должен нести человек, который создает или использует такие программы. А программа «искусственный интеллект», а также его физический носитель должны оцениваться как орудие или средство преступления.

Возрастание роли информационных технологий и потенциальная возможность их использования в процессе принятия юридически значимых решений, сформировало в юридической науке оживленную полемику относительно того, может ли искусственный интеллект провести правильную квалификацию действий виновного лица и назначить наказание, соответствующее степени общественной опасности содеянного, цели которого, в конечном счете, будут достигнуты.

Исследования в области применения искусственного интеллекта в квалификации преступления проводятся во многих государствах. Так, еще в 1996 г. группой исследователей Московского государственного университета им. М.Ю. Ломоносова была создана компьютерная программа оценки преступлений, совершенных с использованием оружия[1]. Представляется, что разработка таких алгоритмов имеет перспективы в будущем, однако необходимо привлечение передовых специалистов, в области теории и практики уголовного права. Алгоритм квалификации преступления возможно построить по дедуктивному принципу путем ответов на вопросы, которые будут отсекать лишние по содержанию понятия.

Однако, как мы уже замечали, сфера действия уголовного права изобилует оценочными признаками. Коллизии в квалификации деяния при крайней необходимости свидетельствуют о том, что в настоящее время люди сами до конца не определились с ценностными приоритетами, не говоря уже о том, способен ли решить этот вопрос искусственный интеллект.

Не менее важными в контексте настоящего исследования являются вопросы о возможности уголовно-правовой оценки искусственным интеллектом малозначительного деяния, назначения наказания, не связанного с лишением свободы, определении необходимости условного осуждения и т.д.

Представляется, что вопрос о дееспособности и возможности использования искусственного интеллекта в квалификации преступлений неразрывно связаны между собой. Именно возможность осознания искусственным интеллектом своих собственных действий свидетельствует о возможности квалификации им противоправного поведения людей.

Мы согласны с многими исследователями, высказывающими мнение о возможности сосуществования искусственного интеллекта и человеческого усмотрения в процессе принятия решений о квалификации преступления[2].

Бесспорно, что искусственный интеллект может оказывать и оказывает уже огромную помощь должностным лицам в правоохранительной сфере в принятии управленческих, процессуальных решений[3]. При этом, на наш взгляд, принятие таких решений искусственным интеллектом без участия человека в настоящее время невозможно.

Один из принципов уголовного права – это принцип гуманизма. Не раскрывая его содержания, остановимся на термине гуманизм, под которым понимается

---

[1]Иногамова-Хегай Л.В. Квалификация преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке: Материалы XVl Международной научно-практической конференции. М., 2019. С. 54.

[2] Щелконогова Е.В. Уголовное право on-line: теория и практика цифровизации // Технологии XXI века в юриспруденции: Материалы Всероссийской научно-практической конференции / под ред. Д.В. Бахтеева. 2019. С. 178.

[3]Нагорных, Р. В. Проблемы модернизации кадрового обеспечения деятельности уголовно-исполнительной системы в условиях становления доктрины административного конституционализма в современной России / Р. В. Нагорных, Я. В. Васильева, Н. А. Мельникова // Пенитенциарная наука. – 2021. – Т. 15. – № 4(56). – С. 791-801.

мировоззрение, в центре которого находится идея человека как высшей ценности, то есть человеколюбие.

Снисхождение, те есть великодушное, не слишком строгое отношение к промахам, ошибкам, к вине или сострадание к лицу, совершившему преступление в силу стечения тяжелых жизненных обстоятельств, все это проявление гуманности, находит свое отражение в уголовном судопроизводстве, но не свойственно искусственному интеллекту. Вряд ли человек сможет придать эти свойства искусственному интеллекту. Искусственный интеллект может их только имитировать, но это не будет основано на чувствах, переживаниях, эмоциях.

Таким образом, рассмотрев некоторые аспекты возможного применения цифровизации в юриспруденции, важно отметить, данное явление оценивается представителями различных сфер либо как негативное явление, либо активно приветствуется. Юриспруденция и отрасль уголовного права с одной стороны также воспринимают внедрение в их сферу компьютерных технологий, с другой стороны призваны регулировать и ставить под охрану законные правоотношения в этой области, такие как интеллектуальные права в Интернете, киберпреступность и др. Цифровизация вызывает опасения в связи с тем, что компьютер в конечном счете заменит человека. Представляется, что на современном этапе невозможно применение искусственного интеллекта в тех сферах, где требуется проявление творческой активности, свойственной поведению человека. Это напрямую связано с правоохранительной деятельностью в сфере уголовного судопроизводства, а именно квалификация деяний, вынесение приговора или принятие иных процессуальных решений.

П.А. Зобнин

Специфика расследования преступлений против личности, совершенных с использованием компьютерных, коммуникационных и высоких технологий

Аннотация. С развитием технологий более изощренными стали и способы совершения преступлений. Технический прогресс не обошел стороной и преступления, против личности, обладающие наиболее высокой общественной опасностью. Данная статья раскрывает специфику и проблематику расследования преступлений, совершенных с использованием компьютерных, коммуникационных и высоких технологий.

Ключевые слова: технологии; расследование преступлений против личности; расследование преступлений; процессуальная проверка.

По данным ГИАЦ МВД России в 2017 году в производстве правоохранительных органов находилось более 100 000 уголовных дел о преступлениях, совершенных с использованием информационно-коммуникационных технологий, и с каждым годом данная цифра неуклонно растет. Однако, следует отметить, что в данную статистику входит всего десять

составов преступлений, все из которых это преступления в сфере экономики, либо в сфере компьютерной информации. Так, в статистику не включен ни один состав преступления против личности, которые в настоящее время все чаще и чаще совершаются с использованием компьютерных технологий.

Данная ситуация возникла в связи с традиционным пониманием преступлений против личности, ведь принято считать, что данные преступления совершаются непосредственно при физическом контакте с потерпевшим. Однако на фоне развития информационных и компьютерных технологий данное понимание ошибочно.

С появлением и последующим распространением технологий, способы совершения преступлений против личности становились все более и более изощренными, а вместе с тем, становилось сложнее расследование данной категории преступлений, в связи с необходимостью подготовки кадров, направленной на расширение знаний в области компьютерных, коммуникационных и высоких технологий.

Еще на стадии процессуальной проверки, необходимо рассмотреть вопрос о совершении преступления посредством компьютерных, коммуникационных или высоких технологий. Так, при рассмотрении вопроса о возбуждении уголовного дела по признакам преступления, предусмотренного ст. 110 УК РФ, необходимо исключить не только физическое воздействие на потерпевшего путем прямого высказывания угроз, жестокого обращения и унижения, а также совершения вышеуказанных действий с помощью информационно-коммуникационной сети «Интернет» или создания психотравмирующей ситуации потерпевшему посредством компьютерных и высоких технологий.

Необходимость установления возможного использования компьютерных, коммуникационных или высоких технологий характерна и для таких составов преступления, как угроза убийством, клевета, понуждение к действиям сексуального характера, развратные действия и другие. Однако, установление фактов использования компьютерных и иных технологий существенно затягивает процесс процессуальной проверки, в связи с чем могут остаться без внимания органов предварительного расследования.

Сложность расследования преступлений против личности, совершенных с использованием компьютерных, коммуникационных или высоких технологий, также заключается в анонимности и труднодоступности лиц, причастных к совершению противоправного деяния, что, в свою очередь порождает другую проблему – определения места совершения преступления, а с ним и места расследования. Ведь место совершения преступления, и место наступления общественно-опасных последствий, могут отделяться тысячами километров, и находится в разных государствах, что делает производство необходимых следственных действий практически невозможным, без взаимных усилий нескольких государств.

Примером слаженного взаимодействия нескольких государств в целях раскрытия преступления можно считать прекращение работы сети обмена детской порнографии путем информационно-коммуникационной сети «Интернет»: в 1998 году путем взаимодействия правоохранительных органов 12

стран, был приостановлен международный обмен детской порнографией в информационно-коммуникационной сети «Интернет», которая имела название «Wonderland Club». Было арестовано 107 человек, среди которых были граждане разных европейских стран и изъято около 750 000 порнографических материалов.

Однако, несмотря на то, что установление места совершения преступления значительно усложняется, определение времени в случае использования технологий наоборот становится значительно проще, нежели при установлении времени исходя из субъективных представлений участников уголовного судопроизводства и восстановления хронологии событий исключительно по памяти.

Кроме того, говоря о расследовании преступлений, совершенных с применением компьютерных и иных технологий, необходимо отметить специфику проведения следственных действий. Так, если в ходе проведения процессуальной проверки или предварительного расследования по преступлениям против личности, будет установлено, что предметом, способом или средством являлись компьютерные, коммуникационные или высокие технологии, необходимо незамедлительное проведение определенных следственных действий, таких как осмотр места происшествия, обыск или выемка. Срочность в данном случае обусловлена наличием специальных программ, имеющих возможность безвозвратного удаления информации, представляющей интерес для следствия, ее искажения или утраты путем физического воздействия на носитель.

Кроме того, при проведении указанных следственных действий имеется необходимость в участии специалиста, обладающего знаниями по поиску, закреплению, переносу и сохранению информации, которая при неверном изъятии может быть безвозвратно утрачена. Однако участие специалиста не освобождает уполномоченное лицо, ведущее расследование, от развития его компетенций в области компьютерных, коммуникационных и высоких технологий, в ином случае, даже при надлежащем сохранении информации, она не будет надлежащим образом осмотрена и признана в качестве доказательств, а также при отсутствии специалиста, например в сельской местности, следователь или дознаватель должен обладать достаточными знаниями для самостоятельного изъятия и сохранения компьютерной информации и последующего его использования в качестве доказательств.

Неэффективное сохранение информации, имеющей значение для следствия, а также дальнейшие проблемы в осмотре и использовании указанной информации в качестве доказательств, возможно обусловлено недостаточной технической оснащенностью органов предварительного расследования, особенно данная ситуация может быть характерна в условиях крайнего севера и отдаленности некоторых населенных пунктов от региональных центров. Использование некачественных служебных компьютеров, отсутствие физических носителей большого объема информации, отсутствие качественного программного обеспечения, все это также может сказаться на расследовании указанных преступлений.

Таким образом, особенности расследования преступлений против личности, совершенных с использованием компьютерных, коммуникационных и высоких технологий требует разработки определенной единой методики, с которой в обязательном порядке должны знакомиться не только следователи и дознаватели, специализирующиеся на преступлениях в сфере компьютерных технологий, но и лица, занимающиеся расследованиями иных категорий преступлений, в том числе преступлений против личности.

Также, помимо разработки методики, следует рассмотреть вопросы о возможном создании отдельного экспертного органа, призванного оказывать содействие органам предварительного расследования при производстве следственных действий по преступлениям, совершенным с использованиям компьютерных, коммуникационных и высоких технологий, а также о непосредственном повышении квалификации сотрудников правоохранительных органов в обрасти компьютерных и иных технологий, и об улучшении технического оснащения органов предварительного расследования.

Литература

1. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации Генеральной прокуратуры Российской Федеральной. 2014 год.
2. Берестнев В.Н., Васюков В.Ф. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий». 2019. С. 6-7.
3. Волеводз А.Г. Противодействие компьютерным преступлениям. 2002. С.34-35.
4. Колиев В.В., Шахкелдов Ф.Г. Методика раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий. 2021.
5. Смолин А.В., Зайцев А.А. Тактика производства отдельных следственных действий по преступлениям, совершенных с применением компьютерной техники. 2019. С. 2-5.

Н.В. Золотухина, П.Н. Жукова

Возможность использования информации, полученной из открытых источников в качестве доказательств в уголовном процессе

Аннотация. Рассматриваются вопросы применимости полученной информации в открытых источниках сети Интернет в качестве доказательств по уголовному делу (в рамках расследования по уголовному делу).

Ключевые слова: информационные ресурсы, открытые данные, расследование, доказательство.

Развитие информационных ресурсов привело к тому, что в открытых источниках информация, в частности в сети Интернет, достаточно разрознена, и, на первый взгляд, ее элементы никак не связаны между собой. Данная ситуация позволяет получить разнородную информацию о юридических либо физических лицах, несмотря на то, что связи между объектами и происходящими с ними событиями неустойчивы. Достоверность результата поиска информации по заданным критериям достигается за счет необходимости обработки значительных объемов информации, сопровождающейся временными издержками. В результате поэтапного анализа собранной информации происходит исключение возникающих возможных недостатков проведенного поиска.

Таким образом, открытая информация, размещенная в сети Интернет, является первоисточником при сборе сведений на физических либо юридических лиц.

Потребность поиска и анализа информации породила такие понятия как OSINT[1] (разведка на основе открытых источников данных, т.е. разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также проведение её анализа), BIGDATA (набор специальных методов и инструментов, которые используются для хранения и обработки огромных объемов данных для решения конкретных задач, данные могут быть как структурированными, так и неструктурированными), LOGGER (специализированные IP-логгеры или Geo-логгеры позволяют устанавливать электронно-цифровые следы пользователей сети. Логирование пользователя в Интернет - специально созданные, гиперссылка или файл, запускающий при своем открытии специальные алгоритмы сбора пользовательских данных при переходе пользователя (в той или иной форме) на внешний веб-ресурс, доступ к логу которого имеется у исследователя. Большое число сервисов, предлагающих подобный функционал, находится в общем доступе. Сбор данных о местоположении происходит при помощи технологий: GPS (спутниковое геопозиционирование), LBS (позиционирование по базовым станциям мобильной связи), WiFi (позиционирования по месту размещения WiFi-роутера), а также по IP-адресу), SERVICE (использование специального программного обеспечения, позволяющего автоматизировать часть поисковой работы) - поиск, сбор и анализ полученной из общедоступных источников информации.

Указанные понятия затрагивают область получения информации с различных сайтов, государственных ресурсов, социальных сетей, форумов и различных приложений для обмена фотографиями и видеозаписями с элементами социальной сети, позволяющее общаться в режиме онлайн/офлайн.

Большинство пользователей открыто выкладывают личную информацию, вступают и формируют виртуальные социальные группы, образующие сеть связей, указывают свои интересы и предпочтения, размещают материалы, содержащие геолокационные данные, по которым предоставляется возможность

[1] Open Source INTelligence.

отслеживания географии перемещения во времени. Перечисленная выше информация предоставляет возможность отследить взаимодействия и установить связи между различными группами лиц.

При рассмотрении OSINT, как процесса, в ходе которого производится выявление, выбор, сбор и анализ информации, находящейся в свободном доступе, необходимо помнить, что открытыми источниками для разведки используются:

- СМИ – публикации в различных изданиях;
- облачное хранилище Интернет, в частности, веб-сообщества и контент, созданный пользователями – социальные сети, видеохостинги, вики-справочники, блоги, веб-форумы и т.д.;
- публичные отчёты правительства, официальные данные о демографии, материалы пресс-конференций, различные публичные заявления;
- наблюдения - радиомониторинг, использование общедоступных данных дистанционного зондирования земли и аэрофотосъемок (например, Google Earth) и т.д.;
- профессиональные и академические отчёты, конференции, доклады, статьи, включая ту литературу, которая относится к «серой».

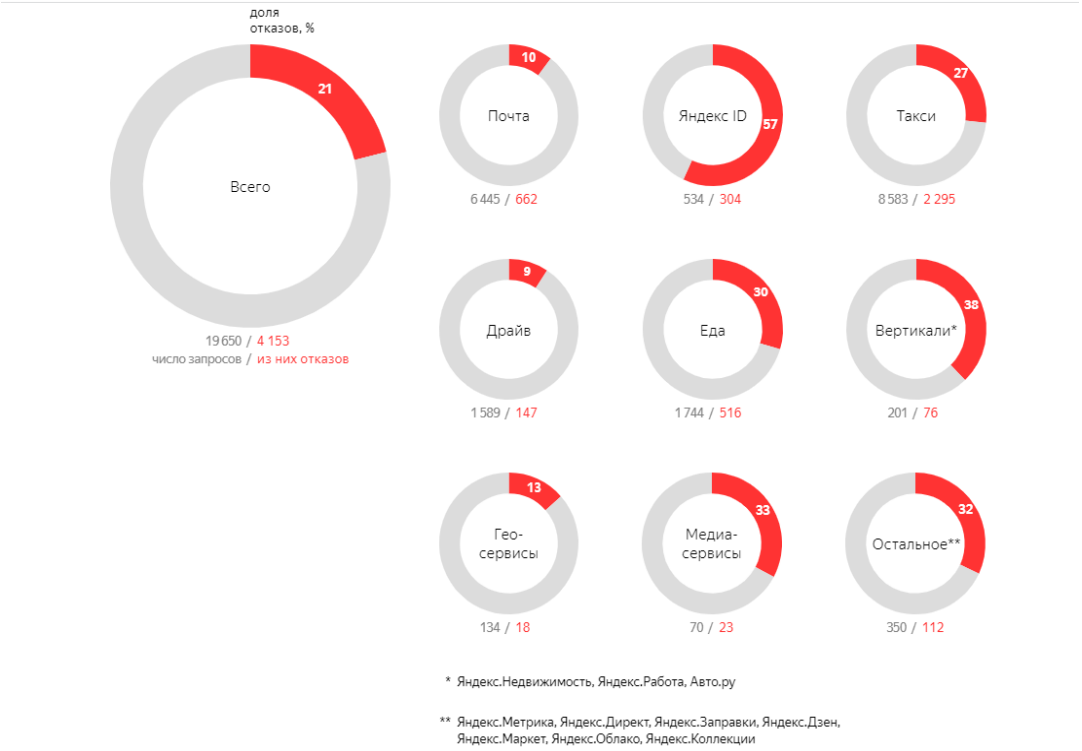
На первоначальном этапе сбора информации в сети интернет о человеке, как правило, происходит поиск известных данных, учетных записей социальных сетей, знакомых лиц из круга общения, адресов электронной почты, абонентских номеров, фотографий и т.д. На этапе обработки полученных данных извлекаются метаданные, восстанавливаются сведения о ранее удаленной информации, устанавливаются новые связи с людьми, и прочие мероприятия, при этом эффективность использования структурированного подхода зависит от объема имеющихся данных.

Вопрос о возможности использования полученных данных в доказывании не вызывает сомнения, но, чаще всего они предоставляются сотрудниками, уполномоченными на осуществление оперативно-разыскной деятельности и находят свое отражение в виде краткой информации в рапорте.

Указанные данные может беспрепятственно получать и следователь, осуществляя свою деятельность по расследованию преступления, но он ограничен перечнем доказательств, предусмотренным УПК РФ. Как показала практика и интервьюирование сотрудников следственных подразделений, для фиксации полученных данных, чаще всего проводится следственный осмотр, в ходе которого осматривается и фиксируется контент интернет страниц и метаданные, характеризующие исследуемый объект.

Кроме проведения осмотра, в рамках предварительного расследования, используется составление запросов на основании статьи 10.1. «Обязанности организатора распространения информации в сети Интернет» Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Ниже приведено количество запросов к Яндексу, касающихся раскрытия пользовательских данных. Отчёт[1] не включает в себя сведения о предоставлении информации правоохранительным органам, предусмотренном ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ.



Порядок направления запроса, его содержание и форма чётко регламентированы в УПК РФ только в главе 53 «Основные положения о порядке взаимодействия судов, прокуроров, следователей и органов дознания с соответствующими компетентными органами и должностными лицами иностранных государств, и международными организациями». В связи с этим международные запросы не вызывают ни практических, ни теоретических вопросов.

В соответствии с ч.1 ст. 144 УПК РФ следователь (дознаватель) в ходе осуществления доследственной проверки вправе истребовать документы и предметы. Порядок их истребования законодательно не закреплён, следователь направляет личный запрос об истребовании конкретных документов, предметов или сведений, или поручает эти действия органу дознания в установленном законом порядке.

Определять круг сведений, подлежащих истребованию как при проверке сообщения о преступлении, так и в ходе осуществления предварительного расследования нецелесообразно. Эти документы, предметы и сведения могут быть истребованы с целью установления обстоятельств, подлежащих доказыванию по уголовному делу. Запросы оформляются по правилам ведения

[1] Открытый отчет компании Яндекс о запросах государственных органов, касающиеся пользовательских данных https://yandex.ru/company/privacy/transparencyreport.

служебной переписки, их форма и содержание императивно уголовно-процессуальным законодательством не определены.

Факт направления мотивированного запроса государственным и муниципальным органам, предприятиям, учреждениям, организациям, должностным лицам и гражданам об истребовании документов, предметов и сведений возлагает на них обязанность по его исполнению в соответствии с ч. 4 ст. 21 УПК РФ. В процессуальной деятельности запрос реализует двоякую функцию – во-первых, является обязательным основанием для направления соответствующему должностному лицу истребуемых документов, предметов и сведений, во-вторых, подтверждает законный способ получения результатов, представленных учреждениями, предприятиями, организациями, должностными лицами и гражданами. Например, с целью изучения обстоятельств, характеризующих личность обвиняемого, подлежащих обязательному доказыванию по уголовному делу, следователем направляются запросы по месту жительства, по месту работы (учёбы) обвиняемого, в психиатрический и наркологический диспансеры, в которых излагаются мотивы данных обращений, а именно факт возбужденного уголовного дела и необходимость получения запрашиваемой информации с целью всестороннего его расследования. В ответ на полученный запрос соответствующие организации и должностные лица направляют документы, которые по сути являются источниками доказательств.

Таким образом, обязательным для предоставления ответа является запрос, оформленный в соответствии с требованиями законодательства.

В случае бумажного носителя необходимо чтобы он был оформлен на официальном бланке ведомства, содержать контакты и собственноручную подпись уполномоченного лица, а в ряде случаев должен быть заверен оригинальным оттиском печати. Запрос в электронной форме считается обязательным для предоставления ответа только в том случае, если он заверен усиленной квалифицированной электронной подписью. Ответы на запросы предоставляются только по официальным каналам связи. Электронная почта к ним не относится, как и телефон или мессенджер.

Литература

1. Золотухина Н.В., Жукова П.Н. Проблемные вопросы собирания доказательств по уголовному делу // Вестник Волгоградской академии МВД России. 2019. № 2 (49). С. 94-100.
2. Золотухина Н.В., Жукова П.Н., Горкина Е.В. Виды процессуальных документов в следственных органах // Вестник Волгоградской академии МВД России. 2021. № 2 (57). С. 108-118.

М.А. Иващенко

Искусственный интеллект в бизнесе

Аннотация. В тексте настоящей статьи обращается внимание на место искусственного интеллекта в бизнесе. Выделены отдельные проблемы, которые можно решить с помощью алгоритмов машинного обучения. Приведены практические примеры того, как используются технологии искусственного интеллекта в бизнесе. Обращено внимание на уже разработанные и действующие платформы искусственного интеллекта, применяемые в бизнесе.

Ключевые слова: искусственный интеллект, бизнес, робототехника, IT-технологии, инвестиции.

Технологии ИИ могут использоваться для достижения самых разных целей, в том числе в процессе выработки и принятия государственными должностными лицами и государственными служащими управленческих решений. Так, задействование технологий ИИ в государственном управлении может осуществляться посредством передачи системе ИИ определённых задач для того, чтобы орган государственного управления (должностное лицо, принимающее или реализующее решение) мог иметь возможность выйти за рамки устоявшихся систем обеспечения принятия решений. ИИ применяют в различных областях, в том числе в бизнесе[1].

В настоящее время разработано и применяется множество различных программ, в том числе для электронных вычислительных машин и баз данных. Проанализировав их сущность, можно прийти к выводу, что все они сведены к упрощённому пониманию и решению, помимо иных, экономических и социальных проблем. В частности, речь идёт о проникновении роботизированной техники в нашу жизнь.

ИИ способен быстро вывести бизнес на принципиально новый уровень, это одна из его ключевых функций и задач. Выделяется несколько проблем, которые можно решить с помощью алгоритмов машинного обучения:

1) Оперативное реагирование. В некоторых сферах бизнеса принципиальное условие успеха – быстро анализировать поступающие данные и моментально на них реагировать – например, в биржевых операциях. В отличие от обычных алгоритмов, которые не способны без предварительного обучения самостоятельно адаптироваться к новым условиям и данным, искусственный интеллект обеспечивает такую возможность.

2) Разработка маркетинговой стратегии на основе предоставленных данных и заложенных целей. ИИ помогает в работе маркетолога: не только анализирует опыт предыдущих продаж, но и использует прогнозирование для «предсказания» будущих, а также учитывает поведение конкурентов и общую ситуацию на рынке.

[1] Роль искусственного интеллекта в бизнесе. URL: https://www.simbirsoft.com/blog/rol-iskusstvennogo-intellekta-v-biznese/ (Дата обращения: 05.01.2021).

3) Человеческий фактор. Даже у самого профессионального и опытного сотрудника бывают неудачный день и неверные решения. У ИИ – нет, вместо эмоций у него функции, а технология и информация заменяют переменчивое настроение.

4) Борьба с мошенничеством. Самообучающиеся нейронные сети помогают анализировать поведение пользователей и выявлять подозрительные операции, а также создавать алгоритмы для предотвращения финансовых потерь. Результат: система становится менее уязвимой, а это ключевое условие доверия клиентов.

5) Увеличение прибыли. Использование машинного обучения в одной только системе ценообразования способно обеспечить прирост выручки на 5%, а при условии комплексного подхода доходы компании могут вырасти в несколько раз.

Правовое регулирование робототехники в Российской Федерации на сегодняшний день проявилось в следующем: 1) внесение изменений в Воздушный кодекс РФ[1], которые связаны с правовым регулированием беспилотных воздушных судов и авиационных систем (дронов); 2) в Стратегии развития автомобильной промышленности Российской Федерации на период до 2020 г.[2], а также в программе «Цифровая экономика Российской Федерации»[3] упоминается о робототехнике. Более того, в декабре 2016 г. юридическая фирма Dentons по заказу Grishin Roboticks разработала концепцию первого в России законопроекта о робототехнике, представленного в виде внесения поправок в Гражданский кодекс Российской Федерации[4], а 22.11.2017 исследовательским центром проблем регулирования робототехники и искусственного интеллекта была представлена Модельная конвенция о робототехнике и искусственном интеллекте[5].

Число компаний, занимающихся ИИ в мире быстро растет. Так, их количество выросло в пять раз с 2015 по 2018 год и составило 3465, в США — 1393. Наибольшее количество таких компаний в 2017 г. зарегистрировано в США — 2905[6]. Большинство компаний, работающих на рынке ИИ, вкладывают средства

---

[1] Федеральный закон от 30 декабря 2015 г. № 462-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации в части использования беспилотных воздушных судов» // СПС «КонсультантПлюс».

[2] Приказ Министерства промышленной торговли России от 23 апреля 2010 г. № 319 «Об утверждении Стратегии развития автомобильной промышленности Российской Федерации на период до 2020 года» // СПС «КонсультантПлюс».

[3] Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

[4] Федорина А.А. К вопросу о правовом статусе робототехники и искусственного интеллекта // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 4. С. 4.

[5] Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта: версия 1:0, ноябрь 2017 г. Текст на русском языке см.: URL: http://robopravo.rU/uploads/s/z/6/g/z6gj0wkwhv1o/file/6dbrNqgu.pdf (дата обращения: 25.12.2020).

[6] Как искусственный интеллект используется в бизнесе: обзор и кейсы. URL: https://vc.ru/marketing/105102-kak-iskusstvennyy-intellekt-ispolzuetsya-v-biznese-obzor-i-keysy (Дата обращения: 11.01.2021).

в разработку приложений для машинного обучения. По последним подсчетам $31,7 миллиарда инвестированы именно в эту категорию[1].

Важно отметить, что в настоящее время работа ИИ в бизнесе строится на так называемых программных платформах. Программные платформы ИИ предлагают пользователям набор инструментов для создания интеллектуальных приложений. При помощи ИИ-платформ становится возможно применять технологии машинного обучения, машинного зрения, обработки текста и прочие.

Чтобы претендовать на включение в категорию ИИ-платформ, программный продукт должен:

1) обеспечивать возможность построения интеллектуальных приложений с поддержкой ИИ;

2) позволять пользователям создавать алгоритмы машинного обучения или предлагать готовые алгоритмы для создания приложений;

3) предоставлять разработчику возможность подключать к собственным алгоритмам источники данных для обеспечения машинного обучения и адаптации производительности.

В научной литературе отмечается, что адаптация ИИ под нужды бизнеса находится в зачаточном состоянии. Наблюдаются только «пилоты» таких проектов или маркетинговые «игрушки», призванные, скорее привлечь внимание к деятельности компании, чем принести реальную пользу.

Большинство примеров использования технологий ИИ в бизнесе сегодня приходят из сферы маркетинга и клиентского сервиса. Роботы и алгоритмы на основе машинного обучения выполняют функции рекомендаций, социального и маркетингового анализа, ретаргетинга, мерчендайзинговой оптимизации.

Одна из топовых розничных сетей США — Macy’s — на базе сервисов Watson от IBM разработала виртуального советника для своих клиентов. Приложение делает трекинг покупок и на основе этой истории выдает рекомендации. Например, система сразу отсечет дорогие бренды из выдачи для человека, ранее интересовавшегося лишь «эконом-классом» товаров из данной категории.

О перспективах ИИ для бизнеса можно судить по объемам инвестиций, которые вливают в исследования и разработку подобных технологий. В 2017 г. компании, специализирующиеся на технологиях ИИ получили от инвесторов более 10,8 миллиардов долларов[2].

Согласно опросу Teradata, 80% коммерческих организаций или уже используют отдельные решения на основе ИИ или собираются это сделать в ближайшее время. Компании планируют получить 123 доллара ROI на каждый вложенный доллар в проект ИИ в течение последующих трех лет. Хотя 91% респондентов отметили существенные сложности с внедрением технологий ИИ: отсутствие подходящей ИТ-инфраструктуры и дефицит специалистов в этой области.

---

[1] Там же.

[2] Искусственный интеллект для бизнеса: ожидание и реальность // URL: https://geoline-tech.com/ai-for-business/ (Дата обращения: 13.01.2021).

В Gartner утверждали, что технологии ИИ к 2020 году будут присутствовать почти во всех программных продуктах и сервисах, а лидеры рынка смогут получать за счет их использования до 30% дополнительной прибыли.

Далее рассмотрим простые примеры того, как используются технологии ИИ в бизнесе. В первую очередь обратим внимание на предприятия, которые работают с продуктами питания, соответственно они должны следить за их сроком годности и своевременно проводить списание. Например, в булочных и пекарнях срок реализации – всего один день, до 30% хлебобулочной продукции ежедневно списывают. Следовательно, главной задачей такого предприятия будет сокращение убытков, но при этом не затрагивая ассортимент. Для решения данной задачи, при использовании технологий ИИ, возможно спрогнозировать спрос на ближайшие 3-4 дня, при этом точность предсказания составляет 90 %[1]. Для этого требуется проанализировать данные из 1С за последние два года и обучить алгоритм. Благодаря прогнозу, сети удаётся оптимизировать работу цеха, снизив объем списываемой продукции (например, выпечки) до 15% и не потеряв при этом в ассортименте.

Во-вторых, на примере работы сети супермаркетов рассмотрим следующее. Так, например, в магазинах была введена система лояльности (карты постоянного клиента) и действовали специальные скидки в «счастливые часы», но эффективность этих акций никак не измерялась, а прибыль увеличилась незначительно. Решение: силами самообучающейся программы надо проанализировать историю покупок клиентов с картой лояльности и, использовав данные за несколько лет, подобрать для каждого из них оптимальную систему поощрений. Если покупатель не интересовался акциями и скидками, ИИ вышлет ему другие оповещения, например, описание ассортимента или даты поступления в продажу любимых товаров. Покупателей, которые интересовались акцией «счастливые часы», компьютер будет информировать о выгодных предложениях и о том, когда начнется следующая акция. Также в магазине использовали такую функцию программы, как отправка персонализированных смс. Результат: своевременная информация повысила лояльность покупателей, повторное обращение клиентов увеличилось на 80%, выросла прибыль[2].

Известно, что российский рынок больших данных уступает своим масштабом западному, но 55,4% отечественных компаний уже начали инвестировать в аналитику Big Data[3]. Нам известны неоднократные примеры успешной попытки соединять большие данные с бизнесом в России. На примере ПАО «Сбербанк России» отметим, что к концу 2020 г. банком прогнозировалось о выдаче кредитов системами ИИ. Для этого он должен будет сопоставить биометрические данные клиента, кредитную историю, доходы, затраты и после этого самостоятельно будет принимать решение. В настоящий момент не

[1] Роль искусственного интеллекта в бизнесе. URL: https://www.simbirsoft.com/blog/rol-iskusstvennogo-intellekta-v-biznese/ (Дата обращения: 05.01.2021).
[2] Там же.
[3] Там же.

известно, реализовался данный прогноз или нет, но попытки предприняты были. В приложении «Сбербанк Онлайн», предпочтения 50 миллионов пользователей будут анализировать по 1000 параметрам и сформируют пакет услуг и информации специально для этого пользователя — частые переводы и платежи, статистика трат. А также предварительное собеседование с кандидатами на массовые вакансии уже сейчас проводит робот, который задает вопросы в зависимости от ситуации и, если кандидат соответствует требованиям, переключает беседу на человека — сотрудника HR-службы.

Кроме того, в России технологии искусственного интеллекта уже внедрили: ПАО «Банк УРАЛСИБ» (анализ данных клиентов), МТС и «М.Видео» (оптимизация клиентского сервиса с выдачей персональных рекомендаций), «Альфа Страхование» (определение риска мошенничества при страховом случае), Aviasales и некоторые другие, в том числе промышленные предприятия.

ИИ напрямую соотносится с Data Science – наукой о данных, которая направлена на извлечение бизнес-ценности из массива информации. Эта ценность может заключаться, например, в расширении возможностей прогнозирования, знании о закономерностях, обоснованном принятии решений.

Некоторыми исследователями данного вопроса отмечается, что знакомство с технологиями ИИ в бизнесе можно начать с уже разработанных и действующих платформ. Перечисленные ниже платформы позволяют понять, чем же ИИ может быть полезен для бизнеса.

1) «HANA» от SAP – облачная платформа, которую можно запустить также на внутренних серверах организации. Используется для управления базой данных компании, собирает информацию с различных источников (стационарные или мобильные рабочие станции, финансовые транзакции, сенсоры и производственное оборудование). Инструменты аналитики позволяют выявлять тренды и нарушения для оптимизации отдельных процессов.

2) «DOMO» (быстрорастущая технологическая компания) выпустила на рынок дашборд под своим брендом, который помогает компаниям собирать информацию для принятия более точных и выгодных решений. Система может собирать данные со сторонних приложений (клиентские сервисы, социальные сети) и настраивать стратегию продаж или инвестиций.

3) «eSales» от Apptus помогает настраивать каналы продаж, автоматизировать складские запасы, предсказывая на базе собранной информации поведение покупателей. Программа использует Big Data и алгоритмы машинного обучения для определения, какие продукты компании будут востребованы в ближайшем будущем на основе истории продаж, выдавать персональные рекомендации клиентам.

4) «Avanade» – совместный продукт Microsoft и Accenture, тоже, по сути, предназначенный для прогностической аналитики, когда на основе исторического поведения клиентов выдаются рекомендации по тонкой настройке клиентского сервиса.

5) «Predix» – фактически полноценная операционная система от General Electrics, предназначенная для использования на сложных технологических производствах. Она собирает данные с датчиков оборудования, анализирует их,

просчитывая вероятность его поломки или остановки. Подобная аналитика помогает сэкономить средства на сервисное обслуживание.

6) «MindSphere» – открытая облачная платформа от Siemens (бета-версия была выпущена в 2016 году). Предназначена для мониторинга парка оборудования на предприятии для сервисных нужд. Анализирует производительность машин в зависимости от множества факторов, выдает рекомендации по оптимизации его работы.

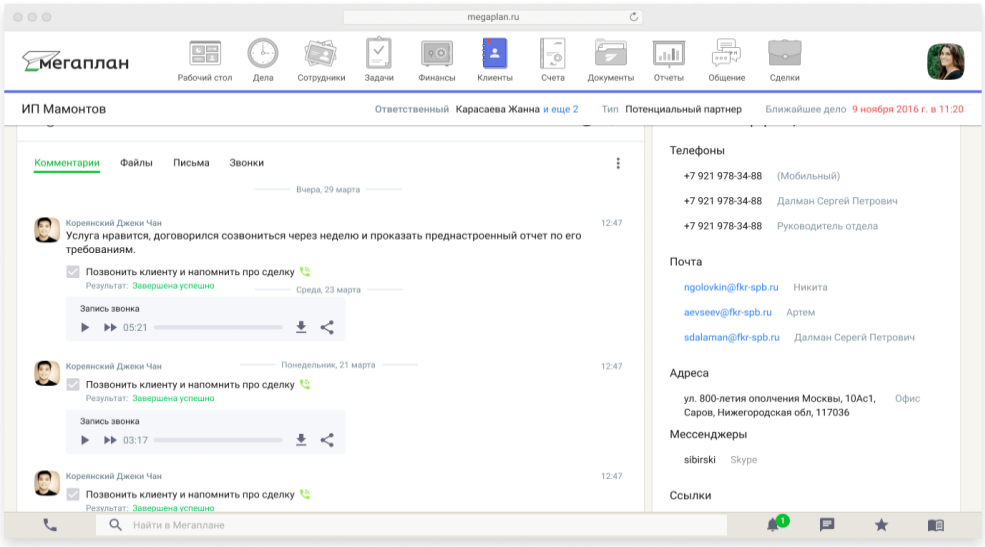
IT-технологии развились до такой степени, что разработки стали финансово доступны малым и средним компаниям. Особенно большой интерес мы наблюдаем к облачным CRM-системам.

Термин CRM в переводе с английского означает управление отношениями с покупателями. По сути это выстраивание долгосрочных связей с клиентской базой для поддержания лояльности и стимулирования к повторным покупкам. Например, у вас магазин инвентаря фехтования и вы поддерживаете связь с клиентами, чтобы вместе что называется «расти в спорте». Сначала продаете ему экипировку и оружие для начинающих, потом для профессионального спорта и показательных выступлений. Чтобы стимулировать покупки и исключить уход к конкурентам, вы регулярно напоминаете о себе, объясняете особенности этого вида спорта, поздравляете с праздниками, даёте скидки. Это и есть профессиональный CRM-подход к продажам.

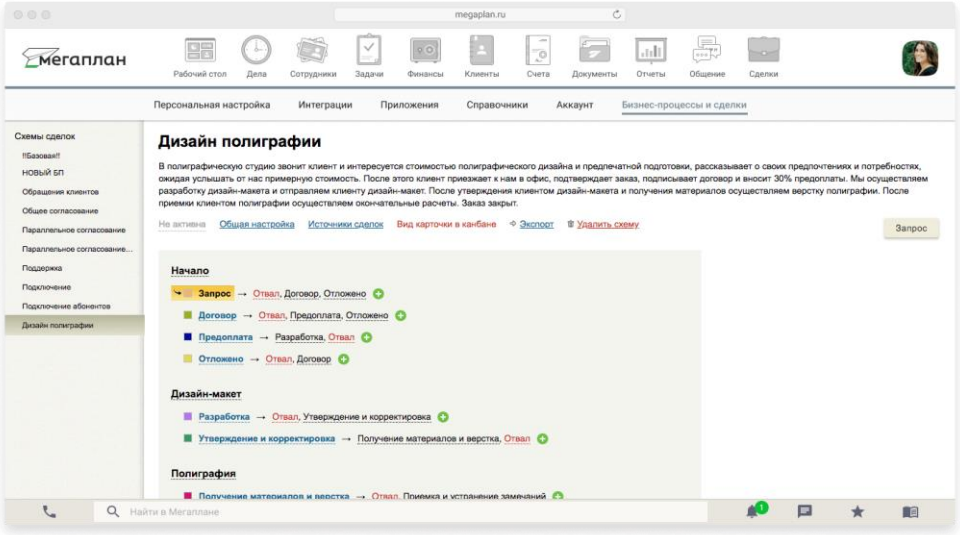
Бизнесу нужен инструмент, который позволит реализовать такую клиентскую стратегию: напомнит о звонке, сделает рассылку, сохранит историю заказов. Именно для этого приобретают CRM для продаж. Автоматизируя основные процессы, CRM помогает «находиться с клиентами на одной волне», получать от них больше заказов и свести на нет ошибки в общении[1].

Как это выглядит в реальности? У каждого клиента есть своя карточка. В ней находятся вся контактная информация и накапливается история заказов. За каждым клиентом закреплен ответственный менеджер. Интеграция с телефонией и электронной почте экономит рабочее время. Менеджер может наметить звонок клиенту, в намеченное время позвонить и тут же отписаться о результатах. По итогам разговорам сформировать из шаблона коммерческое предложение и опять же из карточки отправить на e-mail клиента. Все действия будут зафиксированы, запись разговора и черновик письма сохранятся.

[1] Иващенко М. А. Искусственный интеллект в управлении следственными органами / М. А. Иващенко, С. С. Бурынин. – Москва: Московская академия Следственного комитета Российской Федерации, 2021. С. 44.



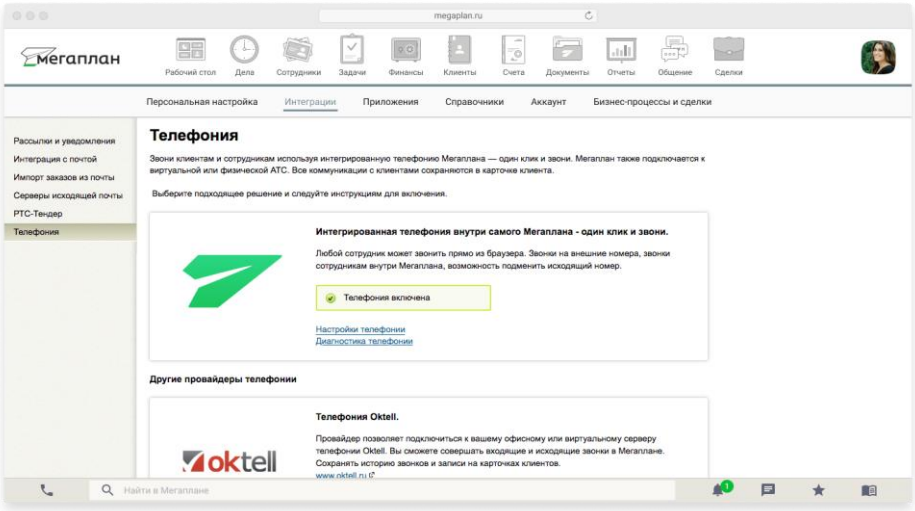
Разработчики ежедневно расширяют возможности CRM-продуктов: добавляют интерактив, игровые элементы, встраивают нетипичный функционал. Если раньше CRM ассоциировалась только с продажами, сегодня она может автоматизировать вообще любой бизнес-процесс.



Несмотря на разнообразное наполнение CRM, в ней должны присутствовать обязательные разделы (модули). К примеру, такие:

- учёт клиентов (единый список, отдельные карточки, журнал с историей);
- учёт сделок (список, отдельные карточки со статусом, сумма счёта);
- воронка продаж и другие отчёты (о результатах менеджеров, прибыли за период, данных по новым людям и др.).

Это три базовые возможности классической программы для автоматизации продаж. Важно, чтобы работала и была настроена интеграция с вашей почтой и АТС. Отлично, если облачная телефония уже встроена.



По данным англоязычного интернет-портала Venture Beat за 2015 год, компании, внедрившие в маркетинг CRM-автоматизацию, на 80% повысили лидогенерацию[1] и на 77% увеличили конверсию[2].

Возникает закономерный вопрос: «сможет ли менеджер самостоятельно выставить счет из CRM?». Да, но если нет, программный модуль API должен быть настолько гибким, чтобы настроить интеграцию с 1С или другими корпоративными учетными программами.

Благодаря тому, что CRM направляет работу сотрудников, они не совершают ошибок, а если о чем-то забывают, то руководитель получает уведомление о просроченном деле. Компания становится более управляемой, прибыль предсказуемой, цифры правдивыми. В такой ситуации директор почти не тратит время на контроль и может сосредоточиться на стратегическом управлении. Внедрение CRM-системы помогает компаниям в целом увеличивать эффективность работы. Автоматизация основных процессов избавляет от огромного количества рутинных операций: от элементарной подготовки документации и отчетов до серьезного финансового планирования[3].

Также рассмотрим другую, не менее известную и рабочую платформу под названием B2B – в переводе с английского языка расшифровывается как «бизнес ради бизнеса». Иными словами, компания реализует в продажу товары либо услуги, необходимые не для потребления покупателя, а для ведения его собственного бизнеса.

Отметим, что B2B продажи претерпели существенные изменения за последние несколько лет. Это связано с появлением новейших технологий, ростом конкуренции и сознательности покупателя. Рынок B2B функционирует по иным правилам, нежели классический потребительский рынок. Соответственно, здесь

---

[1] Лидогенерация (англ. lead generation) — элемент лид-менеджмента, маркетинговая тактика, направленная на поиск потенциальных клиентов с определёнными контактными данными.

[2] Роль искусственного интеллекта в бизнесе. URL: https://www.simbirsoft.com/blog/rol-iskusstvennogo-intellekta-v-biznese/ (Дата обращения: 05.01.2021).

[3] Иващенко М. А. Искусственный интеллект в управлении следственными органами / М. А. Иващенко, С. С. Бурынин. – Москва: Московская академия Следственного комитета Российской Федерации, 2021. С. 47.

существуют совершенно другие стратегии и инструменты, применяемые в процессе продаж.

На практике продажи B2B выглядят следующим образом. К примеру, в фирму, где занимаются переводами текстов, обращается директор строительного магазина с просьбой перевести всю информацию по новым итальянским строительным материалам, обоям и гарнитуре. В этой фирме ему оказывается эта услуга, которая в дальнейшем поможет осуществлять свою деятельность строительному магазину, так как сотрудники получат описание товара на русском языке и смогут консультировать своих клиентов. Именно так на практике выглядят B2B продажи, они нацелены не на конкретного покупателя и его личные нужды, а на нужды того бизнеса, которым он владеет. B2B продажи становятся неким дополнительным звеном, необходимым для осуществления предпринимательской деятельности.

На сегодняшний день эксперты выделяют три основных вида продаж данной платформы, а именно:

1. B2B. Принципиальное отличие данного вида продаж заключается в том, что партнёром и потребителем услуг становится исключительно юридическое лицо, то есть сторонняя организация. Одни бизнесмены осуществляют покупку товаров и услуг у других предпринимателей, полностью оправдывая аббревиатуру «бизнес для бизнеса».

2. B2C. Это более привычный вид бизнес-продаж, ориентированный на среднестатистического потребителя. Его называют бизнесом для потребителей, он осуществляется чаще всего через магазинные продажи. Объёмы реализуемой продукции могут быть небольшими;

3. B2G. Продажи, ориентированные на государство, то есть государство выступает главным покупателем. Получить доступ к сотрудничеству с государством достаточно сложно ввиду высокого уровня конкуренции и строгих требований. Подобными продажами занимается не так много коммерческих организаций, это особая привилегия, которую можно лишь выиграть в ходе тендера.

Исходя из трёх существующих видов продаж, можно отметить, что B2C продажи – наиболее распространённое явление, они понятны, заниматься ими достаточно легко. Что касается B2B продаж, то это более узкоспециализированное направление коммерческой деятельности, перерастающее в форму сотрудничества.

Таким образом, B2B продажи представляют собой продажу товаров и услуг для нужд сторонних предприятий. Это яркий пример сотрудничества юридических лиц с другими юридическими лицами. Сегмент достаточно интересный для российского рынка, требует особого подхода и специфических знаний. «Бизнес для бизнеса» ориентирован на продажи, способные помочь разрешить ряд важных бизнес-задач. Следуя всем рекомендациям, можно выстроить успешный B2B бизнес, приносящий стабильный доход.

В завершение отметим, что у российского бизнеса с каждым годом открывается всё больше возможностей для реализации своей деятельности, однако сделаем оговорку, что если этот бизнес связан с IT-технологиями,

электронными ресурсами и использованием различных технологий ИИ. Безусловно, эти направления в бизнесе становятся всё более масштабными, более востребованными в мире.

Литература

1. Федеральный закон от 30 декабря 2015 г. № 462-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации в части использования беспилотных воздушных судов» // СПС «КонсультантПлюс».
2. Приказ Министерства промышленной торговли России от 23 апреля 2010 г. № 319 «Об утверждении Стратегии развития автомобильной промышленности Российской Федерации на период до 2020 года» // СПС «КонсультантПлюс».
3. Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».
4. Иващенко М. А. Искусственный интеллект в управлении следственными органами / М. А. Иващенко, С. С. Бурынин. – Москва: Московская академия Следственного комитета Российской Федерации, 2021. – 97 с.
5. Искусственный интеллект для бизнеса: ожидание и реальность // URL: https://geoline-tech.com/ai-for-business/.
6. Как искусственный интеллект используется в бизнесе: обзор и кейсы. URL: https://vc.ru/marketing/105102-kak-iskusstvennyy-intellekt-ispolzuetsya-v-biznese-obzor-i-keysy.
7. Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта: версия 1:0, ноябрь 2017 г. Текст на русском языке см.: URL: http://robopravo.rU/uploads/s/z/6/g/z6gj0wkwhv1o/file/6dbrNqgu.pdf.
8. Роль искусственного интеллекта в бизнесе. URL: https://www.simbirsoft.com/blog/rol-iskusstvennogo-intellekta-v-biznese/.
9. Федорина А.А. К вопросу о правовом статусе робототехники и искусственного интеллекта // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 4. С. 3-8.

М.В. Кардашевская

Участие специалиста в производстве следственных действий, направленных на получение компьютерной информации

Аннотация. В статье рассматриваются некоторые проблемные вопросы участия специалиста в производстве следственных действий, направленных на получение компьютерной информации. Выработаны требования, которым должен отвечать внештатный специалист-компьютерщик. Предложено выделение в УПК России нового вида следственного осмотра – осмотр компьютерной информации.

Ключевые слова: специалист, следственные действия, компьютерная информация, киберпреступления, высокие технологии.

В эпоху развития цифровых технологий практически при расследовании любого преступления может сложиться следственная ситуация, при которой возникает необходимость в производстве следственных действий, направленных на получение компьютерной информации. Особенно это актуально при расследовании киберпреступлений и преступлений в сфере высоких технологий.

Согласно ст. 164.1 УПК России при производстве следственных действий, направленных на получение компьютерной информации, должен участвовать специалист[1]. Однако на практике нередко возникает вопрос, а где этого специалиста взять? Штаты экспертов-компьютерщиков в правоохранительных органах, в большинстве случаев, не укомплектованы, да и невозможно постоянно отрывать экспертов от выполнения их прямых обязанностей – производства экспертиз. Одним из способов решения этой проблемы является создание внештатной системы специалистов в области компьютерной информации, которые будут содействовать правоохранительным органам (как следствию, так и оперативным сотрудникам) своими знаниями. Сегодня практически в каждом территориальном органе МВД, управлении СК есть список переводчиков, которых приглашают к участию в следственных действиях на платной основе (в случае возникновения необходимости их участия в уголовном процессе). Представляется возможным создание такого же «списка» специалистов-компьютерщиков. В большинстве своем, специалисты в области компьютерных технологий – это увлеченные своей работой люди, которым интересно оказывать содействие правоохранительным органам.

Однако кандидат в список специалистов-компьютерщиков должен отвечать ряду требований. Во-первых, он должен быть компетентен в области компьютерных технологий, что должно быть подтверждено соответствующим дипломом об образовании или его постоянная работа должна быть связана с компьютерными технологиями, т. к. среди данной категории лиц достаточно большой процент самоучек, по своим умениям и навыкам существенно превосходящих коллег с дипломами. Во-вторых, кандидат не должен быть причастен или даже заподозрен в причастности к совершению киберпреступлений или преступлений в сфере высоких технологий, а значит, его необходимо проверить, как и любого другого кандидата, поступающего на службу в Следственный комитет или МВД, в том числе и с использованием полиграфа. В-третьих, кандидат должен выразить свое добровольное согласие содействовать своими знаниями правоохранительным органам, а также дать расписку о неразглашении сведений, ставших ему известными в связи с участием в производстве следственных действий. Специалист при участии в следственном действии может использовать как собственные научно-технические средства,

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 23.09.2021) // КонсультантПлюс (дата обращения 29.11.2021).

оборудование, аппаратура, приборы, компьютерные программы, так и те, которые находятся на вооружении правоохранительных органов.

От обоснованного мнения специалиста, участвующего при производстве следственных действий, направленных на получение компьютерной информации, зависит принятие следователем одного из следующих тактических решений:

- оставление компьютерной техники у владельца с копированием необходимой информации;
- изъятие компьютерной техники с копированием необходимой владельцу информации;
- изъятие компьютерной техники без копирования информации;
- в случае изъятия – перечень необходимой для изъятия техники.

Для того чтобы специалист сформировал свое мнение, ему необходимо осмотреть содержимое компьютера с учетом тех задач, которые поставлены перед ним следователем. Поэтому при производстве обыска или выемки с целью изъятия компьютерных носителей информации обязательно должно производиться такое следственное действие, как осмотр. В УПК Республики Беларусь регламентирован порядок производства нового вида следственного осмотра - осмотр компьютерной информации. В ст. 204.1 УПК Республики Беларусь определен порядок доступа следователя к компьютерной информации (по согласию владельца, в случае отсутствия согласия – по решению суда (если адаптировать эту статью к российскому законодательству) или по постановлению следователя, в случаях, не терпящих отлагательства; какие действия могут производиться в ходе осмотра; что подлежит отражению в протоколе (использованные научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы, порядок осуществления доступа к компьютерной информации, произведенные в ходе осмотра действия и полученные результаты)[1]. Представляется, что аналогичная статья должна быть принята и в Российской Федерации.

Следует учитывать, что грамотно проведенный осмотр компьютерной информации может, в большинстве случаев, исключить необходимость производства судебной экспертизы в отношении электронных носителей информации, а значит, подобный осмотр может быть длительным по времени, что необходимо учитывать еще при планировании данного следственного действия.

И в заключении хотелось бы отметить на необходимость привлечения специалиста не к одному следственному действию, а ко всему процессу расследования по конкретному уголовному делу, поскольку по одному уголовному делу может проводиться несколько следственных действий, направленных на получение компьютерной информации у разных лиц, и специалист, который уже знает обстоятельства дела, может лучше и главное

[1] Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 года № 295-З (с изменениями и дополнениями по состоянию на 26.05.2021 г.) //http://continent-online.com/document/?doc_id=30414958#pos=2187;4 (дата обращения 29.11.2021).

быстрее ориентироваться в том большом потоке информации, который есть на любом электронном носителе. Кроме того, специалист, который осмотрел компьютерную информацию, может помочь следователю в формулировке вопросов по поводу механизма совершенного преступления.

П.В. Климято

Исследование компьютерной информации с использованием программно-аппаратных комплексов

Аннотация. Важность исследования компьютерной информации обусловлена широким распространением интернета и мобильных устройств как средств доступа к нему. Большие объемы компьютерной информации требуют применения программно-аппаратных комплексов для ее собирания (извлечения) и последующего анализа, в процессе чего возникают определенные сложности получения доступа к компьютерной информации. Статья содержит сведения о доказательственном значении элементов (артефактов) отчета, созданного в ходе извлечения компьютерной информации из конкретного мобильного устройства с применением программно-аппаратного комплекса UFED; анализ артефактов в программе UFED Reader; описание функциональных возможностях программы UFED Reader; перевод результатов анализа артефактов в уголовно-процессуальную форму в целях использования в качестве доказательств при производстве по материалам и уголовным делам.

Ключевые слова: компьютерная информация, программно-аппаратный комплекс, UFED, отчет, категории данных, артефакт, доказательства.

В начале 2021 г. на 9,5 млн жителей Республики Беларусь приходилось 7,82 млн пользователей, или 82,8 % населения, интернета. При этом 3,9 млн, или 41 %, населения пользовалось социальными сетями, и 95 % из них – с мобильных устройств[1]. Интенсивность распространения мобильных устройств, в том числе как средств доступа в интернет, во все сферы общественной жизни и во все слои общества подтверждает тезис об исключительной важности исследования компьютерной информации, хранящейся в тех или иных устройствах, принадлежащих участникам уголовного процесса, как источника обнаружения доказательств по любой категории общественно-опасных деяний в целях установления истины.

Институт собирания доказательств изучался такими учеными как Р.С. Белкин, Г.И. Грамович, В.Я. Колдин, Ю.Г. Корухов, И.М. Лузгин, В.А. Образцов, А.С. Рубис, Н.А. Селиванов, А.В. Дулов, Н.П. Яблоков и др. В научных публикациях по данному направлению рассматривались понятие, содержание, стадии процесса собирания доказательств, обнаружение (розыск, поиск), получение, фиксация, изъятие и сохранение доказательств, способы, требования, условия, методы и средства их собирания и т. д.[2]

[1] Официальный интернет-портал статистической информации. URL: www.datareportal.com

[2] Грамович Г. И. Основы криминалистической техники: Процессуальные и криминалистические аспекты: Выш. шк. Минск, 1981. С. 23.

Однако собирание доказательственной компьютерной информации отличается от общих подходов. Указанный процесс имеет ряд научных и правовых проблем, связанных с определением стадий, способов, средств и закономерностей собирания компьютерной информации и др., что вызывает некоторые сложности.[1]

Так, одна из трудностей – необходимость изучения большого объема компьютерной информации, которая может иметь доказательственное значение. С учетом указанного особую значимость приобретает организация работы по применению современных программно-аппаратных комплексов в целях собирания компьютерной информации, а также ее последующего анализа для определения доказательственного значения, подтверждения либо опровержения версии о виновности лица в совершении определенного преступления.

Рассматривая порядок применения программно-аппаратных комплексов, необходимо разобраться в его реализации с технической точки зрения, а именно изучить возможности применения программно-аппаратных комплексов, в контексте применения которых процесс собирания компьютерной информации допустимо назвать «извлечением компьютерной информации».

В первую очередь необходимо обозначить, что производители программно-аппаратных комплексов всегда следует за развитием технологий в области компьютерной техники, в том числе мобильных устройств. На основании данного утверждения возможно сформулировать некоторые особенности, связанные с извлечением компьютерной информации: большое количество видов операционных систем, используемых мобильными устройствами разных производителей; отсутствие единых стандартов в интерфейсах подключения, оборудовании и программном обеспечении мобильных устройств; перманентная разработка новых моделей устройств, процессоров с новыми средствами защиты и обеспечения конфиденциальности.

Указанные особенности создают объективные технические проблемы извлечения компьютерной информации, вынуждая находить индивидуальные решения под конкретные операционные системы и иное программное обеспечение, оборудование мобильных устройств.

По мере преодоления обозначенных трудностей собирание компьютерной информации из устройств осуществляется различными способами (в различных режимах), от выбора и степени реализации которых напрямую зависит результат извлечения компьютерной информации. В настоящей статье рассмотрены лишь способы извлечения компьютерной информации, доступные в контексте применения программно-аппаратных комплексов и полученных на основании их применения результатов.

Первый способ – «ручной» режим извлечения компьютерной информации. Сущность заключается в визуальном изучении информации, хранящейся в устройстве, фиксации ее посредством самого устройства (путем создания

[1] Россинская Е. Р. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров / Е. Р. Россинская, Т. А. Сааков // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 111.

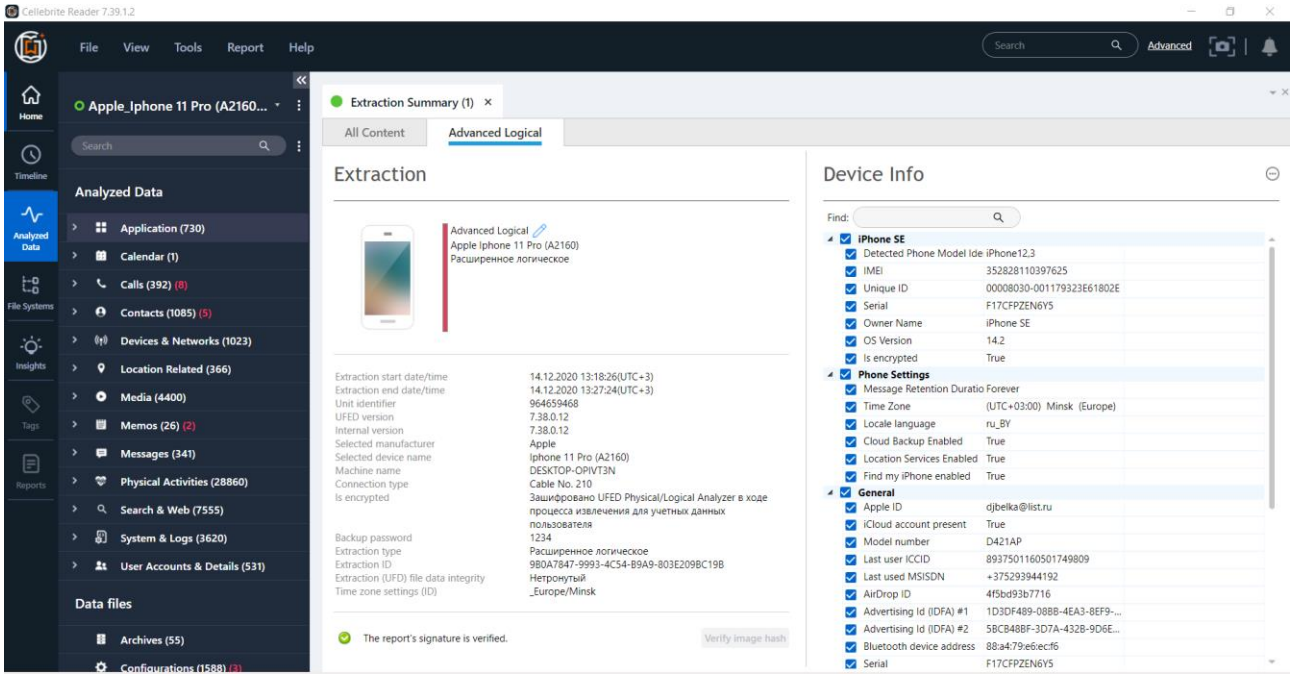
скриншотов) либо с помощью научно-технических средств общего назначения (фотоаппарата, видеокамеры). Кроме того, в таком режиме собирания компьютерной информации могут использоваться прикладные программы, разработанные для синхронизации мобильного устройства с персональным компьютером (например, Huawei HiSuite). При этом необходимо подключение исследуемого мобильного устройства к компьютерной технике посредством интерфейсов передачи данных USB, IrDA, Bluetooth и т. д. Подобным способом невозможно получить все данные, а также произвести восстановление удаленных файлов и записей. В то же время иногда – это единственно возможный, из доступных в той или иной ситуации, способ собирания хранящейся в устройстве компьютерной информации (например, когда применение программно-аппаратного комплекса не привело к извлечению компьютерной информации).

Второй способ собирания компьютерной информации – применение таких программно-аппаратных комплексов, как «Мобильный Криминалист», UFED[1], XRY и др., которые позволяют извлекать информацию в различном ее объеме (даже исключительно ту информацию, которая может быть собрана и в ручном режиме). Интерес и особую ценность данных программно-аппаратных комплексов представляет возможность физического извлечения информации, то есть получение побитовой копии всей внутренней памяти мобильного устройства, в том числе с восстановлением удаленных записей и файлов. В этом случае для создания копии данных разрабатываются собственные загрузчики, посредством которых можно получить доступ не только к внутренней памяти, но и иногда обойти пароли, установленные пользователями. Создать физический дамп памяти получается не всегда, но в большинстве случаев применение программно-аппаратных комплексов позволяет извлечь полезный массив компьютерной информации, который следует подвергать дальнейшему анализу.

Следует указать, что на данном этапе наибольшую научную и практическую значимость представляет рассмотрение вопросов, связанных с результатами извлечения компьютерной информации с применением программно-аппаратного комплекса UFED. Извлеченная компьютерная информация представлена в виде скомпилированных файлов отчета с обозначением доказательственного значения его элементов (артефактов) независимо от объема извлеченной информации.

Отчет запускается в специальной среде (оболочке) – программе UFED Reader, которая имеет интуитивно понятный интерфейс, состоящий из панели инструментов (пункты File, View, Tools, Report, Help), стандартных разделов навигационного меню (пункты Home, Timeline, Analyzed Data, File Systems, Insights, Tags, Reports) и подразделов извлеченной компьютерной информации из конкретного устройства, количество и объем которых вариативны, зависят от удавшегося способа ее извлечения.

[1] Официальный интернет-портал компании «Cellebrite». URL: https://www.cellebrite.com/



Интерфейс отчета по извлеченной информации

Анализ находящейся в отчете компьютерной информации следует начинать с обзорного изучения его содержимого, а именно с подраздела Extraction Summary (в разделе Home), который представляет собой свод данных об отчете – способе и дате извлечения, предмете исследования (вкладка Extractions) и его характеристиках (вкладка Device info), количественных показателях извлеченного контента устройства (вкладка Content). Целесообразно использовать данные о марке, модели и иных идентификационных характеристиках устройства (идентификаторы IDFA, AirDrop, Apple ID, Bluetooth device address, Serial, WiFi address, IMEI, MSISDN и др.), дате и времени извлечения компьютерной информации, помещая их в соответствующий протокол осмотра. Сведения об удавшемся способе извлечения компьютерной информации дают представление об ожидаемом объеме (полноте) ее извлечения. В рассматриваемом отчете – это Advanced Logical (Расширенное логическое), что указывает лишь на частичное извлечение компьютерной информации.

Наиболее информативным и полезным является подраздел Analyzed Data, который содержит распределенные по конкретным категориям следующие данные:

- Application (Applications Usage Log, Installed Applications) – сведения о приложениях, установленных в операционную систему исследуемого устройства, позволяют установить достоверную информацию о времени создания приложений, а иногда - времени их удаления;

- Calendar – записи из стандартного приложения устройства «Календарь»;

- Calls – сведения о соединениях, совершенных пользователем устройства как стандартными средствами телефонии (Native), так и сторонними приложениями – Viber, Skype, Telegram, Instagram и т. д.;

- Contacts – сведения о сохраненных в памяти устройства контактах как в стандартной телефонной книге, так и в мессенджерах (Viber, Telegram и т. п.), а также аккаунтах (Apple ID, Google-аккаунте);

- Device & Networks – сведения о соединениях исследуемого устройства с иными устройствами (например, умными часами, портативными колонками и т. п.) посредством различных протоколов и средств соединения (Bluetooth, Wi-Fi);

- Location Related – сведения о нахождении устройства в конкретный момент времени. Например, во время создания фотоснимка в его метаданные сохраняются сведения о географических координатах, которые соответствуют месту, где находился пользователь в момент создания указанного снимка;

- Media (Audio, Images, Videos) – аудиофайлы, изображения и видеозаписи, собранные из всей файловой структуры памяти устройства;

- Memos (Notes, Recordings) – заметки и аудиозаписи, созданные как стандартными средствами устройства, так и иными приложениями;

- Messages (Chats, Instant Messages) – сообщения из диалогов в профилях приложений обмена мгновенными сообщениями, социальных сетей, а также смс-сообщения, созданные стандартными средствами устройства. Наряду с очевидным доказательственным значением диалогов смс-сообщения могут содержать актуальные учетные данные различных мессенджеров и сервисов, требующих подтверждения соответствующими кодами, приходящими в смс-сообщениях на абонентский номер (например, в случае использования 2FA);

- Physical Activities – сведения из функционирующих в устройстве сервисов об активности пользователя (например, Apple Fitness+);

- Search & Web (Cookies, Searched Items, WEB Bookmarks, WEB History) – сведения о «куках» (файлах, загружаемых на устройство с WEB-сервера в целях быстрой работы в случае повторного обращения к нему же, выполняющих конкретные задачи: хранение логинов и паролей от сайтов в течение интернет-сессии; запоминание действий пользователя (например, для наполнения корзины покупок, запоминания вариантов голосования и т. п.); идентификация пользователей в случае использования вечных «куков»; сохранение индивидуального профиля зарегистрированного пользователя); хранение поисковых запросов в браузерах, инсталлированных в операционную систему исследуемого устройства; хранение истории посещенных интернет-ресурсов (в том числе добавленных в каталог «Избранные»);

- Systems & Logs – сведения об аутентификации пользователя в различных приложениях и сервисах посредством исследуемого устройства;

- User Accounts & Details (Passwords, User Accounts) – сохраненные учетные сведения (логин и пароль, токен) для авторизации в приложениях и сервисах; сведения об аккаунтах пользователя устройства, созданных в различных приложениях и сервисах (электронной почты, мессенджеров).

При изучении содержащейся в отчете компьютерной информации особо следует обратить внимание на:

- артефакты, отмеченные красным цветом, – ранее удалены, но восстановлены в ходе извлечения компьютерной информации средствами UFED;

- функциональные возможности UFED Reader, заключающиеся в использовании встроенных в программу средств фильтрации и сортировки данных по различным критериям; генерирования мини-отчетов командой Export по конкретным подразделам и вкладкам; генерирования полного отчета командой Report с последующим приобщением сгенерированных отчетов и экспортированных файлов (фотоизображений, видеозаписей и т. п.) к протоколу осмотра в качестве приложений, а также их записью на неперезаписываемый носитель информации.

Таким образом, исследование извлеченной с применением программно-аппаратных комплексов компьютерной информации неоценимо полезно в качестве самостоятельного способа получения новых данных, а также позволяет провести ее комплексный анализ в соотнесении с иными установленными обстоятельствами общественно-опасного деяния для их подтверждения либо опровержения. Ход и результаты подобного исследования в последующем приобретают уголовно-процессуальную форму и используются в качестве доказательств при производстве по материалам и уголовным делам.

Литература

1. Digital 2021: Belarus [Электронный ресурс]. – Режим доступа: https://datareportal.com/reports/digital-2021-belarus?rq=Digital%202021%20%3A%20Belarus/. – Дата доступа: 17.12.2021
2. Грамович Г. И. Основы криминалистической техники: Процессуальные и криминалистические аспекты/ Г. И. Грамович. – Минск: Выш. шк., 1981. – 208 с.
3. Компания «Cellebrite» [Электронный ресурс]. – Режим доступа: https://www.cellebrite.com/. – Дата доступа: 17.12.2021.
4. Россинская, Е. Р. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров/ Е. Р. Россинская, Т. А. Сааков// Криминалистика: вчера, сегодня, завтра. – 2020. – № 3(15). – С. 106-123.

П.Н. Кобец

Криминологические проблемы борьбы с преступлениями, совершаемыми с использованием современных информационных технологий

Аннотация. Важность рассматриваемой проблематики подтверждается многочисленными научными исследованиями. При этом, несмотря на детальную проработку многих проблемных вопросов по данной тематике, она нуждается в дальнейшем исследовании. Автором делается вывод о том, что деятельность правоохранителей по противодействию преступлениям совершаемым с использованием современных информационных технологий необходимо выстраивать на основе системного комплекса мероприятий, которые бы сочетали в себе

многообразие методов работы, отдавая при этом приоритеты методам профилактики и межведомственному сотрудничеству.

Ключевые слова: правоохранительные органы, вызовы и угрозы, профилактика, киберугрозы, борьба с преступностью, международное сотрудничество, межведомственное сотрудничество, информационная безопасность, уголовная ответственность, информационные технологии.

В настоящее время, планомерному и устойчивому функционированию нашей страны, помимо различных внешних угроз, представляют серьезную опасность различные криминальные структуры. Деятельность многих преступных организаций осуществляемая на основе криминальных схем, связанных с отторжением государственной и частной собственности, сегодня представляет не только большую опасность жизни и здоровья российских граждан, но также и выступает в качестве преступного механизма по генерированию противоправных деяний[1]. Сегодня в Российской Федерации большинство угроз исходящих со стороны преступных организаций нацелены на национальные приоритеты нашей страны, которые неразрывно связаны с внедрением информационно-телекоммуникационных сетей. Активно внедряемые в условия нового тысячелетия практически во всех сферах жизнеобеспечения российского общества информационно-телекоммуникационные технологии нуждаются в серьезной защите, поскольку слабая защищенность приводит к повышению их уязвимости и дополнительным рискам связанным с утечкой информационных данных[2].

Применение информационных технологий превращается в неотъемлемую часть нашей повседневной жизни и по прогнозам, который был представлен Всемирной ассоциации, представляющей интересы операторов мобильной связи во всем мире, к 2025 г. количество подключений к IoT будет удвоено, и достигнет почти 25 млрд, что только увеличит количество совершаемых IT преступлений[3]. Сегодня цифровые технологии и система «Интернет» приобретают все большее значение для инноваций и экономического роста. Безопасное и надежное киберпространство важно для безопасности, стабильности и процветания нашей страны, а хорошая кибербезопасность имеет решающее значение для конкурентоспособности России, экономической стабильности и долгосрочного процветания. Однако, новые сетевые интернет-технологии обуславливают появление новейших видов социально-группового взаимодействия, к большому сожалению которые приходят на служение криминальных структур. Они могут применяться в процессе дестабилизации общества, совершения всевозможных

[1] Кобец П.Н. Предупреждение экстремистских проявлений в подростковой и молодежной среде - важнейший элемент совершенствования обеспечения общественной безопасности нашей страны // Национальная безопасность и стратегическое планирование. – 2015. – № 4(12). – С. 52-55. С. 53.

[2] Кобец П.Н. О современных информационных технологиях, используемых экстремистскими и террористическими группировками, и необходимости противодействия киберпреступности // Вестник развития науки и образования. – 2016. – № 6. – С. 4-9. С. 7.

[3] Интернет вещей, IoT, M2M мировой рынок UPL: https://www.tadviser.ru/index.php (дата обращения 21.11.2021).

противоправных деяний. При этом важно отметить, что к сожалению, следует констатировать, что сегодня состояние законодательного регулирования об уголовной ответственности за совершение противоправных деяний с использованием современных информационных технологий не в полной мере отвечает современному уровню складывающихся в этой сфере общественных отношений, и поэтому не может способствовать эффективному решению задач УК РФ. Свидетельством этого является рост преступности в данной сфере. Причем с каждым годом число совершаемых с использованием современных информационных технологий в России имеет очень высокие темпы роста. Так, например, в 2020 году МВД России сообщило о резком увеличении количества IT-преступлений. Общее количество «преступлений, совершенных в нашей стране с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети Интернет – на 91,3%, а с помощью средств мобильной связи – на 88,3%»[1].

Противоправные деяния в сфере информационных технологий представляют из себя новую форму преступности, рост которой обусловлен демократизацией доступа к компьютерным сетям и ростом глобализационных процессов. Первоначально интернет использовался в основном для научных и технических целей. Таким образом, при обращении документов не возникало никаких проблем с конфиденциальностью, и данные передавались по сети в открытом виде. Но открытие сети «Интернет» для коммерческого использования многое изменило. Поскольку сегодня конфиденциальная информация циркулирует по каналам связи, безопасность связи стала серьезной проблемой, как для отдельных интернет-пользователей, так и в целом для большинства учреждений и организаций. Все они стремятся защитить себя от мошеннического использования своих данных или от вредоносных вторжений в компьютерные системы, которые приводят к киберпреступности.

Президентом Российской Федерации В.В. Путиным уделяется самое пристальное внимание проблемам киберпреступности. Так в частности, «24 февраля 2021 г. проводя заседание коллегии ФСБ России им было отмечено о необходимости выверенной стратегии, направленной на борьбу с киберпреступностью, которая бы основывалась на обязательных прогнозных оценках ситуации, складывающейся вокруг рассматриваемой проблемы»[2].

Указом Президента Российской Федерации в феврале 2021 г. «утверждена новая шестилетняя Стратегия национальной безопасности, в которой впервые заметное место отведено вопросам информационно-коммуникационных технологий. Так в частности Стратегия указывает, что быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и

[1] Состояние преступности в России за январь–декабрь 2020 года. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184 (дата обращения: 21.11.2021).

[2] Путин призвал создать стратегию по борьбе с киберпреступностью URL: https://ria.ru/20210224/putin-1598783523.html (дата обращения: 21.11.2021).

государства»[1]. Нельзя не отметить, что противоправные деяния совершаемые с использованием современных информационных технологий имеют высокую латентность, о которой говорится многими исследователями, поэтому в целях получения более точных данных о ее масштабах и распространённости необходимы новые методики и источники получения информационных данных. Недостаточное комплексное исследование всех проблемных вопросов, связанных с рассматриваемой преступностью, в купе с их высокой латентностью, обуславливают недостаточную эффективность существующего профилактического комплекса указанных противоправных деяний.

К сожалению, в настоящим момент, пока что одной из сложно решаемой задачей для большинства стран является, деятельность, связанная с получением и анализом необходимой доказательственной базы рассматриваемых преступлений. А для того, что обозначенные задачи эффективно решать, необходима не только совершенная тактика расследования указанных преступлений, но и специальные знания в сфере компьютерных технологий и информации. Решению проблемных вопросов в рассматриваемой сфере в том числе мешает не достаточное количестве методических источников, которые бы помогали раскрывать и расследовать рассматриваемые преступления. Повышению эффективности рассматриваемой деятельности могла бы способствовать обобщенная судебная практика по преступлениям совершаемым с использованием современных информационных технологий. Кроме того, правоохранительные органы должны быть в полном объеме обеспечены специалистами, разбирающимися в вопросах информационных технологий, компьютерной техники, а также выявлении и расследовании рассматриваемых преступлений. В целях совершенствования обозначенной проблемы существует необходимость по введению новых специализаций в вузах юридического профиля и в специальных учебных заведениях.

Учебные программы для специалистов в сфере правоохранительной деятельности, также должны включать элементы подготовки по вопросам кибербезопасности. В свете растущего спроса со стороны всех субъектов рассматриваемой деятельности, когда это возможно, часть предложения по обучению и образованию должна быть адаптирована для межведомственного взаимодействия. Наверстывание упущенного должно сопровождаться повышением безопасности цифровой жизни всех правоохранительных структур, начиная с повышения безопасности их информационных систем. Межведомственная координация должна быть структурирована и усилена. В дополнение к региональным и часто изолированным мерам, которые необходимо создать адаптированную организацию поддержки всем субъектам бобры с киберпреступностью. Наряду с возможным созданием конкретных систем поддержки для заинтересованных сторон в секторе кибербезопасности необходимо уточнить и оптимизировать условия доступа к существующим

[1] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 21.11.2021).

системам поддержки, а также методы их внедрения. Для предупреждения рассматриваемых преступлений использование только технических средств защиты совершенно недостаточно. Необходимо международное сотрудничество и мобилизация всех участников, от отдельных гражданин до государств. Также, важно учитывать опыт зарубежных правоохранительных органов и частных структур в сфере противодействия преступлениям совершаемым с использованием современных информационных технологий.

В целом необходимо отметить, что деятельность правоохранительных органов нашей страны по предупреждению IT преступлений необходимо выстраивать на основе системного комплекса мероприятий, которые бы сочетали в себе многообразие методов работы, отдавая при этом приоритеты методам профилактики. В целях успешной профилактической работы по рассматриваемому направлению необходимо развивать взаимодействие со всеми правоохранительными органами нашей страны.

Литература

1. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 21.11.2021).
2. Интернет вещей, IoT, M2M мировой рынок UPL: https://www.tadviser.ru/index.php (дата обращения 21.11.2021).
3. Кобец П.Н. Предупреждение экстремистских проявлений в подростковой и молодежной среде - важнейший элемент совершенствования обеспечения общественной безопасности нашей страны // Национальная безопасность и стратегическое планирование. – 2015. – № 4(12). – С. 52-55.
4. Кобец П.Н. О современных информационных технологиях, используемых экстремистскими и террористическими группировками, и необходимости противодействия киберпреступности // Вестник развития науки и образования. – 2016. – № 6. – С. 4-9.
5. Путин призвал создать стратегию по борьбе с киберпреступностью URL: https://ria.ru/20210224/putin-1598783523.html (дата обращения: 21.11.2021).
6. Состояние преступности в России за январь–декабрь 2020 года. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184 (дата обращения: 21.11.2021).

К.А. Костенко

Обеспечение информационной безопасности детей путем мониторинга информационно-телекоммуникационной сети Интернет

Аннотация. Мониторинг информационно-телекоммуникационной сети «Интернет», являясь одним из наиболее важных направлений обеспечения информационной безопасности детей, позволяет решать самые сложные задачи по

выявлению негативного контента в интернет пространстве. Следственным комитетом Российской Федерации такие задачи решаются с помощью современных систем онлайн-мониторинга. Автором отмечается, что своевременно проведенные мониторинговые мероприятия, позволяют оперативно оградить несовершеннолетних от информации, причиняющей вред их здоровью и развитию, а также незамедлительно приступить к восстановлению их прав и законных интересов.

Ключевые слова: мониторинг сети «Интернет», Следственный комитет Российской Федерации, информационная безопасность детей, негативный контент.

Мониторинг, как процесс постоянного наблюдения, в наиболее широком его понимании, следует рассматривать как методику и систему наблюдений за состоянием определенного объекта или процесса, дающую возможность наблюдать их в развитии, оценивать и оперативно выявлять результаты воздействия различных внешних факторов[1].

В системе Следственного комитета Российской Федерации (далее также Следственный комитет или СК России) мониторинг сети «Интернет» является одним из наиболее важных направлений взаимодействия со средствами массовой информации. Потребность в нем продиктована необходимостью оперативно реагировать на различные события, в т. ч. связанные с распространением негативного контента и принимать решения в условиях полной информированности[2].

В России исследователи негативный контент делят на следующие категории:

- незаконный (детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления); все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализм и др.), а также разжигание ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным); призывы к участию в незаконных митингах, шествиях, акциях; азартные игры и т.д.;
- неэтичный (противоречащие принятым в обществе нормам морали и социальным нормам: агрессивные онлайн-игры, азартные игры, нецензурная брань, оскорбления, и др.).
- вредоносный (который может нанести прямой вред психическому и физическому здоровью детей и подростков: пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей и т.д.)[3].

---

[1] Большой Российский энциклопедический словарь. - Репр. изд. - Москва: Большая Российская энцикл., 2009. С. 911.

[2] См.: Костенко К.А. Основные задачи мониторинга СМИ и информационно-телекоммуникационной сети Интернет в Следственном комитете РФ // Российская юстиция. 2020. №5. С. 56-57.

[3] Смирнов А.А. Негативный контент: проблемы идентификации в контексте правового регулирования // Информационное право. 2015. № 2. С. 18 – 25; Сайт конференций [Электронный ресурс] // [Сайт]. - Режим доступа: https://www.sites.google.com/site/saitkonferencii/sekcia-3/negativnyj-kontent-kak-izbezat-ego-v-

Выделяя негативный контент среди потока информации, получаемой в сети «Интернет», необходимо обратить внимание на то, что применение автоматизированных систем при осуществлении мониторинга СМИ не может полностью создать так называемый «фильтр», способный вовремя обнаружить и локализовать негативный контент. Здесь необходим, и не исключается, так называемый мониторинг в «ручном» режиме, поскольку качественный анализ текста предполагает оценку таких нюансов, как эмоции, угрозы, характер отношений между объектами. При этом, достаточно часто, субъекты размещения негативного контента пытаются его завуалировать, исключая прямое указание слов, фото и видео материалов, которые могут быть распознаны, как негативный контент и выявлены в автоматическом режиме. Случаи завуалирования негативного контента в сети «Интернет» происходят достаточно часто. Лишь только в качестве примера приведем, имевший место в г. Хабаровске.

Так, для привлечения молодежи на несанкционированные митинги и шествия в поддержку бывшего губернатора Хабаровского края С. Фургала, обвиняемого в организации убийств, его сторонники устроили заранее продуманный флешмоб с безобидным названием «покормиголубей». Переквалификацию птицы голубя запустил сторонник Фургала, Хабаровский журналист Алексей Романов. 16.07.2020 он выложил на своем ютуб-канале ролик с призывом выйти 18.07.2020 на площадь им. Ленина в г. Хабаровске и накормить изголодавшихся птиц. Ролик впоследствии стал «вирусным», он распространился в сети «Интернет» и послужил одним из поводов, проведенных позже незаконных митингов и шествий с участием молодежи во многих городах России[1].

Указанный пример свидетельствуют, что при мониторинге сети «Интернет» серьезное значение имеет постоянное выделение и обоснование критериев вредоносности контента. Такая работа позволяет постоянно выявлять и корректировать перечень деструктивной информации. Фактически это можно сравнить с проактивным принципом работы антивирусной программы, которая выявляет вирус посредством описания и детекции признаков вредоносности. В таком случае имеется возможность автоматического сканирования информационного пространства и выявления негативного контента, подпадающего под описанные признаки. Положительным в такой схеме работы является то, что можно работать на опережение и не допустить распространения негативного контента по сети «Интернет», однако следует учесть, что такой способ очень трудоемок.

Между тем, организаторы незаконных акций для вовлечения в них несовершеннолетних все чаще используют наиболее популярные в молодёжной среде сайты, пытаясь использовать неопытность, незрелость и любопытство подростков.

---

pomos-roditelam.(дата обращения: 21.11.2021).

[1] Собеседник.ру [Электронный ресурс]: Птица протеста: уличные акции с кормлением голубей охватили всю Россию URL: https://sobesednik.ru/politika/20200722-ptica-protesta-ulichnye-akcii (дата обращения 18.11.2021).

Так, на прошедшем в Совете Федерации в начале ноября 2021 года Круглом столе «Право детей на безопасность: вызовы современности и эффективные практики» в докладах участников прозвучало, что в августе текущего года МВД провело анкетирование 464 подростков с наибольшей протестной активностью. Результаты обработки анкет показали, что более 60% опрошенных шли на протестные акции в поддержку А. Навального[1] из любопытства, 17% — за компанию с друзьями, а осознано только 2%. При этом, информацию о протестных мероприятиях в его поддержку подростки в основном получали из сети «Интернет», в том числе, социальной сети TikTok. Организаторы несогласованных акций хотели сделать из детей сакральных жертв полицейского террора и развернуть очередную антироссийскую кампанию. Некоторых школьников подстегнуло к участию в акциях любопытство, стремление заработать лайки на фото среди одноклассников[2].

В рамках изучения проблемы интернет-зависимости подростков и влияния на них распространяемого в сети «Интернет» негативного контента в ноябре 2021 года были опрошены школьники 8-9 классов частного образовательного учреждения «Школа «Талант» г. Хабаровск. Опрос открыл достаточно негативные стороны Интернет – зависимости детей: более трети из числа опрошенных школьников проводят в сети Интернет ежедневно более 3-х часов, а почти 20% более 5 часов; более четверти опрошенных вообще не читают печатные СМИ и не смотрят телевидение (заменив указанные СМИ сетью «Интернет); почти половина детей ежедневно сталкиваются с негативным контентом в сети «Интернет», реагируя на него по-разному; каждый 7-8 подросток приобрел вредную привычку или стал придерживаться нетрадиционных взглядов на жизнь в связи с получением определенной информации об этом из сети «Интернет».

Результаты опроса свидетельствуют, что сеть «Интернет» является определенным инструментом в формировании физического и психического развития несовершеннолетних в силу доминирования над всеми другими СМИ и высоким доверием к размещаемому в ней контенту. В связи с этим, мониторинг сети «Интернет» с целью выявления негативного контента является наиболее приоритетным.

Территориальные следственные органы при осуществлении мониторинга СМИ и социальных медиа нацелены на максимальное использование доступных автоматических систем для повышения эффективности в рассматриваемой деятельности. Сотрудниками ответственными за взаимодействие со СМИ СК России практически в ежесуточном режиме осуществляется мониторинг информационно-телекоммуникационной сети «Интернет» (ЯНДЕКС-

[1] Российский оппозиционный лидер, в настоящее время отбывает наказание за мошенничество в особо крупном размере и легализацию (отмывание) денежных средств.

[2]Сайт [Электронный ресурс]: URL: https://news.mail.ru/politics/48686032/?frommail=1&utm_partner_id=899 (дата обращения: 18.11.2021).

НОВОСТИ), RSS-лент информационных агентств, просмотр социальных сетей «Вконтакте», «Фейсбук», Instagram, видеохостинга YouTube, сайта Change.org[1].

Выявление в ходе такого мониторинга незаконного контента, содержащего сведения о совершенных(ом) преступлениях (преступлении) является основанием немедленно организовать процессуальную проверку или их предварительное расследование. В свою очередь, это позволяет оперативно оградить несовершеннолетних от информации, причиняющей вред их здоровью и развитию, а также приступить к восстановлению их прав и законных интересов.

Следует с сожалением констатировать, что сеть «Интернет», социальные сети достаточно часто наполнены контентом, в котором культивируется насилие, равнодушие к проблемам окружающих, безнравственность. В совокупности с отсутствием правильных ориентиров и ценностей у несовершеннолетнего это может быстро смениться корыстью, эгоизмом, злостью, что в итоге приводит к неконтролируемой агрессии подростка. Все это очень часто приводит подростков в группу риска совершающих преступления.

Проблема такого поведения зачастую кроется в систематическом получении негативного контента в соцсетях, закрытых интернет-сообществах, участниками которых они были, либо стремились стать. В этой связи, Председатель СК России А.И. Бастрыкин предложил ряд мер, которые, по его мнению, позволят существенно улучшить ситуацию в рассматриваемой сфере. Среди них: увеличение штатной численности психологической службы в образовательных организациях, увеличение их финансирования и усиление воспитательного потенциала; введение ограничений на демонстрацию в эфире телеканалов и сети «Интернет» сцен насилия, жестокости, фильтрация деструктивной информации и т.п.; поощрение и развитие института студенчества, развитие детского и молодежного движения, возрождение и модернизация общероссийских спортивных мероприятий[2].

Подводя итоги рассмотрения вопроса, следует отметить, что системный мониторинг сети «Интернет» позволяет, не только достаточно быстро организовывать проверочные мероприятия по размещенному негативному контенту, но и своевременно принять меры к его удалению. При этом, актуальность и значимость проводимой в СК России работы по организации мониторинга информационно-телекоммуникационной сети «Интернет» действительно является важной составляющей всего процесса обеспечения защиты прав и законных интересов несовершеннолетних.

Литература

1. Большой Российский энциклопедический словарь. - Репр. изд. - Москва: Большая Российская энцикл., 2009. - 1887 с.

[1] Взаимодействие следственных органов СК России со средствами массовой информации: учебно-методическое пособие; под ред. А.М. Багмета, С.Л. Петренко. – М.: Московская академия СК России, 2020. С. 107-110.

[2] Из Сети – к реальной жизни (публикация) // Газета «Следственный комитет России» № 18 (72) С. 1-2.

2. Взаимодействие следственных органов СК России со средствами массовой информации: учебно-методическое пособие; под ред. А.М. Багмета, С.Л. Петренко. – М.: Московская академия СК России, 2020. 157 с.
3. Из Сети – к реальной жизни (публикация) // Газета «Следственный комитет России» № 18 (72) С. 1-2.
4. Костенко К.А. Основные задачи мониторинга СМИ и информационно-телекоммуникационной сети Интернет в Следственном комитете РФ // Российская юстиция. 2020. №5. С. 56-57.
5. Смирнов А.А. Негативный контент: проблемы идентификации в контексте правового регулирования // Информационное право. 2015. № 2. С. 18 - 25.

В.О. Морар

Организованная преступность, киберпреступления и высокие технологии

Аннотация. В статье представлены выявленные автором тенденции развития криминальных проявлений в России. Основу анализа составил информационный массив, полученный из ГИАЦ МВД России. Первостепенно были изучены данные относящиеся к показателям проявления организованной преступности с выделением соответствующих тенденций. Далее приведены результаты анализа данных относящихся к показателям преступлений, совершенных с использованием информационно-телекоммуникационные технологий.

Ключевые слова: тенденции, организованная преступность, информационно-телекоммуникационные технологии, ИТТ, статистика, безопасность, МВД России.

Стремительное развитие технологий происходит год от года. Современные технологии проникли практически во все сферы жизнедеятельности человека и сделали обыденным существование и развитие «облачных» сервисов, «больших данных», Интернета, Интернета вещей, индустриального Интернета, социальных сетей, разнообразных платформ и сервисов в цифровой среде, цифровизацию социальных и бизнес процессов и многого другого. Все это оказывает влияние на окружающий нас мир и структуру отношений в нем. Не является исключением и трансформация криминальных проявлений. Все чаще в качестве средств совершения преступления используются информационно-коммуникационные технологии и социальная инженерия. Актуальность указанной теме придает и тот факт, что Президентом Российской Федерации в 2017 году была утверждена Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы[1].

Реализация Стратегии, как и борьба с преступностью, в особенности с организованной преступностью (далее – ОП), являются важными задачами государства.

[1] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. 2017, № 20. Ст. 2901.

Если борьба с ОП ведется достаточно давно, начавшись до принятия в 1989 году Постановления «Об усилении борьбы с организованной преступностью»[1], которое было утверждено в качестве экстренной и неотложной меры. Борьба же с преступлениями, совершенными с использованием информационно-телекоммуникационных технологий (далее – ИТТ), существует не так давно. При этом, функционирование и развитие компьютерных и телекоммуникационных технологий до сих пор не контролируется в достаточной мере. На этом фоне происходит активизация противоправных проявлений. Растет количественный показатель, проникновение «киберпреступности» практически во все сферы деятельности. Все это порождает новые вызовы и угрозы безопасности страны, кратно усиливая опасность данного явления, недооценка которой ведет к ослаблению позиций государства.

В качестве примера недавний инцидент, в результате которого хакеры, осуществив атаку на один из банков, похитили с его корсчета в Центральном банке России около 500 млн. руб.[2] Причиненный ущерб от одного этого преступления превысил весь материальный ущерб (339,5 млрд. руб.) от преступлений экономической направленности (по оконченным и приостановленным уголовным делам) за 2020 год.

«Современные информационные технологии широко используются в незаконном обороте наркотиков, пропаганде деструктивной идеологии, при совершении различного рода мошеннических действий, незаконных финансовых операций и других противоправных деяний»[3], совершаемых в том числе разными формами криминальной кооперации.

Приоритетность и наступательность в борьбе с организованной преступностью, криминальными лидерами, преступлениями, совершенными с использованием ИТТ, является важными задачами, которые систематически актуализируются главой государства и руководителями силовых ведомств. Возможной причиной этому является динамика сменяемости одних вызовов и угроз другими, что обусловливает необходимость постоянного совершенствования мер по их нейтрализации и ликвидации.

Одним из важных моментов в борьбе с организованной преступностью и преступлениями, совершенными с использованием ИТТ, является определение тенденций их развития.

Тенденции развития организованной преступности. За основу анализируемого массива статистических данных взят показатель, отражающий количественно зарегистрированных преступлений, совершенных в составе организованных групп и преступных сообществ (далее – ОГиПС). Во-первых, этот показатель не

---

[1] Постановление СНД СССР от 23.12.1989 «Об усилении борьбы с организованной преступностью» // Ведомости СНД СССР и ВС СССР. 1989. № 29. Ст. 576.

[2] Group-IB сообщила о хищении хакерами средств с корсчета банка в ЦБ // Официальный сайт ИД «КоммерсантЪ». URL: https://www. kommersant.ru/doc/5130099 (дата обращения: 15.12.2021).

[3] Выступление Министра внутренних дел Российской Федерации В.А. Колокольцева на расширенном заседании коллегии МВД России 28 февраля 2019 года // Официальный сайт МВД России. URL: https://mvd.ru/document/7393866/ (дата обращения: 12.12.2020).

относится к конкретным статьям действующего УК РФ. Во-вторых, затрагивает разные направления проявления организованной преступности и формы криминальной кооперации в России.

1. Рост числа зарегистрированных преступлений, начавшийся в 2017 году и сохраняющийся по настоящее время. Средний показатель прироста без учета данных 2021 года составил 9 % в годовом выражении: с 13 232 (2017) до 17 727 (2020) преступлений. За десять месяцев 2021 года указанный показатель, вырос более чем на 25,7 % (19 988) по сравнению с аналогичным периодом прошлого года. Фактически, рост данного показателя продолжается на протяжении 5 лет, что свидетельствует об относительной устойчивости данной тенденции и возможном ее сохранении в будущем, при отсутствии возникновения условий способных оказать влияние на данную тенденцию.

2. Изменение вектора со снижения (2009-2016 годы) на рост (с 2017 года по настоящее время), безотносительно к причинам данных изменений. Так, количество зарегистрированных преступлений сократилось с 36 601 в 2008 году до 12 581 в 2016 году, то есть, более чем в 2 раза (исключение составил 2012 год, показавший прирост на 1,7%. Вместе с тем, если сопоставить все периоды роста и снижения данного показателя, с учетом его роста в период с 1988 по 1991 годы, то за 33 года данный показатель снижался только в каждом третьем случае. Или в среднем, на один год снижения приходится два года роста. Таким образом, основным трендом является рост количества зарегистрированных преступлений совершаемых в составе ОГиПС.

3. Цикличность динамики: рост сменяется снижением, который затем сменяется ростом числа регистрируемых преступлений, и так далее.

4. Изменение характера цикличности динамики со скачкообразной (+27,1% в 1993, +36,7% в 1994 и +34,6% в 1996 годах) на поступательную (изменение не превышает 20%).

5. Рост удельного веса тяжких и особо тяжких преступлений, совершенных в составе ОГиПС в общем числе расследованных преступлений, который продолжается на протяжении последних нескольких лет. Например, если в 2016 году он составлял 5,0 %, то в 2020 году – 7,8 %. За десять месяцев 2021 года указанный показатель по сравнению с аналогичным периодом прошлого года составил 9,7%.

6. Рост общественной опасности организованной преступности. Подтверждением этого выступает эффект синергии от сохраняющихся на протяжении последних нескольких лет трендов связанных с ростом: во-первых, количества регистрируемых преступлений совершаемых ОГиПС; во-вторых, удельного веса тяжких и особо тяжких преступлений, совершенных в составе организованной группы или преступного сообщества в общем числе расследованных преступлений. Данное явление можно охарактеризовать не как негативное, а как опасное.

Тенденции развития преступлений, совершенных с использованием ИТТ:

1. Рост числа зарегистрированных преступлений, совершенных с использованием ИТТ, с 90,5 тыс. в 2017 году до 510,6 тыс. в 2020 году. Таким образом, фактическое количество преступлений увеличилось более чем в 5,5 раз

за 3 года. За 10 месяцев 2021 года данный показатель составил 454,6 тыс. преступлений, что больше показателя за аналогичный период на 8,1 %.

2. Формирование устойчивого тренда на изменение характера со скачкообразности роста на менее амплитудную поступательность: + 92,9 % в 2018, + 68,5 % в 2019, + 73,2 % в 2020 годах, то есть, если в период с 2018 по 2019 год скачек составил 24,4 %, то с 2019 по 2020 годы скачек не превышал 5 %.

3. Рост количества тяжких и особо тяжких преступлений в общем объеме преступлений, совершенных с использованием ИТТ, с 48,5 5% в 2019 году до 56,6 % за 10 месяцев 2021 года. То есть, фактически, усредненный рост данного показателя составил около 4 % в год, что можно охарактеризовать, как опасную тенденцию.

4. Снижение прироста вышеуказанного показателя со 149 % в 2019 году до 18,9 % за 10 мес. 2021 года, что можно охарактеризовать положительно. То есть, идет процесс замедления прироста количества зарегистрированных преступлений, совершаемых с использованием ИТТ.

5. Увеличение доли тяжких и особо тяжких преступлений в общем числе преступлений, совершенных с использованием ИТТ, с 8,8 % в 2018 году до 26,6 % за 10 мес. 2021 года. То есть, фактически, данный показатель вырос за 4 года на 17,8% или усредненный его рост составил около 4,5 % в год, что можно охарактеризовать, как опасную тенденцию.

6. Схожесть в направлении снижения темпов прироста таких показателей преступлений, совершенных с использованием ИТТ, как количество зарегистрированных преступлений, так и их тяжести. Снижение этих показателей, можно охарактеризовать положительно, так как это может свидетельствовать о коррекции процессов связанных с раскрываемостью данных преступлений.

Представленный перечень тенденций не является исчерпывающим[1].

Вместе с тем, осуществление подобного анализа, в основу которого положены статистические данные ГИАЦ МВД России, может помочь в:

- определении причинно-следственных связей, лежащих в основе изменений рассматриваемых направлений криминальной кооперации;
- подготовке прогнозов относительно дальнейшего развития оперативной обстановки в Российской Федерации;
- разработке возможных сценариев по принятию тех или иных мер реагирования, в зависимости от возникновения определенных условий.

Хочется надеяться, что представленные результаты проведенной работы будут учтены и использованы не только в научных исследованиях, но и при разработке практических мер.

[1] С учетом динамики изменений происходящих в окружающем нас мире, основная часть анализируемых статистических данных, на момент исследования, уже является историей, вчерашним отражением криминальной обстановки в обществе и государстве.

Е.А. Мухтарова

К вопросу об ограничении доступа несовершеннолетних к ресурсам сети Интернет, как альтернативной мере принудительного воспитательного воздействия

Аннотация. В статье автор рассматривает проблему об ограничении доступа несовершеннолетних к ресурсам сети Интернет, как альтернативной мере принудительного воспитательного воздействия. По его мнению, постоянное развитие интернет-технологий и их широкое проникновение в общество ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий.

Ключевые слова: несовершеннолетние, ответственность, принудительные меры воспитательного воздействия, интернет.

Использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьёзным вызовом, как для общества, так и для правоохранительных органов. От данных преступлений страдают все: люди, учреждения, организации, органы власти различных уровней[1].

Д. А. Керимов по данному поводу говорит следующее: «…чем глубже и более всесторонне познана внешняя среда, чем рациональнее использованы добытые знания, чем в большей мере они отражают назревшие потребности этой среды, тем выше теоретический уровень правотворчества, тем эффективнее действие правовых норм, тем оптимальнее достижение целей и задач правового регулирования»[2].

В. Н. Кудрявцев также указывает, что «важнейшей предпосылкой любой правотворческой деятельности – это анализ объективных общественных процессов (негативных и позитивных), определяющих как саму необходимость в принятии законодательства или практики его применения, так и конкретное содержание этих изменений»[3].

Постоянное развитие Интернет-технологий и их широкое проникновение в общество ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий.

---

[1] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2022. С. 3.

[2] Керимов Д.А. Методология права: Предмет, функции, проблемы философии права / Ин-т соц.-полит. исслед. Рос. акад. наук и др. М.: Изд-во Соврем. гуманитар. ун-та, 2003. с. 9-10.

[3] Кудрявцев В. Н. Закон, поступок, ответственность / Репр. воспр. изд. 1986 г. Москва: Норма: ИНФРА-М, 2017. С. 100.

Дифференциация уголовной ответственности является ключевым направлением развития уголовного законодательства Российской Федерации в решении отечественного механизма уголовно-правовой охраны к условиям информационного общества. Отечественная доктрина уголовного права характеризуется наличием целого ряда фундаментальных исследований сущности, видов, средств и критериев дифференциации уголовной ответственности[1].

Т.А. Лесниевски-Костаревой дает классическое определение дифференциации уголовной ответственности как «градацию, разделение, расслоение ответственности в уголовном законе, в результате которой законодателем устанавливаются различные уголовно-правовые последствия в зависимости от типовой степени общественной опасности преступления и личности виновного»[2].

С 2006 года федеральными органами государственной власти Российской Федерации осуществляется целенаправленная деятельность, связанная с ограничением в образовательных организациях доступа обучающихся к негативной информации.

Министерство образования и науки Российской Федерации в 2006 году разработало методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих ограничение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания[3].

Уголовное законодательство в нашей стране предусматривает более лояльное отношение к лицам, совершившим преступления, будучи несовершеннолетними. Указанное обусловлено тем, что в силу возраста и малого жизненного опыта подростки нуждаются, прежде всего, в воспитательной коррекции поведения, для чего не требуется их изоляция от общества.

Главой 14 УК РФ предусматриваются специальные виды освобождения несовершеннолетних от уголовной ответственности и наказания: освобождение несовершеннолетних от уголовной ответственности с применением к ним принудительных мер воспитательного воздействия (ст. 90 УК РФ);

---

[1] См.: Васильевский А.В. Дифференциация уголовной ответственности и наказания в Общей части уголовного права: дис. … канд. юрид. наук. Ярославль, 2000; Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: дис. ... д-ра юрид. наук. М., 1999; Рогова Е.В. Учение о дифференциации уголовной ответственности: дис. ... д-ра юрид. наук. М., 2014 и др.

[2] Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: Теория и законодат. практика / Т. А. Лесниевски-Костарева; Ин-т законодательства и сравн. правоведения при Правительстве РФ. М.: НОРМА, 1998. VIII, С. 52:

[3] Письмо Минпросвещения России от 07.06.2019 № 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»).

освобождение несовершеннолетних от наказания с применением к ним принудительных мер воспитательного воздействия (ст. 92 УК РФ)[1].

Принудительные меры воспитательного воздействия могут быть применены к лицам, не достигшим возраста 18 лет, при наличии двух условий:

- если совершенное преступление относится к категории небольшой или средней тяжести,
- если данные о личности позволяют суду сделать вывод о том, что исправление виновного может быть достигнуто путем применения принудительных мер воспитательного воздействия.

Указанный в ч. 2 ст. 90 УК РФ перечень видов принудительных мер воспитательного воздействия является исчерпывающим. Выбор конкретной меры воспитательного воздействия осуществляется судом с учетом мотивов совершенного несовершеннолетним преступления, его поведения после содеянного, а также с учетом того, применялись ли к нему ранее вышеперечисленные меры и какие именно. Возможно применение к несовершеннолетнему нескольких мер одновременно.

Компетенция, полномочия и регламенты применения мер воспитательного воздействия – это вопросы, урегулированные законодательством РФ[2]. В соответствии с законодательством принудительные меры воспитательного воздействия могут применяться к несовершеннолетним Комиссиями по делам несовершеннолетних и защите их прав вне отношений уголовной ответственности в целях предупреждения их правонарушений, обеспечения социального контроля за несовершеннолетними с отклоняющимся поведением.

Уголовное право заинтересовано в совершенствовании мер воспитательного воздействия[3], но не решает этой задачи по существу. Оно лишь использует меры государственного не уголовного принуждения иной отраслевой принадлежности в качестве предупредительной гарантии в случае освобождения несовершеннолетнего от уголовной ответственности или наказания.

Конституция РФ ст.29 п.4 гласит: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»[4].

Рано или поздно, подросток и социальные сети встречаются. По разным данным, несовершеннолетние начинают проявлять интерес к социальным сетям

---

[1] Уголовно-правовое воздействие: монография / Г.А. Есаков, Т.Г. Понятовская, А.И. Рарог и др.; под ред. А.И. Рарога. М.: Проспект, 2012. 288 с.

[2] Федеральный закон от 24.06.1999 № 120-ФЗ (ред. от 24.04.2020) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // Собрание законодательства РФ. 1999. № 26. Ст. 3177.

[3] См.: Поводова Е.В. Принудительные меры воспитательного воздействия: Проблемы теории и правового регулирования: автореферат дис. ... кандидата юридических наук: 12.00.08 / Моск. гос. юрид. акад. Москва, 2005. 31 с.

[4] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). UPL: http://www.pravo.gov.ru 04.07.2020 (дата обращения: 26.01.2022).

достаточно рано. Они открывают для себя самые популярные площадки: «вконтакте» и «одноклассники».

У большинства людей понятия «преступление», «преступник» ассоциируются, в первую очередь, с насилием, хищением имущества либо незаконными действиями с наркотиками. Однако Уголовный кодекс РФ содержит гораздо больший перечень деяний, которые признаются преступлениями и влекут ответственность в установленном порядке. Для того, чтобы совершить некоторые из них, вовсе не обязательно иметь изначально криминальные наклонности, и более того, их можно совершить путем использования Интернета.

Даже высказывание на форуме или в социальной сети, обращенное к неопределенному кругу лиц, может быть расценено как преступление, если содержит в себе запрещенные законом призывы либо суждения.

Между тем, многие считают, что в Интернете можно позволить себе больше свободы в выражениях, нежели в реальной жизни, так как есть возможность общаться анонимно. Это не так, поскольку у правоохранительных органов имеются технические средства для установления устройства (компьютера, планшета, телефона), с которого отправлена та или иная информация в сеть, а также лица, которому это устройство принадлежит. Судебная практика насчитывает множество примеров, когда люди понесли уголовную ответственность за деяния, совершенные при помощи Интернета.

Более того, некоторые статьи уголовного закона предусматривают более суровую ответственность именно за те преступления, которые совершены при помощи информационно-телекоммуникационных сетей, поскольку в Интернете круг лиц, которые могут прочитать либо посмотреть то или иное информационное сообщение, гораздо шире, чем мог быть при простом публичном выступлении, а, следовательно, общественная опасность таких действий более серьезная.

Следует отметить, что, общаясь в сети, свобода слова, установленная Конституцией РФ, небезгранична, и неосторожные высказывания могут повлечь очень серьезные последствия. Кроме того, незнание закона не освобождает от ответственности, поэтому каждый гражданин должен ознакомиться с положениями УК РФ.

Литература

1. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М.: ИНФРА-М, 2022.
2. Керимов Д.А. Методология права: Предмет, функции, проблемы философии права / Ин-т соц.-полит. исслед. Рос. акад. наук и др. М.: Изд-во Соврем. гуманитар. ун-та, 2003.
3. Кудрявцев В. Н. Закон, поступок, ответственность / Репр. воспр. изд. 1986 г. Москва : Норма : ИНФРА-М, 2017.

4. Васильевский А.В. Дифференциация уголовной ответственности и наказания в Общей части уголовного права: дис. … канд. юрид. наук. Ярославль, 2000.
5. Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: дис. ... д-ра юрид. наук. М., 1999.
6. Рогова Е.В. Учение о дифференциации уголовной ответственности: дис. ... д-ра юрид. наук. М., 2014.
7. Лесниевски-Костарева Т.А. Дифференциация уголовной ответственности: Теория и законодат. практика. М.: НОРМА, 1998.
8. Уголовно-правовое воздействие: монография / Г.А. Есаков, Т.Г. Понятовская, А.И. Рарог и др.; под ред. А.И. Рарога. М.: Проспект, 2012.
9. Поводова Е.В. Принудительные меры воспитательного воздействия: Проблемы теории и правового регулирования: автореф. дис. ... канд. юрид.наук. М., 2005.

С.А. Нестерович, Ю.И. Купцова

Влияние информации из сети Интернет на безопасность детей и подростков в России

Аннотация. В данной статье рассматривается негативное влияние информации из сети «Интернет» на несовершеннолетних. Выявляются формы и причины девиантного поведения, предлагается введение ряда профилактических мер. Проводится анализ некоторых положений Концепции информационной безопасности детей.

Ключевые слова: социализация, подростки, девиантное поведение, суицид, информация, безопасность, зависимость, причины, профилактика.

В настоящее время информационные каналы, в связи с постоянным наращиванием скорости передачи и объемов информации, стали еще более доступными и открытыми для изучения. В связи с большим объемом деструктивного контента в сети, растет уровень недовольства и агрессивности подростков. Погружаясь ежедневно в эту среду, у подростков стираются грани между реальной жизнью и виртуальной. Как результат, мы получаем новые формы девиантного поведения[1]: буллинг, троллинг, суицидальные квесты, скулшутинг, колумбайн и тд.

В Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р (далее Концепция), указано, что сеть «Интернет» стала частью процесса социализации, дополнением традиционных институтов семьи и школы.

Одновременно с этим информационные технологии становятся не дополнением вышеуказанных институтов, а полным их замещением. Такая ситуация становится возможной, когда родители сознательно или не осознанно

[1] Девиантное поведение (лат. deviation — отклонение) — устойчивое поведение личности, отклоняющееся от общепринятых, наиболее распространённых и устоявшихся общественных норм.

уклоняются от своих прямых обязанностей по воспитанию и развитию ребенка, полагаются на педагогов, психологов образовательных учреждений. С детства родители компенсируют недостаток внимания дорогими гаджетами. При этом, отсутствует контроль с их стороны по возрастному критерию посещаемых сайтов и скаченных игр.

В рассматриваемой Концепции ответственность семьи за соблюдение законных интересов детей в информационной сфере не предусматривается, её несет государство. Следовательно, государство также должно обеспечить информационную безопасность детей и подростков в сети «Интернет». В Концепции же указано, что «обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи».

В этой связи, «важнейшей задачей является налаживание согласованного взаимодействия семьи, главного института социализации и воспитания детей, с государством и всеми элементами современного медиарынка – производителями и распространителями контента, психолого-педагогическими экспертными сообществами и экспертными сообществами в области художественного образования».

Согласно статистическим данным, приведенным Советом безопасности, за 6 месяцев 2021 года выявлено 3064 попытки самоубийств и суицидов среди подростков. В аналогичном периоде прошлого года - 2146 случаев. Эксперты полагают, что рост числа самоубийств во многом связан с пропагандой в социальных сетях опасного контента.[1]

Воздействие осуществляется по средствам воспроизведения музыкальных произведений, компьютерных и ролевых игр, рассказов и разного рода диалогов, угнетающих и подавляющих детскую психику, создающих общий депрессивный фон в сообществах, развивая у подростков мысль о совершении суицида. Подростковый суицид имеет такие характерные особенности, как отсутствие реального желания и четко обозначенного мотива совершения самоубийства.

Также, прослеживается зависимость подросткового поколения от мнения общества, реализуемого в сети «Интернет» в виде «лайков» и «подписок». Для их получения, подростки подвергают себя и окружающих опасности, при этом фиксируют свои действия при помощи различных видеоустройств, и размещают материал в популярных социальных группах и медиаплатформах. Так, в 2017 году была популярна игра «Беги или умри». Дети перебегали дорогу перед движущимся автомобилем в последний момент и фиксировали это на видео.

Одновременно с этим, компания Google привлечена к административной ответственности по ст. 13.41 КоАП РФ на общую сумму 32.5 млн. руб. в связи с большим количеством не удаленного противоправного контента на своих интернет - ресурсах. На 25 октября 2021 года количество материалов составляло 2650. Ранее в апреле проходила видеоконференция по аналогичному вопросу,

[1] Е. Герасимова. «В России растет число преступлений против детей». URL:https://www.ng.ru/education/2021-12-08/8_8321_children.html.

где по представленным данным за период с 2012 по 2021 год было выявлено 5746 материалов деструктивного не удаленного контента.

Блокировке подлежат ресурсы, содержащие уголовно – наказуемые материалы в целом, и в частности, такие как открытое оправдание терроризма и экстремистской деятельности, призывы к её осуществлению, трансляция материалов, содержащих нецензурную брань, культ насилия и жестокости, места приобретения наркотиков и их аналогов, рецепты изготовления и т.д.

Ряд экстремистских роликов до настоящего времени находятся в YouTube в открытом доступе более 3 лет. Согласно законодательства Российской Федерации, подобные материалы должны быть удалены не позднее суток с момента поступления обращения Роскомнадзора.[1]

Вспомним трагические события в мае 2021 года в Казани и в сентябре 2021 года в Перми. Скулшутеры 17-18 лет находясь в помещениях образовательных учреждений, открыли стрельбу по школьникам, студентам и преподавателям. Следствием установлено, что они оба состояли в деструктивных сообществах в социальных сетях.

В связи с этим, необходимо пересмотреть систему профилактических мероприятий, направленных на выявление и блокирование сайтов в интернет-пространстве и усилить контроль за их исполнением.

В рамках профилактической работы, Московская городская межведомственная комиссия по делам несовершеннолетних и защите их прав, Главное следственное управление СК России по г. Москве, коллектив специалистов факультета Юридической психологии и Центра экстренной психологической помощи Московского государственного психолого – педагогического университета, для сотрудников образовательных организаций, разработана профилактическая программа по снижению виктимного поведения учащихся. В нее включены методические материалы по признакам девиаций[2], действиям специалистов системы образования в ситуациях социальных рисков и профилактике девиантного поведения обучающихся.[3]

С целью профилактики, инспекторы подразделений по делам несовершеннолетних посещают учебные заведения, проводят профилактические беседы на темы существующих опасностей при пользовании сетью «Интернет».

Кроме того, в настоящее время активно создаются такие общественные движения и организации как «Лига безопасного интернета»[4], требующая поддержки со стороны государства, для дальнейшего развития и качественного выполнения своих задач.

Целесообразно введение периодического планового медицинского и психологического обследования в образовательных учреждениях, направленные

[1] Официальный интернет – портал правовой информации. URL: duma.gov.ru.

[2] Девиа́ция (от лат. deviatio — отклонение): в естественных науках — отклонение параметров от нормы.

[3] Официальный интернет – портал правовой информации. URL: https://mgppu.ru/about/publications/deviant_behaviou.

[4] Официальный интернет – портал правовой информации. URL: https://ligainternet.ru.

на установление детей «группы риска» и наличие у них аутоагрессивных повреждений.

Необходимо ведение поэтапной работы с детьми и их родителями, предполагающей разработку индивидуальных программ реабилитации. Цель: устранение недопонимания между подростками и родителями, формирования доверительных, уважительных и доброжелательных отношений в семье. Сама программа должна быть направлена на общее повышение стрессоустойчивости ребенка, развитие адекватной самооценки, повышение культуры в области норм права.

Для продвижения разумных, интересных жизнеутверждающих советов, правил и инструкций, которые будут излагаться подростковому поколению и их родителям известными медийными личностями, простым и понятным языком, можно использовать популярный видеохостинг YouTube.

На данном канале опубликован фильм, где экскурсоводом является генеральный директор Третьяковской галереи Зельфира Трегулова, а в качестве гостя был приглашен Сергей Шнуров. Фильм с его участием набрал около 1 млн. 100 тыс. просмотров. Другие фильмы канала имеют 290 тыс. количества просмотров. Использование подобного не стандартного приема, позволило расширить границы знаний подростков, пробудить интерес к истории объектов культурного наследия.

Детский омбудсмен при президенте РФ Мария Львова – Белова внесла инициативу по созданиям бесплатных досуговых центров для детей и подростков. Предполагается, что коллектив такого центра будет состоять из активных молодых вожатых, психологов и социальных педагогов.

Выявленные проблемы в настоящее время актуальны и критичны. Необходимо уже сейчас принимать решительные меры, направленные на недопущение деградации, ожесточенности подрастающего поколения, повышение качества жизни и значительного уменьшения статистики детской смертности.

Литература

1. Банников Г. С., Вихристюк О. В., Миллер Л. В., Синицына Т. Ю. Методические рекомендации (памятка) психологам образовательных учреждений по выявлению и предупреждению суицидального поведения среди несовершеннолетних. М.: ГБОУ ВПО МГППУ, 2013, С. 11, 19
2. Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р
3. Соломатина Е.А., Трощанович А.В., Черкасова Л.И. Особенности расследования доведения до самоубийства несовершеннолетних: учебно – методическое пособие. М., 2014. С. 11.
4. Тарасенкова А.Н. Интернет: правовые аспекты безопасного использования. М, 2017, С.144 – 146.

М.М. Савченко

Причины латентности хищений денежных средств, совершаемых с использованием цифровых банковских технологий

Аннотация. В статье проводится исследование динамики хищений денежных средств, совершенных с использованием современных цифровых технологий. Проводится оценка уровня латентности преступлений в данной сфере. Определяются причины латентности, формулируются предложения по противодействию преступлениям в сфере цифровых технологий.

Ключевые слова: хищения денежных средств; цифровая преступность; банковские технологии; несанкционированные банковские операции; латентная преступность; банковское мошенничество.

В последние годы в России наблюдается стремительное развитие дистанционных и других цифровых технологий, предлагаемых банками для своих клиентов в рамках банковского обслуживания. Количественный и качественный рост объемов операций с применением вышеуказанных технологий, влияет на повышение привлекательности данного сектора со стороны преступного сообщества.

Анализ тенденций развития современных и дистанционных банковских технологий в контексте их влияния на динамику и структуру хищений в банковской сфере является предметом изучения многих исследователей[1][2][3]. В последние годы уделяется внимание также криминологическим аспектам, связанным с изучением латентности, причин роста преступности в банковской сфере в условиях развития современных цифровых технологий[4][5].

При анализе сообщений о преступлениях необходимо учитывать их уровень латентности, который связан с нежеланием потерпевших по различным причинам обращаться в правоохранительные органы, а также в некоторых случаях с ненадлежащей работой правоохранительных органов в части регистрации сообщений о преступлениях и их проверке.

---

[1] Долганов С. И. Банковское мошенничество в период пандемии COVID-19 // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года, Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020. С. 256-259

[2] Трунцевский Ю. В. Современные вызовы банковского мошенничества финансовому обеспечению электронной коммерции / Ю. В. Трунцевский // Банковское право, 2020, № 6. С. 28-36.

[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] Машлякевич В. А Латентность мошенничеств, совершаемых с использованием средств телефонной связи: криминалистический аспект // Вестник Барнаульского юридического института МВД России, 2019, № 2(37). С. 129-130.

[5] Астафьев К. В. К вопросу о причинах высокой латентности мошенничества // Социально-экономические и технические системы: исследование, проектирование, оптимизация, 2006, № 10. С. 4.

Согласно статистике Банка России[1] за последние десять лет стремительно 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 38670,3 млн. (29495,5 млрд. руб.) в 2020 году – то есть частота использования электронных средств платежа увеличилась более чем в 38 раз. В 2020 году доля платежей с использованием платежных карт достигла 55,9% в совокупном объеме розничного товарооборота[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.

Банк России ведет статистику таких операций на основании сведений, представленных отчитывающимися операторами по переводу денежных средств и операторами услуг платежной инфраструктуры с 2015 года. В период с 2015 года по 2018 год в статистику включались «несанкционированные переводы денежных средств». С 2019 года в соответствии с изменениями законодательства[3] Признаки таких операций утверждены приказом Банка России от 27 сентября 2018 г. № ОД-2525[4].

В 2019-2020 гг. продолжалась тенденция увеличения числа и объема рассматриваемых операций. Однако, доля операций без согласия клиентов в общем объеме таких осуществленных операций существенно не менялась. Так, за 2020 год доля операций без согласия клиента в общем объеме операций по переводу денежных средств составила 0,00117% (в 2019 году – 0,00089%).

При анализе количества операций, совершенных без согласия клиентов, наблюдается постоянный рост доли таких операций, совершенных с использованием социальной инженерии. Так, например, в 2019 году среди операций по оплате товаров и услуг в Интернете доля таких операций была зафиксирована 74%, в 2020 году – 64%. По операциям с использованием ДБО физических лиц в 2019 году доля составила – 87%, в 2020 году – 82%.

Рассматриваемая статистическая информация, основанная на данных, представленных банками и иными платежными агентами, по нашему мнению, с достаточной достоверностью отражает фактическое количество и объем преступных посягательств, на денежные средства с использованием цифровых технологий. Причиной является тот факт, что практически за каждым таким случаем следует клиентское обращение в банк, совершаемое с требованием возврата незаконно перечисленных денежных средств либо содействия таковому.

---

[1] Банк России. Статистика национальной платежной системы. https://www.cbr.ru/statistics/nps/psrf/.

[2] СберИндекс. Итоги 2020 года https://www.sberbank.ru/common/img/uploaded/files/pdf/analytics/itogi2020.pdf.

[3] Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» // СПС «КонсультантПлюс».

[4] Приказ Банка России от 27 сентября 2018 г. № ОД-2525// СПС «КонсультантПлюс»

Для более детального рассмотрения данного вопроса необходимо провести исследование объемов, структуры и динамики преступных посягательств, совершенных с использованием современных цифровых технологий, регистрируемых правоохранительными органами. С этой целью были использованы данные статистики, представленные Главным управлением правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации в виде ежемесячных отчетов и Формы федерального статистического наблюдения № 4-ЕГС, а также ведомственного отчета МВД России формы 1-А[1].

На основании изученных данных можно сделать вывод о том, что за рассматриваемый период общее количество зарегистрированных тайных хищений чужого имущества значительно не меняется. Есть определенные сезонные колебания, повторяемые ежегодно, которые, в основном, связаны с увеличением количества квартирных краж в летние месяцы.

В то же время можно наблюдать значительный рост хищений, совершенным путем обмана и злоупотребления доверием: так, в 1 квартале 2018 года было зарегистрировано 54667 по статьям «мошенничество», в 4 квартале 2020 года по данной группе статьей зарегистрировано 88039 преступлений, что означает рост более чем на 61 процент.

Анализ представленных данных позволяет сделать вывод о том, что в общей структуре краж наблюдаются определенные изменения. Так, за период 2018 – 2020 год, происходит значительный рост тайных хищений денежных средств, совершенных с использованием ИКТ: с 4942 в 1 квартале 2018 года до 49008 в 4 квартале 2020 года – то есть почти в 10 раз, при этом доля краж с использованием ИТТ в их общем количестве в последний квартал 2020 года составила более 25%.

Проведенный анализ демонстрирует рост числа зарегистрированных хищений за счет деяний, совершенных с использованием обмана и злоупотребления доверием потерпевших. Данную тенденцию можно объяснить следующими факторами, значительно облегчающими преступную деятельность, с одновременным снижением возможностей правоохранительных органов по установлению личности виновных:

- виновное лицо действует дистанционно, не имеет личного прямого контакта с потерпевшим, в связи с чем, не может быть идентифицировано;
- затруднено установление фактического местонахождения лица, совершающего хищение;
- неудавшиеся попытки хищений, имеющие признаки покушения на преступление, чаще всего не фиксируются, поэтому совершаются в несравнимо большем количестве, чем завершенные инциденты.

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.

---

[1] Генеральная прокуратура Российской Федерации. Портал правовой статистики. http://crimestat.ru/analytics.

Для оценки уровня латентности хищений денежных средств с банковских счетов проведено сопоставление информации о зарегистрированных преступлениях (кражи и мошенничества, совершенные с использованием ИТТ) со сведениями об операциях без согласия клиентов, фиксируемых платежными операторами (рис. 1).

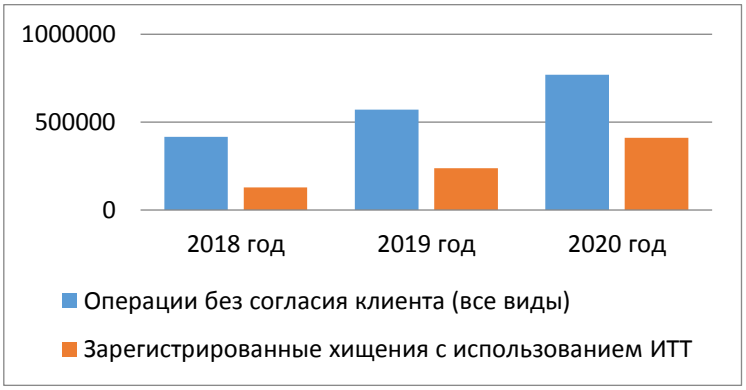


Рис. 1 – Сравнение общего количества операций без согласия клиентов (по сведениям платежных агентов) и зарегистрированных хищений с использованием ИТТ.

На основании сведений, представленных на диаграммах, можно сделать вывод об уровне латентности преступлений в рассматриваемой сфере: в 2018 году – 69%, в 2019 году – 58,5%, в 2020 году – 46,7%. Таким образом, при общем росте обоих показателей, уровень латентности таких преступлений снижается.

В качестве причин латентности преступлений, совершенных методами социальной инженерии, можно выделить следующие:

- нежелание потерпевших обращаться в правоохранительные органы по причине отсутствия доверия к возможностям раскрытия данных преступлений;
- в силу незначительности ущерба, нежелание нести временные и моральные затраты;
- нежелание предавать огласке факт посягательства.

Рост числа случаев обращения может быть связан с политикой финансовых организаций – платежных агентов, направленной на побуждение потерпевших-клиентов обратиться в правоохранительные органы с целью исключения неправомерных действий со стороны клиентов.

Выявленная тенденция по увеличению доли зарегистрированных преступлений в рассматриваемой сфере, что говорит о снижении их уровня латентности. Данная тенденция способствует накоплению и систематизации информации относительно способов совершения преступлений; позволяет разрабатывать и реализовывать более эффективные меры по предупреждению, пресечению и раскрытию таких хищений.

Литература

1. Астафьев К. В. К вопросу о причинах высокой латентности мошенничества // Социально-экономические и технические системы: исследование, проектирование, оптимизация, 2006, № 10, С. 4.

2. Банк России. Статистика национальной платежной системы. https://www.cbr.ru/statistics/nps/psrf/.
3. Генеральная прокуратура Российской Федерации. Портал правовой статистики. http://crimestat.ru/analytics.
4. Долганов, С. И. Банковское мошенничество в период пандемии COVID-19 // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года, Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020. – С. 256-259.
5. Машлякевич, В. А Латентность мошенничеств, совершаемых с использованием средств телефонной связи: криминалистический аспект // Вестник Барнаульского юридического института МВД России, 2019, № 2(37), С. 129-130.
6. Приказ Банка России от 27 сентября 2018 г. № ОД-2525// СПС «КонсультантПлюс».
7. 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.
8. СберИндекс. Итоги 2020 года https://www.sberbank.ru/common/img/uploaded/files/pdf/analytics/itogi2020.pdf.
9. Трунцевский, Ю. В. Современные вызовы банковского мошенничества финансовому обеспечению электронной коммерции / Ю. В. Трунцевский // Банковское право, 2020, № 6, С. 28-36.
10. Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» // СПС «КонсультантПлюс».

Э.С. Сарыгина, И.Н. Озеров

Цифровая гигиена и цифровая санитария в аспекте информационной безопасности молодого поколения

Аннотация. В статье поднимаются проблемы безопасности молодого поколения в свете цифровизации и информатизации общества страны и на глобальном мировом уровне. Новые веяния времени требуют понимания о происходящих новых формаций в обществе, при которых должны быть сохранены адекватные механизмы межличностных взаимоотношений на основе соблюдения высокой нравственности, морали и этики, особенно молодым поколением. Предметом исследования являются закономерности формирования правил поведения в аспекте информатизации молодого поколения, соблюдение которых направлено на повышение безопасности личности. Объектом исследования являются практика поведения молодого поколения в информационной среде. Дифференцированный подход социальных групп и поколений во взаимосвязи с правилами поведения в информационном пространстве должен позволить разграничить цифровую гигиену и цифровую санитарию. Под цифровой гигиеной, мы полагаем понимать, такое поведение личности конкретной социальной

группы, которое направлено на недопущение распущенности и неадекватного поведения в информационной среде. Цифровая санитария представляет собой деятельность по выработке правил, алгоритмов и норм поведения в информационной среде для личности конкретной социальной группы на основе методов междисциплинарного подхода. Без соблюдения цифровой гигиены и цифровой санитарии как основ безопасности в информационной среде личностью, группами людей, поколениями невозможно сохранять цифровое здоровье всех поколений.
Ключевые слова: цифровая гигиена, цифровая санитария, концепция информационной безопасности, цифровое здоровье поколения, информационная безопасность молодого поколения.

Тенденции развития механизмов регулирования общественных отношений в информационной сфере, обусловливают необходимость выработки механизма защиты личностей и их социальных групп от проявления информационных угроз, посягательств, в том числе на национальном уровне, безопасности страны в аспекте происходящей новой формации общества и общественных отношений. Это особенно актуально в условиях всё большей аномии сверхсовременного общества в условиях которой индивидуумы склонны ориентироваться на индивидуальные экономические цели и теряют способность организовываться для решения общих задач.

Дестабилизация информационной инфраструктуры через информационно-техническое воздействие в «военных» целях зарубежными странами, предвзятая оценка отечественной государственной политики иностранными СМИ, информационное воздействие террористическими и экстремистскими организациями, иллюзии безнаказанности компьютерной преступности могут формировать представление о слабо развитой институции как обеспечения информационной безопасности, осуществление которой может и должно строится на консолидированном подходе, сочетающим законодательную, правоприменительную, правоохранительную, судебную, контрольную и других форм деятельности государственных органов во взаимодействии с гражданами и социальными группами различных поколений более либо менее вовлеченными в информатизацию общественных отношений.

Интерес к информационной безопасности обусловлен внедрением средств информационных коммуникаций между людьми, осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесён ущерб путём воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Современная жизнь плотно связана с интернет-пространством. Обычным делом сегодня является покупка любого товара или получение услуг через Интернет.

Этому способствует чрезвычайная динамика общественных отношений, виртуализация коммуникации как между индивидами, так и с государственно-властными структурами, широчайшие возможности для получения различных данных в информационном пространстве, их обработки и самостоятельного анализа, построения прогнозов при помощи программных продуктов,

способность практически беспрепятственно делиться в информационном пространстве своими мнениями и убеждениями, объединяться в группы, мобильно координировать свою деятельность в оффлайне и т.п.

Информационно-коммуникационные технологии и их проникновение в жизнь людей фактически перевернули прежние устои социума, основанные преимущественно на постфигуративной культуре (подрастающее поколение учится у старших, живет по их моделям поведения), перейдя к установкам, характерным для кофигуративной (опыт приходится перенимать у сверстников) и префигуративной (старшие вынуждены перенимать опыт у младших) культур.

Можно согласиться с мнением М. Мид[1], что кризис постфигуративной системы наступил вследствие развития новых форм техники, не известных старшим. В данном случае таким своего рода технологическим триггером выступили цифровые технологии. Цифровая эпоха принесла с собой глубинные изменения в сознании общества и характере социальных связей. Укрепились модели, при которых молодежь сама вырабатывает стандарты поведения (социальные нормы), становящиеся образцом, как для сверстников, так и во многом для старшего поколения. В частности, успешность в современном мире исчисляется размером доходов, состояния индивида, занимаемой им должностью и соответственно, местом в социальной иерархии, сколько оценкой его представленности в виртуальном пространстве – просмотрами связанного с ним (в том числе созданного им) контента в виртуальном пространстве, количеством подписчиков блога, полученными «лайками».

Нередко именно нестандартные, новые решения приводят современных людей к желаемому результату. Вследствие этого молодежь во многом игнорирует стереотипы поведения старших поколений или безразлично относится к ним. Авторитет старших становится объектом критического оценивания. Параллельно происходят изменения в структуре важных социальных установок в сфере взаимодействия людей. Постепенно снижается значение привычной иерархичности, вертикальные связи уступают место горизонтальным, а субординация координации. Представляется, что эти процессы экстраполируется и на отношение к власти. Долгосрочное наблюдение реакции интернет-пользователей (комментарии, блоги и т.п.) на различные информационные провокации, связанные с деятельностью официальных структур, дают повод предположить, что в настоящее время институты власти преимущественно оцениваются с позиций полезности, удобства для конкретного индивида, близкой ему социальной группы. Из общественного сознания постепенно уходят последние отголоски сакрализации власти как явления. На первый план выходит бюрократический, технологический и утилитарный аспекты. Государственной власти в меньшей степени хотят просто подчинятся, от нее ожидают взаимодействия по понятным и выгодным алгоритмам. Индивид видит себя чаще самостоятельным гражданином – выгодополучателем. Он требует, прежде всего, признания его самого (как самостоятельной личности), ценности его прав, интересов, воззрений и переживаний.

[1] Мид, М. Культура и мир детства / М. Мид. – М.: Наука, 1988. с. 322–361.

Решая эту проблему, ведутся постоянные научные поиски ведущих ученых различных областей знания. Например, А.А. Алиева обращала внимание на правила поведения и безопасности старшим поколением в цифровой среде[1]: не выкладывать личную информацию (адрес, родной город, дату рождения и т. д.) в сеть «Интернет», поскольку мошенники могут воспользоваться этой информацией в корыстных целях путем использования незамысловатых преступных схем; не выкладывать в социальные сети фотографии, сделанные в своей квартире; не принимать заявки «в друзья» от незнакомых лиц и не отвечать им в социальных сетях, не скачивать файлы, поступившие в социальные сети с незнакомых аккаунтов; необходимо регулярно менять пароли в социальных сетях, посещать только проверенные сайты, а также установить на свой компьютер антивирус, чтобы создать всевозможные преграды для совершения преступления различными мошенниками.

Становится очевидным то, что степень вовлеченности поколений и социальных групп в происходящую цифровизацию различна, существующая практика поведения особенно молодых людей в информационной среде вызывает обеспокоенность. И.А. Молодцова и Л.П. Сливина с медицинской точки зрения поднимали проблемы информационной гигиены на примере адаптации Z-поколений к цифровой среде. Как отмечали ученые, в современных условиях на фоне больших психологических нагрузок, активного использования цифровых технологий появился новый фактор риска нарушений здоровья – информационный; на фоне роста традиционных заболеваний возникли новые информационно-зависимые синдромы[2]. Вместе с тем, выделяют элемент цифровой культуры личности такой как информационную гигиену, под которой понимают систему мер сопровождения индивидуума при формировании, реализации и развитии ключевых компетенций цифровой «жизни»[3]. Очевидно, что это междисциплинарная новая отрасль научного знания, взаимосвязанная с гигиеной, физиологией, биологией, биохимией, математикой, физикой, информатикой, психологией, информационной безопасностью, конфликтологией и другими науками[4].

Новые веяния времени требуют понимания о происходящих иных формаций в обществе, при которых должны быть сохранены адекватные механизмы межличностных взаимоотношений на основе соблюдения высокой нравственности, морали и этики. Вместе с тем, требуется изучение

---

[1] Алиева, А. А. Цифровая гигиена для старшего поколения / А. А. Алиева, П. Ф. Иванова // Сборник научных трудов по итогам конкурсов научных работ: материалы конкурсов научных работ, проведенных Кузбасским институтом ФСИН России в 2020-2021 учебном году. – Новокузнецк: Кузбасский институт Федеральной службы исполнения наказаний, 2021. – С. 6-7.

[2] Максимова, Е. А. Информационная гигиена как фактор предотвращения последствий z-цифровизации / Е. А. Максимова, И. А. Молодцова, М. В. Бердник // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(29). – 20 с. – DOI 10.14529/SECUR180311.

[3] Там же.

[4] Там же.

формирования правил поведения в аспекте информатизации особенно молодого поколения, соблюдение которых было бы направлено на повышение безопасности личности. Возникающая множественность субъектов, стремящихся доминировать в освоении и внедрении цифровых технологий, приводит к ускорению перемен в жизни общества. Это провоцирует ситуацию, когда привычные для общества модели поведения и институты, определяющие его развитие на протяжении длительного периода времени, утрачивают свою актуальность намного быстрее, оказываясь не способными своевременно принимать необходимые решения и шаги для предупреждения рисков.

Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Утверждена Доктрина информационной безопасности в Российской Федерации, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Другой аспект проблемы, это подготовленность самого общества, социальных групп, гражданина и личности, его вооруженность и сплочённость перед проблемами цифровой сферы, возможных угроз, участию и соучастию в обеспечении информационной безопасности. Полагаем, что в этом ракурсе целесообразно говорить о цифровом здоровье, не с точки зрения медицины, а междисциплинарно, где факторы риска нарушений здоровья цифровой среды также будут контентные, коммуникационные, технические, зональные, психо-эмоциональные и многие другие.

Дифференцированный подход социальных групп и поколений во взаимосвязи с правилами поведения в информационной среде должен позволить разграничить цифровую гигиену и цифровую санитарию. Мы полагаем, что цифровая гигиена – это такое поведение личности конкретной социальной группы, которое направлено на недопущение распущенности и неадекватного поведения в информационной среде. Цифровая санитария представляет собой деятельность по выработке правил, алгоритмов и норм поведения в информационной среде для личности конкретной социальной группы на основе методов междисциплинарного подхода. Без соблюдения цифровой гигиены и цифровой санитарии как основ безопасности в информационной среде личностью, группами людей, поколениями невозможно сохранять цифровое здоровье всех поколений.

Итак, пока граждане и социальные группы людей накапливают негативный опыт по соблюдению цифровой гигиены, дают советы по санитарии в сфере цифровой реальности, которые не имеют отношение к общепризнанным правилам, остается надеется на новый формат работы в аспекте информационной безопасности. При этом «новый формат» в текущей ситуации должен быть связан с четким пониманием тех рисков, которые формируются в эскалирующем развитии цифрового общества.

Литература

1. Алиева, А. А. Цифровая гигиена для старшего поколения / А. А. Алиева, П. Ф. Иванова // Сборник научных трудов по итогам конкурсов научных работ:

материалы конкурсов научных работ, проведенных Кузбасским институтом ФСИН России в 2020-2021 учебном году. – Новокузнецк: Кузбасский институт Федеральной службы исполнения наказаний, 2021. – С. 6-7.
2. Доктрина информационной безопасности в Российской Федерации [Электронный ресурс]: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения 01.12.2021)
3. Максимова Е. А. Информационная гигиена как фактор предотвращения последствий z-цифровизации / Е. А. Максимова, И. А. Молодцова, М. В. Бердник // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(29). – С. 67-73. – DOI 10.14529/SECUR180311.
4. Мид М. Культура и мир детства / М. Мид. – М.: Наука, 1988. – 429 с

Е.Б. Серова

Некоторые вопросы доказывания по уголовным делам о преступлениях, совершенных с использованием высоких технологий

Аннотация. В статье рассматривает вопрос использования в доказывании по делам о преступлениях, совершенных с использованием высоких технологий, информации, находящейся на различных электронных устройствах. Автором анализируется правоприменительная практика и научные источники в части, касающейся необходимости получения судебного решения на осмотр указанных устройств. Проведенный автором анализ приводит его к выводу о необходимости дифференцированного подхода к решению данного вопроса в зависимости от только, изъят носитель электронной информации надлежащим образом или не.

Ключевые слова: электронное устройство, следственный осмотр, судебное решение, информация на электронных носителях, следователь

Анализ современной судебно-следственной практики показывает, что высокие технологии все чаще используются в криминальных целях. С их помощью могут быть совершены практически любые преступления, на что справедливо обращается внимание в литературе[1]. Между тем, их раскрытие и расследование вызывают определенные проблемы, обусловленные трансформацией ключевых элементов системы преступления, а значит и появлением новых закономерных связей, характеризующих данную систему и проявляющихся в особенностях следообразования, на что исследователи обращают свое внимание достаточно

[1] См., напр.: Жердев П.А., Бондарчук А.С. Криминалистические и процессуальные аспекты производства следственных действий на первоначальном этапе расследования мошенничества в сфере компьютерной информации // Право и правопорядок: вопросы теории и практики: Сборник научных трудов. Под общей редакцией С.Е. Туркулец, Е.В. Листопадовой. – Хабаровск: Изд-во Дальневосточного государственного университета путей сообщения, - 2018, С. 33 – 38; Кириллова Н.П., Кушниренко С.П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий // Правоведение, 2013, № 3. – С. 78.

давно[1]. Кроме того, правы авторы, указывающие на зависимость хода расследования, степени организованности взаимодействия, алгоритма и очередности следственных действий и оперативно-розыскных мероприятий от способа совершения конкретного преступления[2].

Сказанное позволяет утверждать, что в настоящее время назрела насущная необходимость выработки новых подходов к поиску, обнаружению, фиксации и изъятию следов преступлений исследуемой группы, разработке новых тактических рекомендаций по производству различных следственных действий, наиболее типичными их которых являются следственные осмотры, допросы, назначение судебных, прежде всего, компьютерно-технических, экспертиз, обыск, выемка и др. [3]

По нашему мнению, важное, а возможно, и центральное, место в системе доказательств по делам о преступлениях рассматриваемой группы занимают протоколы следственных осмотров: места происшествия, предметов и документов, которые должны содержать сведения как об обнаруженном носителе информации, так и хранящейся на нем информации, имеющей интерес для дела. В связи с этим возникает вопрос о возможности производства такого осмотра без судебного решения, поскольку до настоящего времени процедура доступа к данным, содержащимся в памяти электронных носителей информации, включающим сведения о контактах абонента, его переписке, телефонных соединениях и проч., в уголовно-процессуальном законодательстве надлежащим образом не урегулирована.

Согласно ст. 186.1 УПК РФ при наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами имеет значение для уголовного дела, получение следователем указанной информации допускается на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ. Следует ли толковать данную правовую норму расширительно и распространять ее действие на производство иных следственных действий, в ходе которых может быть получена информация из электронных устройств. Однозначного решения данный вопрос до настоящего времени не нашел.

По мнению А.М. Багмета и С.Ю. Скобелина, на сегодняшний день следователи не имеют необходимой законодательной поддержки при получении информации, содержащейся в различных электронных устройствах, а самым распространенным является ее извлечение из электронных устройств в рамках следственного осмотра. При этом практики ссылаются на ч. 6 ст. 164 УПК РФ, в которой оговаривается возможность применения при производстве

[1] Кириллова Н.П., Кушниренко С.П. Указ. соч. С. 83.
[2] Жердев П.А., Бондарчук А.С. Указ. соч.
[3] См., напр.: Коломинов, В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: автореф. дис. … канд. юрид. наук/ В.В. Коломинов – Иркутск, 2017 – С. 19.

следственных действий технических средств и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств[1].

Если обратиться к имеющимся в науке исследованиям данного вопроса, можно увидеть разнообразие предлагаемых способов его решения. Так, одни ученые пришли к выводу, что в ситуациях, когда сотовый телефон участника уголовного судопроизводства изъят и находится у следователя, получать судебное решение на его осмотр и ознакомление с цифровым содержимым не требуется[2]. Другие, напротив, полагают получение судебного разрешения необходимым[3]. Нам наиболее близка позиция ученых, по мнению которых, порядок работы с мобильным абонентским устройством должен дифференцироваться в зависимости от ее значения для расследования[4], и источника происхождения технического устройства, из которого планируется получить информацию[5].

По нашему мнению, правоприменитель должен руководствоваться позицией Конституционного Суда Российской Федерации, который полагает, что 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. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке,

---

[1] Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. — 2013. — № 2. — С. 22—27.

[2] Багмет А.М., Скобелин С.Ю. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства // Уголовное право. — 2017, № 6. — С. 97—103.

[3] Даниленко И.А., Васильев Н.В. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт). // Вестник университета им. О.Е. Кутафина (МГЮА). — 2020, №10 — С.150—157; Когосов А.П. Отдельные проблемы обеспечения конституционных прав при осмотре сотового телефона. // Вестник ЮУрГУ. Серия «Право». — 2019. Т. 19, № 4. — С. 23—26 и др.

[4] Грачев С.А. Конституционные права личности при осмотре мобильного устройства: коллизия толкований в правовых позициях высших судебных инстанций России требует законодательного разрешения// Вестник Восточно-Сибирского института МВД России. — 2020, №3 — С. 134—145.

[5] Елагина Е.В. О процессуальных действиях, затрагивающих право граждан на тайну переписки // Криминалистъ. — 2019. №2. С.3—8.

предусмотренном ст. 125 УПК РФ[1]. Данная позиция находит свое подтверждение в судебной практике[2].

Еще один довод в защиту нашей позиции вытекает из того, какая именно информация запрашивается по судебного решению, получаемому в случаях, предусмотренных ст. 186.1 УПК РФ. Верховный Суд РФ разъяснил, что это сведения о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций[3]. Нетрудно заметить, что информация, получаемая в рамках следственного осмотра изъятого гаджета гораздо шире и разнообразнее, нежели чем то, что требует судебного решения.

Таким образом, если осматриваемое техническое устройство, находится в распоряжении следователя на законных основаниях, получение судебного разрешения на осмотр этого устройства не требуется. Тем более, что ст. 176 УПК РФ прямо предписывает производить осмотр следов преступления и иных обнаруженных предметов на месте производства следственного действия, не устанавливая при этом никаких дополнительных требований к процедуре осмотра и не делая никаких изъятий из возможных объектов осмотра.

Литература

1. Багмет, А. М. Извлечение данных из электронных устройств как самостоятельное следственное действие / А. М. Багмет, С. Ю. Скобелин // Право и кибербезопасность. — 2013. — № 2. —С. 22—27.
2. Багмет, А. М. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства / А. М. Багмет, С. Ю. Скобелин // Уголовное право. — 2017. — № 6. — С. 97—103.
3. Грачев, С. А. Конституционные права личности при осмотре мобильного устройства: коллизия толкований в правовых позициях высших судебных инстанций России требует законодательного разрешения. / С. А. Грачев // Вестник Восточно-Сибирского института МВД России. — 2020. — №3 — С.134—145.

[1] Определении Конституционного Суда Российской Федерации № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» — Доступ из справ.-прав. системы «КонсультантПлюс» 02.12.2021.

[2] Апелляционное постановление Верховного суда Республики Дагестан от 22.01.2019 по делу № 22-2255/2019; Апелляционное постановление Верховного суда Республики Дагестан от 22.01.2019 № 22К-95/2019 — Доступ из справ.-прав. системы «КонсультантПлюс» 02.12.2021.

[3] Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)». — Доступ из справ.-прав. системы «КонсультантПлюс» 02.12.2021.

4. Даниленко, И. А. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт) / И. А. Даниленко, Н. В. Васильев. — Вестник университета им. О. Е. Кутафина (МГЮА). — 2020. — №10 — С. 150—157.
5. Елагина, Е. В. О процессуальных действиях, затрагивающих право граждан на тайну переписки. / Е. В. Елагина — Криминалистъ. — 2019. — №2. — С. 3—8.
6. Жердев, П. А. Криминалистические и процессуальные аспекты производства следственных действий на первоначальном этапе расследования мошенничества в сфере компьютерной информации / П. А. Жердев, А. С. Бондарчук // Право и правопорядок: вопросы теории и практики: Сборник научных трудов. Под общей редакцией С.Е. Туркулец, Е.В. Листопадовой. — Хабаровск: Изд-во Дальневосточного государственного университета путей сообщения. — 2018. — С. 33—38.
7. Кириллова, Н. П. Кушниренко С.П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий / Н. П. Кириллова, С. П. Кушниренко // Правоведение. — 2013. — № 3. — С. 74—90.
8. Когосов, А. П. Отдельные проблемы обеспечения конституционных прав при осмотре сотового телефона. / А. П. Когосов // Вестник ЮУрГУ. Серия «Право». — 2019. — Т. 19, № 4, — С. 23—26.
9. Коломинов, В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: автореф. дис. … канд. юрид. наук / В. В. Коломинов — Иркутск. — 2017 — 25 с.

А.М. Смирнов

Кибербуллинг как актуальная проблема современного общества и проблемы с противодействием ему в России

Аннотация. В статье актуализируется проблема кибербуллирга, раскрываются формы его проявления и излагаются причины его распространения в обществе. Обращается внимание на проблемы борьбы с этим негативным социальным явлением в России, связанные с медлительностью законодательной власти в принятии социально значимых нормативных актов, обеспечивающих защиту личности от противоправных посягательств и иного негативного влияния.

Ключевые слова: кибербуллинг, буллинг, насилие, психологическое насилие, хэйт.

К сожалению, мы живем в обществе, в котором насилие над личностью, особенно психологическое, получает достаточно широкое распространение. Несмотря на, казалось бы, все более цивилизованное развитие современных государств, распространение идей гуманизма и толерантности, элементы

насилия, ненависти и вражды все больше распространяются в обществе, получая все более изощренные способы своей реализации. Все это становится возможным благодаря современному научно-техническому прогрессу, в частности развитию Интернета.

Интернет и иных средства Масс-медийной коммуникации стали активно использоваться злоумышленниками для оказания психологического давления на людей в целях достижения своих противоправных целей. Это явление получило в науке свое название – киббербуллинг.

Кибербуллинг (Интерент-травля, кибертравля) представляет собой целенаправленные намеренные оскорбления, угрозы, различного рода диффамации и сообщения другим компрометирующих данных с помощью современных средств коммуникации, как правило, осуществляемые систематически в течение продолжительного периода времени для более верного достижения ожидаемого результата[1].

Таким образом можно сказать, что основными признаками кибербуллинга являются: 1) оказание психологического давления на выбранную жертву; 2) систематичность этого давления; 3) реализация такого давления посредством сети Интернет или иных средств коммуникации.

Распространенность данного негативного явления обусловлено не только развитием различного рода средств электронной коммуникации, но и психологической ослабленностью и высоким уровнем психологической чувствительности представителей современного общества, особенно несовершеннолетних и молодежи. Так сказать «тепличные условия» их жизни негативно сказались на адекватности мировосприятия и формировании способности правильно реагировать на негативное воздействие внешней среды.

Нередко можно услышать вопрос: как отличить кибербуллинг от неудачной шутки? Ведь иногда какое-либо высказывание действительно может не нести в себе издевательства. Случается, что от виртуального друга мы можем слышать неприятные или даже оскорбительные шутки.

Но если это не «разовая акция», а уже манера общения, приносящая дискомфорт, нужно попросить собеседника это прекратить. Если «заигравшийся» извинится и изменит свое поведение, скорее всего, его действия не были намеренной травлей в Интернете. В противном случае можно говорить о кибербуллинге. Здесь нужно добавить, что оскорбления в интернете, даже сделанные в личные сообщения, административно наказуемы. Оскорбления стоит научиться отличать от клеветы и диффамации, т.к. за них предусмотрена разная ответственность[2].

Согласно результатам зарубежных исследователей, которые первыми обратили внимание на рассматриваемую социальную проблему, кибербуллинг проявляется в следующих формах:

---

[1] Интернет-травля. Миф или реальность? / Н. М. Лахмытко // Методист. 2015. № 6. С.21-24; *Парфентьев У.* Кибер-агрессоры //Дети в информационном обществе. 2009. Т. 2. С. 66-67.

[2] Кибербуллинг: как не стать жертвой // Газета.ru / URL: https://www.gazeta.ru/comments/2021/11/10_a_14189803.shtml?updated.

1. Оскорбление. Как правило, происходит в открытом публичном пространстве Интернета, посредством оскорбительных комментариев, вульгарных обращений и замечаний.

2. Домогательство. Целенаправленные, систематические кибер-атаки от незнакомых людей, пользователей социальных сетей, людей из ближайшего реального социального окружения.

3. «Очернение» и распространение слухов. Намеренное выставление жертвы в чёрном свете с помощью публикации фото- или видеоматериалов на Интернет-страницах, форумах, в новостных группах, через электронную почту, например, чтобы разрушить дружеские отношения или отомстить экс-подруге.

4. Использование фиктивного имени. Намеренно выдавать себя за другого человека, используя пароль жертвы, например, для того, чтобы оскорбить учителя.

5. Публичное разглашение личной информации. Распространение личной информации, например, интимных фотографий, финансового положения, рода деятельности с целью оскорбить или шантажировать, например, экс-партнера.

6. Социальная изоляция. Отказ общаться (как на деловом, так и на неформальном уровне), исключение из Instant-Messenger'а группы или игрового сообщества и так далее.

7. Продолжительное домогательство и преследование. Систематическое (сексуальное) преследование кого-либо, сопровождающееся угрозами и домогательствами.

8. Открытая угроза физической расправы. Прямые или косвенные угрозы убийства кого-либо или причинения телесных повреждений[1].

Как отмечают исследователи, к факторам, оказывающим эффективное влияние на проявление буллингового поведения относятся следующие:

- личные факторы – отсутствие воспитания, заниженная/ завышенная самооценка и излишняя эмоциональность;
- факторы поведения – мешающее другим людям поведение, вандализм, прогулы и низкая успеваемость в учебном заведении, ранние сексуальные контакты, ранняя судимость;
- социальные факторы – влияние средств массовой информации, культ насилия в обществе, поведение родителей, люди в круге общения с отклоняющимся поведением;
- различного рода конфликты внутри семьи;
- проблемы в личной жизни – наступление фазы полового созревания и связанные с этим проблемы физиологического и психологического характера[2]

Очевидно, что с данным явлением необходимо бороться и осуществлять данную борьбу на всех уровнях с использованием всех возможных средств и методов. Это связано, прежде всего с тем, что проблема Интернет-травли актуальна для всего мира.

---

[1] Nancy Willard, M.S. Educator's Guide to Cyberbullying and Cyberthreats // URL: http://csriu.org/cyberbully/docs/cbcteducator.pdf.

[2]Ильин Е. П. Психология агрессивного поведения: учебник. – Санкт-Петербург, 2018. С. 182.

Необходимо отметить, что в нашей стране данная проблема также существует. Вместе с тем, она не получает должного внимания как это делается во всем цивилизованном мире. И это не смотря на то, что согласно исследованиям Всемирной организации здравоохранения (ВОЗ) (исследования проводились в 2009–2010 гг. и в 2013-2014 гг. в отношении несовершеннолетних) Россия занимает лидирующие позиции по распространению рассматриваемого нами явления. По данным ВОЗ в России каждый пятый ребенок становился жертвой буллера. По результатам исследования, проведенного РОЦИТ (общественная организация, объединяющая активных интернет-пользователей России (официальный сайт: https://rocit.ru), проведенного в 2017 г., жертвой кибербуллинга в России стал каждый второй подросток[1].

В российском законодательстве, к сожалению, нет специальной статьи за оскорбление в Интернете. Оскорбления проходят по статье 5.61 Кодекса Российской Федерации об административных правонарушениях. Раньше этот состав подпадал под статью 130 Уголовного кодекса Российской Федерации (УК РФ), но с 2011 г. она утратила силу. Распространение ложных данных и подрыв репутации подпадает под статью 128.1 УК РФ «Клевета» и статья 119 УК РФ «Угроза жизни».

Однако эти нормы носят общий характер по отношению к специфике рассматриваемой проблемы и потому не обладают достаточным уровнем эффективности при ее решении. Именно поэтому нужны специальные нормы, предусматривающие непосредственное привлечение к юридической ответственности за травлю в средствах Масс-медиа.

Положительный пример в этом можно взять у передовых стран, которые более быстро реагируют на негативные изменения в социальных процессах и вносят соответствующие изменения в «наказательное» законодательство. Например, Кодекс Украины об административных правонарушениях в недавнем времени был дополнен статьей 173-4, регламентирующей понятие «буллинга», а также устанавливающий ответственность за указанное деяние. В законе «Об образовании» данной страны предусмотрели типичные признаки буллинга (травли), а также расширили права и обязанности участников образовательного процесса[2].

В России в Государственную Думу еще весной 2020 г. введен законопроект о борьбе с преследованием в Интернете[3]. Однако до сих пор он еще находится на рассмотрении у парламентариев, что, к сожалению, демонстрирует инертность и медлительность российской законодательной власти в принятии социально

---

[1] Раненкова Е.А. Проблемы борьбы с буллингом и скулшутингом: совершенствование уголовного законодательства Российской Федерации / В сборнике: Актуальные проблемы уголовного законодательства на современном этапе сборник научных трудов Международной научно-практической конференции. 2020. С. 151-156.

[2] Рада ввела ответственность за буллинг: за травлю будут жестко штрафовать. Электронный ресурс [URL: https://www.segodnya.ua/]. Режим доступа: https://www.segodnya.ua/ukraine/rada-vvela-otvetstvennost-za-bulling-za-travlyu-budut-zhestko-shtrafovat-1199139.html

[3] Травля под статьей // Российская газета / URL: https:rg.ru/2020/08/10/zakonoproekt-o-borbe-s-travlej-v-seti-vnesut-v-gosdumu-oseniu.html.

значимых нормативных актов, обеспечивающих защиту личности от противоправных посягательств и иного негативного влияния.

М.С. Смолин

Аспекты собирания и использования в доказывании цифровых следов

Аннотация. Эффективное использование цифровых следов в доказывании требует изменения подхода к их собиранию. На современном этапе применяется подход, согласно которому описывается внешняя сторона цифрового следа, доступная через программный интерфейс. Сущность цифровых следов состоит в наличии активного и пассивного компонентов, содержащих доказательственную информацию, отображающую поведение человека, а не его желание распространить или получить определенный объем информации. Фиксация пассивного компонента цифровых следов позволяет принципиально изменить доказательственную ценность цифровых следов.

Ключевые слова: цифровые следы, форма доказательств, активные цифровые следы, пассивные цифровые следы, доказывание с использованием цифровых следов, цифровое алиби, инсценировка.

Так называемая «цифровизация» и связанные с ней изменения в социальных отношениях привлекают пристальное внимание юридической науки и практики, в особенности, последние несколько лет.

Вместе с тем, существенных изменений в уголовном судопроизводстве эти исследования не принесли. Полагаю, что причина подобного положения вытекает из попыток адаптировать имеющиеся концепции, классификации и подходы к «новым» юридическим фактам – возникающим в процессе взаимодействия людей при помощи цифровых устройств, обладающих нетипичными свойствами.

Общая тенденция сводится к тому, что информация, полученная в процессе использования цифровой техники, рассматривается и учеными и правоприменителями либо как новая форма документа – иного доказательства, то есть цифровой документ, цифровое доказательство[1], либо процесс ее извлечения и интерпретации отнесен к области специальных знаний, результат применения которых должен представляться в виде заключений специалиста либо эксперта, то есть оценка проводится с позиции содержания текстов, извлеченных из электронного носителя.

Юридический (криминалистический) аспект формирования цифровых следов в практике расследования не изучается[2], чему способствует отсутствие единства в понимании как самого термина, так и явлений, им описываемых.

С этой позиции, цифровой след может быть определен как «совокупность информации о посещениях и вкладе пользователя во время пребывания в цифровом пространстве».

[1] Зуев С.В. Цифровая криминалистика. Учебник для ВУЗов. М., 2021. С. 105.
[2] Зуев С.В. Цифровая криминалистика. Учебник для ВУЗов. М., 2021. С. 97, 103-104.

Следствием, вытекающим из этого определения, является то, что цифровой след формируется и существует не сам по себе, а как элемент особой цифровой среды – «киберпространства». Человек сам «попасть», точнее воспринять ее с помощью своих чувств, не может, и взаимодействует с ней посредством компьютерного устройства, способного подключаться к телекоммуникационным сетям. В результате, традиционная классификация следов на идеальные и материальные, для цифровых следов утрачивает свое практическое значение[1], а доказательственный смысл цифровых следов вытекает из их деления на активные и пассивные.

Под активными цифровыми следами понимается та информация, которую человек стремится целенаправленно сообщить, передать, разместить; к пассивным относится та информация, которая передается с технической целью, например, чтобы получить доступ к ресурсу при так называемой регистрации, или служебная, техническая информация, которая часто не осознается человеком, и формируется устройством в связи с доступом к сетевому ресурсу – например, программный лог или метаданные мультимедийного файла.

На сегодняшнем этапе реально производится отыскание преимущественно следов активных, желательно – в форме текстов, описывающих процесс совершения преступления и иную связанную с ним информацию. Пассивным следам должное внимание не уделяется.

Примером служит любое применение комплексов для извлечения данных, когда в качестве задачи ставится чтение переписки лиц, прикосновенных к преступлению, что реализуется протоколом осмотра предметов – отчетов, представленных программной частью соответствующего комплекса. Сведениям о системных событиях в контексте доказывания внимание не уделяется в принципе, из числа пассивных следов анализируется, как правило, журнал соединений – как подтверждающий наличие связи между людьми.

При этом, цифровое устройство воспринимается субъектом расследования как грубая аналогия традиционного материального объекта, конкретно – записной книжки. В лучшем случае, электронный носитель или цифровая среда отождествляются с неким местом, хранилищем информации.

Представляется, что причина недооценки цифровых доказательств состоит в неверном определении обстоятельства подлежащего доказыванию с использованием цифровых следов: в виде попытки ответить на вопрос «что делал человек с объектом (что делал человек в телекоммуникационной сети сети)».

Как только криминалистическая задача ставится правильно – «каким образом человек взаимодействовал с киберпространством в ходе преступления и для достижения какой цели вступал в подобное взаимодействие», значение пассивных следов в системе доказывания становится очевидным.

---

[1] Смолин М.С. Цифровые следы в раскрытии преступлений против половой свободы и неприкосновенности личности // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития (материалы Международной практической конференции). М. 2019. С. 539.

Таким образом, познавательные усилия должны быть направлены не на конкретное устройство и содержащуюся в нем письменную (вербализованную) продукцию в «готовом» виде, а на поведение человека по взаимодействию с цифровыми устройствами, объединенными в сеть, которое фиксируется в цифровой сети распределено, то есть без привязки к конкретному месту, ресурсу или устройству.

Цифровые следы, также, как и идеальные, фиксируют не «осколок» информации, а процесс, человеческое поведение в динамике. В отличие от идеальных следов, они объективны, в отличие от материальных, они не запечатлевают какой-либо физический процесс «во всей его полноте и многообразии», а сохраняют только заранее определенные его свойства, характеристики, что принципиально очерчивает границу для познания и моделирования отображаемого поведенческого акта, в т.ч., путем экспертного исследования. Применительно к цифровым следам, компьютерно-техническая экспертиза не может выявить новые свойства и признаки поведения людей, а сводится к выявлению совокупности таких - относящихся к преступлению следов, и анализу процесса их формирования по критериям времени создания, места выявления, способности лица влиять на их содержание (т.е. отнесению следа к активному либо пассивному). Процедура «выявления цифровых следов» невозможна без принятия решений об относимости и достоверности анализируемой информации. Таким образом, в существующем виде компьютерно-техническая экспертиза во многом выполняет функции отыскания и оценки следов, что не соответствует закрепленной в УПК РФ модели распределения функций между субъектом доказывания и экспертом[1].

Результатом отсутствия должного внимания к процессам формирования цифровых следов является подмена предмета доказывания, когда вместо выявления и фиксации поведения людей – времени и места взаимодействия с информационно-телекоммуникационной сетью, используемого устройства, продолжительности взаимодействия, цели взаимодействия в виде получения или передачи определенной информации, в протоколах следственных действий описываются манипуляции с интерфейсом программных продуктов в упрощенном виде с использованием неконкретных формулировок «через мобильное приложение»[2] «вошел в программу»[3], «зашел на страничку», «скинул файл», «поместил в свободном доступе». Из протоколов следственных действий эти формулировки, через текст обвинительного заключения, перемещаются в описание преступных деяний в приговорах суда. В результате, доказательственное значение информации, извлеченной из цифровых устройств, во многом утрачивается, кроме того, создается благоприятная среда для искусственного создания заведомо ложных доказательств защиты путем

[1] П. 4 Постановления Пленума Верховного суда РФ от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам».

[2] Приговор Волгодонского районного суда Ростовской области по уголовному делу №1-465/2020 от 23.11.2020.

[3] Приговор Первомайского районного суда Ярославской области по уголовному делу № 1-28/2020 от 22.07.2020.

формирования «цифрового алиби» - искусственно созданной переписки относительно преступного события, создания и размещения на устройствах и в телекоммуникационных сетях недостоверной информации. Следует отметить, что основным механизмом «цифровой» инсценировки обстоятельств преступления на современном этапе становится не уничтожение, изменение либо модификация информации, хранящейся в цифровой среде или на цифровом носителе, а формирование дополнительных цифровых следов, информационное содержание которых противоречит сведениям, содержащимся в уже имеющихся следах, в целях придания недостоверности всей системе доказательственной информации, полученной из цифровых носителей.

Кроме того, подмена исследования сущности цифровых следов формальным описанием их внешней, доступной посредством интерфейса, формы, порождает ошибку восприятия, когда киберпространство начинает восприниматься как некий аналог места «материального» мира, с последующим применением средств и способов работы с цифровыми следами как предметами, обнаруженными в ходе осмотра места происшествия.

Способом устранения указанных недостатков является включение в предмет доказывания не только содержательного аспекта информации, доступной на цифровых носителях, но и выяснение и фиксация процесса следообразования – с установлением технического канала связи ее передачи, времени и места размещения, метаданных, то есть пассивных аспектов цифровых следов. На современном этапе это может быть реализовано в трех процессуальных формах – путем предоставления иной информации – документа владельцем сетевого ресурса размещения информации либо провайдером, путем осмотра предмета и путем формирования заключения эксперта. Каждая из этих форм не является безупречной, нередко один цифровой след правоприменитель вынужден «распределять», фиксировать при помощи нескольких процессуальных форм одновременно, что создает дополнительные сложности как для закрепления доказательства, так и для его оценки и использовании в доказывании, что, в свою очередь, влечет пробелы в логике доказывания и трудности в вербальном описании следа в итоговых процессуальных документах.

Представляется, что дальнейшее использование цифровых следов в доказывании будет сопровождаться увеличением конкретизации пассивного компонента цифрового следа, результатом чего станет возникновение новой процессуальной формы, направленной на полноту фиксации признаков этого вида следов.

Литература

1. Постановления Пленума Верховного суда РФ от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам»
2. Зуев С.В. Цифровая криминалистика. Учебник для ВУЗов. М., 2021.
3. Смолин М.С. Цифровые следы в раскрытии преступлений против половой свободы и неприкосновенности личности // Криминалистика – прошлое,

настоящее, будущее: достижение и перспективы развития (материалы Международной практической конференции). М. 2019.

Э.Г. Хомяков

О некоторых проблемах в расследовании киберпреступлений и путях их решения

Аннотация. В статье акцентируется внимание на том, что в связи с непрерывным ростом киберпреступлений, фиксируемым в последние годы, необходим четкий, детальный анализ проблем, имеющих место при их расследовании. Данные проблемы не могут быть решены без серьезных преобразований в сложившейся системе юридических наук, а также нового подхода в подготовке лиц, ведущих расследование киберпреступлений. Предлагаются отдельные пути решения обозначенных проблем.

Ключевые слова: киберпреступления, киберпреступность, расследование, методика расследования, проблемы, криминалистика, уголовное право.

В последние годы представители федеральных органов исполнительной власти отмечают значительный рост киберпреступлений, которые в различных источниках фигурируют как «компьютерные преступления», «преступления в сфере компьютерной информации», «интернет-преступления», «сетевые преступления», «преступления в виртуальном пространстве», «преступления в сфере высоких технологий», «информационные преступления» и т.п.

Следует отметить, что до 2017 года в официальной регистрации велся учет преступлений в сфере компьютерной информации (т.е. преступлений, сведенных в главу 28 УК РФ), количество которых по отношению к общему количеству зарегистрированных в Российской Федерации преступлений не превышало десятых долей процента[1]. Однако с 2017 года в статистической отчетности появляется новая группа преступлений – преступления, совершенные с использованием компьютерных и телекоммуникационных технологий, а с 2020 года – преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. В указанные годы зафиксирован непрерывный рост преступлений указанной группы: 2017 год – 90587, 2018 год – 174674, 2019 год – 294409, 2020 год – 510396[2]; при этом данные преступления имеют низкую раскрываемость[3].

Данная ситуация требует детального анализа, выявления конкретных проблем в области исследования, раскрытия, расследования, учета, профилактики данных преступлений, а также планирования путей решения обнаруженных проблем.

---

[1] Хомяков Э.Г. Об актуальных проблемах раскрытия и расследования преступлений в сфере компьютерной информации // Тенденции развития уголовной политики в современной России: сб. ст. Ижевск: Издат. центр «Удмуртск. ун-т», 2019. С. 298-314.

[2] Официальный сайт МВД Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения 03.12.2021).

[3] Заседание коллегии Генпрокуратуры РФ 17 марта 2020 года. URL: http://kremlin.ru/events/president/news/62998 (дата обращения 03.12.2021).

Эффективное противодействие киберпреступности невозможно без серьезных преобразований в сложившейся системе юридических наук и связанных с ними учебных дисциплин, прежде всего в уголовном праве, криминалистике, уголовном процессе и криминологии, а также без реорганизации деятельности российских правоохранительных органов, выработки нового подхода в подготовке лиц, ведущих расследование киберпреступлений.

От уголовного права требуется прежде всего четкая понятийная характеристика и классификация данной группы преступлений, находящая отражение как в действующем уголовном законе, так и в системе учета данных преступлений; для этого в уголовном законе должны быть четко обозначены квалифицирующие признаки данных преступлений. Также необходимо изменить сложившуюся в настоящее время систему наказаний за киберпреступления, зафиксировав более высокую степень их общественной опасности и сделав возможным признание рецидива при их совершении. Безусловно действующий Уголовный кодекс РФ должен быть изменен в части, касающейся киберпреступлений; за основу при разработке его новой редакции может быть взят либо Модельный кодекс для государств – участников СНГ 1996 года (содержащий отдельный раздел – раздел XII «Преступления против информационной безопасности», включающий 7 статей (статьи 286-292)), либо соответствующие элементы зарубежного уголовного законодательства, демонстрирующие эффективность в борьбе с киберпреступностью.

Криминалистика как наука о раскрытии и расследовании преступлений должна быть подвергнута коренной модернизации, прежде всего в плане изменения ее системы. Это возможно либо включением в ее структуру в качестве самостоятельного раздела цифровой криминалистики, либо наполнением существующих разделов соответствующим цифровым содержанием. Прежде всего необходимо определиться с понятием цифрового следа (наверное, данная характеристика следа, образующегося при совершении любого киберпреступления, более корректная, чем виртуальный или электронный след), разработать классификацию цифровых следов, способов (средств, методов) их обнаружения, фиксации, изъятия и исследования. Возможно необходима разработка криминалистического учения о цифровом следе и о цифровом доказательстве. Также необходима корректировка тактики существующих следственных действий, а также возможно дополнение действующего УПК новыми следственными действиями, необходимыми для обнаружения и закрепления цифровых следов в процессе расследования киберпреступлений. Методики расследования киберпреступлений должны быть разработаны для каждой их разновидности; в процесс расследования должны быть внедрены современные информационные и компьютерные технологии, доступные на уровне территориальных подразделений правоохранительных органов (например, разработаны специализированные автоматизированные рабочие места для лиц, участвующих в процессе расследования киберпреступлений). В любом случае при наполнении цифровой криминалистики соответствующим содержанием должен быть изучен передовой зарубежный как научный, так и

практический опыт противодействия киберпреступности. При этом инертность и длительная раскачка в решении этой проблемы недопустимы.

Следователям необходим практический инструментарий, позволяющий проводить расследование не только на территории Российской Федерации, но и с учетом трансграничного характера отдельных киберпреступлений дающий возможность ориентироваться в зарубежном уголовном законодательстве, получать необходимую информацию и материалы из других стран; следователи данной специализации должны знать международные договоры и соглашения, заключенные Россией и ее правоохранительными органами по линии информационного взаимодействия и обмена информацией, уметь составлять и направлять запросы в другие страны в процессе расследования киберпреступлений.

Здесь возникает закономерный вопрос: какие знания необходимы лицу, производящему расследование киберпреступлений?

Интересное заявление привлекло мое внимание при изучении соответствующих зарубежных источников.

Так Сломо Кениг – детектив из США, эксперт по расследованию киберпреступлений и компьютерной криминалистике в 2003 году заявил, что научить хорошего детектива расследовать компьютерные преступления гораздо легче, чем сделать из компьютерщика хорошего детектива[1]. Возможно в то время с этим утверждением можно было согласиться, однако в настоящее время информационные, компьютерные и телекоммуникационные технологии достигли качественно нового более высокого уровня своего развития. В ближайшем будущем эти технологии будут стремительно совершенствоваться и, вероятно, данное выражение применительно к России можно будет перефразировать с точностью наоборот: «научить хорошего следователя расследовать компьютерные преступления гораздо труднее, чем сделать из компьютерщика хорошего следователя». Следователям потребуется стать специалистами в области высоких технологий, а в уголовно-процессуальном законе необходимо будет раскрыть понятие «специальные знания», а также наделить лиц, проводящих расследование необходимым объемом специальных знаний, которые сейчас являются прерогативой эксперта и специалиста.

Если несколько лет назад, когда киберпреступления составляли менее 1% от общего количества зарегистрированных в РФ преступлений, привлечение специалистов к участию в следственных действиях никаких проблем не составляло, то в настоящее время, когда киберпреступления уже составляют почти четвертую часть в массиве зарегистрированных в РФ преступлений, привлечение в указанных целях специалистов, которых в территориальных подразделениях МВД РФ и СК РФ недостаточное количество, весьма проблематично; при этом специалистами, как правило, выступают эксперты, производящие компьютерно-технические экспертизы, для которых производство данных экспертиз является приоритетным видом деятельности.

[1] Griffith D. How To Investigate Cybercrime. November 1, 2003. URL: https://www.policemag.com/339099/how-to-investigate-cybercrime (дата обращения 03.12.2021).

Пять тысяч человек в составе специализированных подразделений МВД России, о которых говорил В.В. Путин на расширенном заседании коллегии МВД РФ в 2021 году[1], распределенные по 85 субъектам Российской Федерации, вряд ли будут повсеместно привлекаться в качестве специалистов при производстве следственных действий и позволят решить данную проблему.

Еще одна проблема уже криминологического характера – это изучение личности киберпреступника. Множество работ, посвященных изучению криминологических признаков лиц, совершающих киберпреступления, дают настолько абстрактный портрет киберпреступника, что под него подходит любой мужчина в самом расцвете сил (достаточно широкого возрастного диапазона), имеющий определенный объем знаний, умений и навыков из области компьютерной техники, совершающий, как правило разовые преступления указанной направленности, чаще всего в одиночку. Из данной характеристики складывается впечатление, что киберпреступники-профессионалы остаются вне поля зрения российских правоохранительных органов, также, как и преступные сообщества, организованные группы. Вместе с тем, именно грамотная организация подобных преступных сообществ позволяет им находиться в тени в процессе совершения длящихся (многоэпизодных) и неоднократных преступлений. В отдельных источниках подобные преступные организации, совершающие киберпреступления определенного вида, тем не менее рассматриваются[2], но конкретные и подробные методики расследования подобных киберпреступлений, как правило, не предлагаются.

Можно обозначить и другие проблемы, возникающие в процессе расследования киберпреступлений – низкую выявляемость и раскрываемость киберпреступлений, их высокую латентность, устаревшую систему их учета (регистрации), недосточное оснащение экспертных подразделений необходимым и современным инструментарием, потребность в новых методиках производства отдельных видов судебных экспертиз (вполне возможно, в ближайшее время может появиться отдельный род судебных экспертиз – цифровых). Также существуют проблемы процессуального характера, связанные со сроками расследования подобных преступлений, закрепления в УПК РФ понятий «цифровые доказательства» и «место преступления» и т.д.

В этой связи для решения рассмотренных и иных проблем, со стороны государства, правительства РФ была бы целесообразна разработка целевой федеральной программы по борьбе с киберпреступностью, в которой в течение ближайшего периода (не более 5 лет) были бы обозначены конкретные задачи, требующие соответствующих финансовых затрат и незамедлительного решения.

Со стороны государства либо конкретных заинтересованных федеральных органов исполнительной власти возможна организация грантовой или конкурсной поддержки исследований по линиям гражданских и ведомственных

---

[1] Расширенное заседание коллегии МВД России. 2021-03-03. URL: http://www.kremlin.ru/events/president/transcripts/copy/65090 (дата обращения 03.12.2021).

[2] Корнилов Г. Кейсы компьютерной криминалистики. 2018. URL: https://www.youtube.com/watch?v=BEIfF0QACd0 (дата обращения 03.12.2021).

вузов, направленных на разработку соответствующих учебных материалов, технического, аппаратно-программного и иного обеспечения деятельности, связанной с расследованием киберпреступлений.

Литература

1. Заседание коллегии Генпрокуратуры РФ 17 марта 2020 года. URL: http://kremlin.ru/events/president/news/62998 (дата обращения 03.12.2021).
2. Корнилов Г. Кейсы компьютерной криминалистики. 2018. URL: https://www.youtube.com/watch?v=BEIfF0QACd0 (дата обращения 03.12.2021).
3. Официальный сайт МВД Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения 03.12.2021).
4. Расширенное заседание коллегии МВД России. 2021-03-03. URL: http://www.kremlin.ru/events/president/transcripts/copy/65090 (дата обращения 03.12.2021).
5. Хомяков Э.Г. Об актуальных проблемах раскрытия и расследования преступлений в сфере компьютерной информации // Тенденции развития уголовной политики в современной России: сб. ст. Ижевск: Издат. центр «Удмуртск. ун-т», 2019. С. 298-314.
6. Griffith D. How To Investigate Cybercrime. November 1, 2003. URL: https://www.policemag.com/339099/how-to-investigate-cybercrime (дата обращения 03.12.2021).

МОЛОДЫЕ УЧЕНЫЕ

В.С. Аверьянов

Современный подход к противодействию сетевым атакам на космические сервисы: основные направления исследования

Аннотация. В материалах статьи отражен ряд важных вопросов, касающихся направлений и этапов развития мирного освоения космоса. За основу принят комплекс мероприятий по разработке совершенно новых, отличных от существующих методов, набор компонент НС (наземный сегмент). Это определено и целью исследования – способам построения сверхзащищенных космических линий связи, с учетом структур сигналов и алгоритмов взаимодействия программно – аппаратных средств. В задачи исследования входят – способы анализа трафика циркулирующего между КА-НС, НС-потребитель услуг космической связи, методы обнаружения аномалий, потенциальных угроз вторжений, целенаправленных сетевых атак и эффективная защита от них.

Ключевые слова: информационная безопасность, канал связи, космические сервисы, сетевой трафик, сетевые атаки, технология.

27 января 1967 главы государств СССР, США и Великобритании Л.И. Брежнев, Л.Б. Джонсон и Д.Г. Вильсон подписывают международный договор о принципах деятельности и сотрудничества государств в сфере освоения космического пространства. В зону действия договора включены естественный и искусственные спутники Земли, наземные станции связи, иные целевые инфраструктурные объекты. К ряду условий по данному документу относятся: меры разумности и осторожности в случаях проведения космических экспериментов, отсутствие помех для деятельности других государств в процессах освоения внеземного пространства, минимизация разрушающих воздействий на земную среду из космоса.

Спустя более половины столетия оборонным подрядчиком L3Harris Technologies Incorporation выпущена установка наземного базирования для Космических сил США, способная вызывать блокировку коммуникационных сигналов с КА связи на околоземной орбите. На этапах разработки стран большой семёрки находится ещё более десятка подобных систем, в том числе и Meadowland. Космическая гонка вооружений не прекращается до сих пор, а космическое киберпространство представляет собой полигон по отработке тактико-технических мероприятий и навыков ведения цифровых боевых действий.

Современное Российское государство обеспечивает безопасность национальных интересов во многих технологических областях, к одной из самых востребованных в последнее время следует отнести космическую отрасль с её прорывными технологиями и высокими темпами роста. В условиях гипервысоких объемов трафика, «общение» устройств через космический сегмент становится небезопасным, подверженным различным целевым кибератакам со стороны злоумышленников. В связи с этим коммуникационное оборудование НС нуждается в дополнительных мерах по обеспечению ИБ

(информационная безопасность), отвечающих последнему слову техники. К числу подобных мер следует отнести: эвристический анализ сетевого трафика, построение математической модели (портрета) киберпреступника, оценку защищенности линий связи, стоит учесть и вероятностную составляющую киберинцидентов, а также возможный экономический ущерб от незаконных вторжений и хищений защищаемой информации.

Комплекс мер по модернизации программно – аппаратных средств НС позволит выявлять потенциальные угрозы вторжения в защищаемую систему на ранних, «околонулевых» этапах, выстраивать эффективные защитные механизмы на основе существующей аппаратуры, проектировать новые линии космической связи с запасом по «информационной прочности». К первичным механизмам обнаружения и противодействия киберугрозам для НС следует отнести: анализ трафика циркулирующего в линиях связи методами математического моделирования, сигнатурного анализа кода и обучаемого искусственного интеллекта. При этом необходимо задействовать вычислительный потенциал существующей аппаратуры по защите информационных потоков и обеспечения информационной безопасности узлового объекта. В перспективе, результатом такого подхода станет эффективная система защиты от космических сетевых атак типа: DDoS – атаки (отказ в обслуживании), R2L – атаки на наземный сегмент (неавторизованный доступ), U2R – атаки на основе существующих уязвимостей (получение Root прав), атаки зондированием на основе перехвата и анализа сетевого трафика. Необходимый набор программно – аппаратных компонент по сбору, идентификации и эксплуатации сетевых уязвимостей позволит сформировать требуемый уровень безопасной эксплуатации информационно-телекоммуникационных систем по обработке большого объема информации со встроенными функциями сетевой защиты от вторжений как внутри, так и вне системы.

Методы обнаружения сетевых атак. Современные наземные комплексы, станции космической связи имеют достаточно серьезную защиту на основе российских криптографических алгоритмов с поддержкой стандартов: ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001. В большинстве случаев их аппаратная часть реализована на базе сервера специализированной, фиксированной платформы, способной обеспечивать высокий класс защищенности по требованиям ФСБ России. Системы обнаружения вторжений, мониторинг трафика, сетевых соединений при этом расположены на иной, отличной от существующей аппаратной платформе. В большинстве случаев подобная разрозненность систем затрудняет управление и эффективность обнаружения вторжений для специалистов в области защиты информации. В связи с этим современные криптомаршрутизаторы предлагается дооснастить функциями обнаружения кибератак и мониторинга сетевого трафика для сбора информации о сетевых атаках «на месте». Далее представлены способы построения системы обнаружения вторжений на базе криптомаршрутизатора, которые способны увеличить эффективность обнаружения киберугроз, повысить общую защищенность наземного сегмента космических линий связи:

Интерфейсная система обнаружения вторжений.

Система защиты основана на локальном наблюдении и анализе сетевых соединений, состоит из следующих основных частей:

a) Программная часть. Обнаружение отклонений от существующих настроек внутреннего и внешнего интерфейса криптомаршрутизатора позволяет: просматривать в режиме реального времени log file, журнал регистрации событий. В случаях выявления несанкционированного доступа оповещает администратора системы о возможных изменениях критических параметров программной части комплекса. Событие направлено на выявление противоправных действий злоумышленника в файловой системе на внешнем либо внутреннем хосте;

b) Аппаратная часть. За основу необходимо принять мониторинг сетевых соединений и сигнатурный анализ трафика. В случаях обнаружения аномалий в автоматическом режиме прервать существующие сетевые соединения по данному хосту до передачи процесса на уровень представления данных согласно эталонной модели OSI (Open System Information);

c) Сетевая часть. Поскольку криптомаршрутизатор оснащен внутренними и внешними сетевыми интерфейсами, система обнаружения вторжений не должна быть ограничена только входящим либо исходящим трафиком. Вредоносные воздействия, такие как сканирование портов, DDoS атаки, несанкционированные попытки проникновения в сеть могут происходить внутри сети и не отражаться на внешнем защищаемом периметре системы. В связи с чем, сетевая часть обнаружения вторжений должна производить комплексный мониторинг, в случаях выявления нелегитимного трафика [2] выполнять процедуру согласно пункту b).

Космическое пространство является наиболее развивающейся сферой, как с научной, так и с технической точки зрения. Острая борьба и соперничество между государствами порождают новые, технологически сложные способы разрушающего воздействия на космические информационные потоки.

В данной работе автором рассмотрены возможные сетевые атаки на наземный сегмент связи с КА. Представлены возможные способы выявления и обнаружения вторжений на основе дополнительных возможностей криптомаршрутизатора. При этом отмечено, что нет ни одного средства, способного предоставить абсолютную информационную безопасность. Надежная защита сетевого взаимодействия, а также сохранность критически важных данных возможна лишь в комплексе с необходимым набором программно-аппаратных средств, проведением жесткой политики безопасности и неукоснительным соблюдением требований информационной безопасности пользователей системы.

Литература

1. Аверьянов В.С, Карцан И.Н. Уязвимости современных IPS/IDS систем // Актуальные проблемы авиации и космонавтики: Сборник материалов VI Международной научно-практической конференции, посвященной дню

космонавтики / Под ред. Ю.Ю. Логинова. – Красноярск: СибГУ им. М.Ф. Решетнева, 2020. – С. 194-197.
2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – М.: МГТУ им. Н.Э. Баумана, 2016. – 415 с.
3. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В. Котенко, И.Б. Саенко, А.А. Чечулин; под общ. ред. И.В. Котенко, И.Б Саенко. – СПб.: БХВ – Петербург, 2019. – 400 с.
4. Балансировщики нагрузки [электронный ресурс]. – URL: www.aosabook.org/en/distisys.html (дата обращения: 01.12.2021).
5. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 1. Базовая модель. – Москва: Госсандарт России, 2006. – 58 с.

Д.Р. Белодед

Обеспечение психологической защищённости несовершеннолетних в сети Интернет в целях предотвращения преступлений против жизни и здоровья

Аннотация. Всемирная сеть интернет уже не первый год является пространством, в котором совершаются преступления против жизни и здоровья несовершеннолетних пользователей. Среди них – растление детей, вовлечение их в преступные группы, распространение наркотической зависимости, увлечение «смертельными играми», результатом которых становится запланированный суицид и др. Киберпреступления обретают глобальные масштабы и патологические формы. В настоящей статье рассмотрены некоторые преступления, совершаемые в интернете в отношении несовершеннолетних пользователей и предложены меры по обеспечению психологической защищенности пользователей.

Ключевые слова: киберпреступность, суицид, психологическая безопасность, интернет-преступность, несовершеннолетние пользователи сети интернет, детская порнография.

Возникновение интернета датируют 1969 годом, но его мировое распространение (в т. ч. появление в России) относят к периоду 1989-1991 гг. В 1995 году ответственность за интернет была передана в частные руки, после чего существенно возросло количество коммерческих поставщиков и пользователей услуг.[1] Возможность передачи данных посредством глобальной Сети стало рубежным технологическим и социальным событием, не только решившим многие сложные коммуникативные задачи, но и изменившим саму среду обитания человечества. К сегодняшнему дню это стало частью обыденной жизни взрослых и детей, и число пользователей уже близится к 5

[1] История Интернета. Информационное агентство РИА. [Электронный доступ]. URL: https://ria.ru/20190902/1558095640.html (дата обращения 13.12.2021).

миллиардам[1], что составляет 60% мирового населения. Интернет удобен и полезен для каждого пользователя, он расширяет границы знаний, позволяет получить доступ к необходимой информации из любой точки доступа, способствует онлайн-общению с родными и близкими посредством аудио- и видеосвязи, упрощает и ускоряет множество социально-психологических и иных процессов. Нынешнему пользователю уже невозможно отказаться от такого комфортного способа получения и передачи данных, оплаты товаров, услуг и потребления инфопродуктов.

Коммерциализация виртуального пространства, к сожалению, повлекла за собой и рост киберпреступности. Отсутствие надежных инструментов контроля над инфоданными приводит к разрушительным последствиям для психологической безопасности пользователей. Пользователем ресурсов и возможностей Сети может оказаться человек с сомнительной репутацией, с криминальным прошлым и с любым психическим заболеванием – в интернете все равны. И даже более того, различные формы отклоняющегося поведения, которое ранее подвергалось критике, преследованию, суду, в настоящее время на интернет-просторах легко обретает очертания современной нормы. Стало существенно проще собирать сообщества единомышленников, где их участники получают положительное подкрепление своим порой причудливым, в то и прямо запретным, наклонностям и начинают воспринимать их как варианты нормы.

Одним из самых распространённых преступлений против несовершеннолетних является детская порнография. По результатам исследования зарубежных коллег (Durkin K.F., DeLong R. L), подобные преступления чаще всего совершаются мужчинами старше 25 лет, 70% которых являются холостыми. У преступников оказывались материалы порнографического характера с несовершеннолетними участниками (почти половина изображений была с детьми возраста 4-6 лет).[2] Педофильные расстройства имеют давнюю историю, а в 80-х годах прошлого века была даже попытка их легализации в Западной Германии, США, Нидерландах, Канаде, Великобритании, которая так и не увенчалась успехом[3].

Не менее страшным и жестоким киберпреступлением против несовершеннолетних является доведением до суицида через «группы смерти»[4].

---

[1] Цифра дня: Сколько человек в мире пользуются интернетом? Ferra. [Электроный журнал]. URL: https://www.ferra.ru/news/techlife/cifra-dnya-skolko-chelovek-v-mire-polzuyutsya-internetom-29-01-2021.htm (дата обращения 10.12.2021).

[2] Durkin K. F., DeLong R. L. Internet crimes against children. Encyclopedia of Cyber Behavior. 2012, № 1. Pp. 799-807. DOI: 10.4018/978-1-4666-0315-8.ch066. URL: https://www.researchgate.net/publication/288096120_Internet_crimes_against_children (дата обращения 12.12.2021)

[3] Rogers T. A Major German Political Party Used to Support Pedophilia—And It's Coming Back to Haunt Them. 2014. The online version of The New Republic magazine. URL: https://newrepublic.com/article/120379/german-green-party-pedophilia-scandal (дата обращения 13.12.2021).

[4] Миронова М. Н. Наши дети и деструктивные интернет-сообщества. М. Просветитель. 2021. 165 с.

Классификация суицида насчитывает множество его видов[1], но общим для всех них является то, что эти преступления приводят к реальной гибели ребенка, когда единственным способом избавления от мучительных психоэмоциональных терзаний детям представляется лишение себя жизни. По различным причинам каждый год намерено уходят из жизни 703 тысячи человек, в разы больше количество тех, кто совершает попытки, но не достигают запланированного результата.[2] Использование интернета для подготовки пользователей к самоубийству было впервые зарегистрировано в Японии в 2000 году.[3] За минувшие 20 лет это явление получило широкое распространение и теперь с «кураторами смерти» борется весь мир.

В условиях культуроразрушающих тенденций во Всемирной сети, подменой идеалов, демонстрацией роскоши и суррогата истинных чувств сложно сохранять психологическую защищенность, особенно тяжело приходится несовершеннолетним пользователям. Гормональные изменения подросткового периода, смена авторитетов, первое осознание своей «самости» (по К.Г. Юнгу), поиск границ самой самодостаточности, мысли о профессиональном самоопределении – всё это оказывает серьёзную психофизиологическую и психологическую нагрузку на формирующую личность молодого человека, с которой бывает сложно справиться самостоятельно. Замыкание в себе, зацикленность на нерешаемых проблемах – всё больше усугубляют положение, подросток расценивает свою ситуацию тупиковой и пытается выбраться из нее посредством ответов и подсказок Сети. И если в таком состоянии подросток попадает в деструктивное сообщество, то может случиться трагедия – подчас подросток не видит других выходов, кроме как сведения счетов с жизнью. Самоубийство занимает четвертое по значимости место в причине смертности для лиц в возрасте 15-19 лет. Хотя помощь психолога может предотвратить неблагоприятный исход благодаря психодиагностическим методикам и инструментам коррекции потенциально опасных личностных особенностей[4], не все, к сожалению, знают о таких возможностях, если и знают, не всегда своевременно обращаются за помощью.

Для оказания своевременной психологической помощи важно уметь распознавать признаки возможных суицидальных размышлений. Среди них могут быть: резкие перемены в общении, глубокие эмоциональные переживания, апатичное состояние, бессонница, плохой аппетит, повышенный интерес к загробному миру, раздаривание личных вещей, повышенное

---

[1] Енгалычев В.Ф. Посмертная судебно-психологическая экспертиза // Прикладная юридическая психология: учебное пособие для вузов / / В.Ф. Енгалычев, под ред. А.М. Столяренко, М: ЮНИТИ-ДАНА, 2001. 420-430 с.

[2] Самоубийство. Основные факты. ВОЗ. [Электронный доступ]. URL: https://www.who.int/ru/news-room/fact-sheets/detail/suicide (дата обращения 15.12.2021).

[3] Naito A. Internet suicide in Japan. Clin Child Psychol Psychiatry. 2007. 12(4). Pp. 583–597 URL: https://pubmed.ncbi.nlm.nih.gov/18095539/ (дата обращения 18.12.2021).

[4] Енгалычев В.Ф. Психологические основы вузовской подготовки специалистов в юридической психологии //Дисс. на соиск. уч. ст. д.псих.н./ В.Ф. Енгалычев, СПб: 2006. 530 с.

внимание к возможным орудиям суицида и др.[1] Нередко заранее готовят предсмертные записки.[2] Всемирная организация здравоохранения осуществляет мониторинг пациентов, склонных к самоубийству и предлагает ряд рекомендаций по его предотвращению. В их число входит – ограниченный доступ к возможным средствам преступления против жизни, например, к огнестрельному оружию; психолого-педагогические мероприятия в образовательных учреждениях, предложения по сокращению алкогольного и наркотического опьянения, подготовка медицинских работников.[3]

Мероприятия по обеспечению психологической защищенности несовершеннолетних должны быть направлены, в первую очередь, на контроль контента, доступного детям. Самые надежные инструменты контроля должны быть утверждены на государственном уровне, так как физически и психически здоровое молодое поколение является лучшим гарантом национальной безопасности. Не менее значимым условием предотвращения угроз психологической безопасности является обстановка в семье: внимание к проблемам друг друга, любовь, поддержка, уважение и забота.

Предоставляя доступ к Всемирной сети несовершеннолетнему пользователю, надо осознавать, что потенциально деструктивной информации в ней гораздо больше, чем может показаться на первый взгляд. Со стороны лиц, ответственных за информационную безопасность государства, за семейную политику (защиту детства), необходимо утверждение четких правил, регулирующих размещение и потребление деструктивного контента. Помимо ответственности государственных структур, важно помнить об ответственности родителей и образовательных учреждений за воспитание детей, становление личности и её социализацию.

В последнее время в нашей стране неоднократно предпринимались попытки совершенствования законодательства по части подготовки законов, подзаконных актов и решений отдельных министерств по защите интересов молодого поколения в интернете. Представляется целесообразным включение в комиссии по разработке таких документов и решений известных судебных экспертов-психологов, имеющих опыт исследований и экспертиз всего спектра криминального психологического воздействия на несовершеннолетних в цифровом пространстве.

---

[1] Войцех В. Ф. Что мы знаем о суициде. Под редакцией профессора В. С. Ястребова. М. 2007. 20 с.

[2] Chernov Y., Engalychev V. Formal handwriting analysis as an instrument for forensic and criminal psychology // Armenian journal of mental health: Current issues of forensic psychology. 2018 (9). № 1, P. 140–143.

[3] Самоубийство. Основные факты. ВОЗ. [Электронный доступ]. URL: https://www.who.int/ru/news-room/fact-sheets/detail/suicide (дата обращения 15.12.2021).

Литература

1. Chernov Y., Engalychev V. Formal handwriting analysis as an instrument for forensic and criminal psychology // Armenian journal of mental health: Current issues of forensic psychology. 2018 (9). № 1, P. 140–143.
2. Durkin K. F., DeLong R. L. Internet crimes against children. Encyclopedia of Cyber Behavior. 2012, № 1. Pp. 799-807. DOI: 10.4018/978-1-4666-0315-8.ch066. URL: https://www.researchgate.net/publication/288096120_Internet_crimes_against_children (дата обращения 12.12.2021).
3. Naito A. Internet suicide in Japan. Clin Child Psychol Psychiatry. 2007. 12(4). Pp. 583–597 URL: https://pubmed.ncbi.nlm.nih.gov/18095539/ (дата обращения 18.12.2021).
4. Rogers T. A Major German Political Party Used to Support Pedophilia—And It's Coming Back to Haunt Them. 2014. The online version of The New Republic magazine. URL: https://newrepublic.com/article/120379/german-green-party-pedophilia-scandal (дата обращения 13.12.2021).
5. Бычкова А.М., Раднаева Э.Л. Доведение до самоубийства посредством использования интернет-технологий: социально-психологические, криминологические и уголовно-правовые аспекты // Всероссийский криминологический журнал. 2018. №1. С. 101-115.
6. Войцех В. Ф. Что мы знаем о суициде. Под редакцией профессора В. С. Ястребова. М. 2007. 20 с.
7. Енгалычев В.Ф. Посмертная судебно-психологическая экспертиза // Прикладная юридическая психология: учебное пособие для вузов / / В.Ф. Енгалычев, под ред. А.М. Столяренко, М: ЮНИТИ-ДАНА, 2001. 420-430 с.
8. Енгалычев В.Ф. Психологические основы вузовской подготовки специалистов в юридической психологии //Дисс. на соиск. уч. ст. д.псих.н. / В.Ф. Енгалычев, СПб: 2006. 530 с.
9. История Интернета. Информационное агентство РИА. [Электронный доступ]. URL: https://ria.ru/20190902/1558095640.html (дата обращения 13.12.2021).
10. Миронова М. Н. Наши дети и деструктивные интернет-сообщества. М. Просветитель. 2021. 165 с.
11. Самоубийство. Основные факты. ВОЗ. [Электронный доступ]. URL: https://www.who.int/ru/news-room/fact-sheets/detail/suicide (дата обращения 15.12.2021).
12. Цифра дня: Сколько человек в мире пользуются интернетом? Ferra. [Электроный журнал]. URL: https://www.ferra.ru/news/techlife/cifra-dnya-skolko-chelovek-v-mire-polzuyutsya-internetom-29-01-2021.htm (дата обращения 10.12.2021).

К.П. Грицианова
Научный руководитель: **Проваторова К.В.**

Борьба с киберпреступностью в мире

Аннотация. В настоящее время направления деятельности правоохранительных органов, связанное с борьбой против киберпреступлений, характеризуется использованием стереотипных методов и приемов, не учитывающих особенностей новых видов преступлений, отсутствие наработанных методик, несовершенство нормативной базы. Возникает необходимость пересмотра не только методов организации предварительного расследования в отношении «компьютерных» преступлений, но и многих устоявшихся юридических взглядов, уголовно-правовых и уголовно-процессуальных механизмов. В этой связи немаловажным представляется изучение соответствующего опыта государств, также как и Россия столкнувшихся с проблемами Интернет-мошенничеств, возникает необходимость исследования вопросов противодействия киберпреступности в мире и рассмотрения мер, предпринимаемых не только Российской Федераций, но и зарубежными странами в указанном направлении.

Ключевые слова: кибератаки, интернет, киберзащита, глобальные сети, интернет-мошенничества.

Быстрое развитие информационно-коммуникационных технологий (ИКТ) в наше время является преимущественно положительным явлением, ведь оно охватывает все сферы деятельности человека, а также упрощает его жизнь, однако при всех положительных воздействиях, человечество не предвидело, какие возможности для злоупотребления смогут создать эти технологии. Сегодня не только отдельные люди, но и вся страна могут стать жертвами преступников, действующих в киберпространстве. В этом случае несколько злоумышленников могут повлиять на безопасность тысяч пользователей. Повышение опасности связывается и с тем, что уязвимостью глобальных сетей для достижения своих целей могут воспользоваться не только иные государства, преступные и террористические группировки, но даже отдельные личности с относительно невысоким уровнем подготовленности. Процесс, который некоторые исследователи называют «демократизацией высоких технологий»[1], приводит к тому, что в настоящее время такие лица способны организовать сбои в работе национальных и глобальных информационных структур. Небольшая компьютерная программа может в определенных обстоятельствах причинить более существенный ущерб, чем взрыв бомбы. При этом затраты на реализацию «компьютерного» нападения и риск быть в дальнейшем обнаруженным, как правило, несоизмеримо ниже, чем для «традиционных» видов террористических действий.

[1]Гридчин М.М. Проблемы влияния информационных технологий на молодежь [Электронный ресурс] URL: https://cyberleninka.ru/article/n/problemy-vliyaniya-informatsionnyh-tehnologiy-na-molodezh/viewer (дата обращения 24.11.2021).

Нарастание, усложнение и видоизменение преступной деятельности, связанной с использованием глобальных компьютерных сетей, происходит постоянно, и нет никаких оснований считать, что в ближайшее время ситуация может измениться в лучшую сторону.

Согласно данным в исследовании IT-компании «Positive Technologies» (международная компания, специализирующаяся на разработке инновационных решений в сфере информационной безопасности), число кибератак в мире во втором квартале 2021 года увеличилось на 0,3% по сравнению с первым кварталом года, при этом на 16% выросла доля связанных с получением финансовой выгоды атак на организации[1].

Основными причинами развития и роста информационной преступности являются ее транснациональный характер и определенные технические особенности, такие как отсутствие материальных следов и анонимность пользователей Интернета. Кроме этого, сложности в раскрытии и расследовании преступлений указанной категории возникают в связи с отсутствием у сотрудников оперативных и следственных подразделений полноценных знаний и опыта в данном направлении, а также достаточной оперативности при сборе сведений, подлежащих установлению. Производство следственных действий при расследовании Интернет-мошенничеств осложняется довольно высоким уровнем технической и юридической грамотностью мошенников, умелым использованием преступниками технологий, позволяющих работать инкогнито в сети Интернет и уничтожать следы совершенных правонарушений.

Первыми попытками создания законодательства для кибербезопасности предприняты в США и странах Европейского союза. Особенностью финансовой системы США можно назвать безналичный формат средств. Кредитные карты имеет практически каждый житель США, и 49% всех преступлений в США приходится на «кардинг» и только 18% на кражу конфиденциальной информации. Срок наказания за указанный вид преступления достаточно жестокий и достигает 7 лет лишения свободы.

По вопросам борьбы с киберпреступностью США выдвинуло новую инициативу, согласно которой правительственные подрядчики этой страны, скрывшие факт киберинцидента от уполномоченных органов, будут отвечать за это по суду. Борьба с кибермошенничеством предусматривает, что ведомство будет привлекать к суду и тех правительственных подрядчиков, что не обеспечили себе киберзащиту, соответствующую стандартным требованиям[2].

В 2021 году Европейский союз ужесточил регулирование интернета. В конце апреля 2021 года Европейский парламент принял закон, требующий от интернет-компаний «удалять или отключать доступ к контенту, помеченному как террористический» в течение одного часа после уведомления национальных

[1] Исследование: количество кибератак в мире выросло на 0,3% во II квартале 2021 [Электронный ресурс] URL: https://tass.ru/ekonomika/12250541 (дата обращения 24.11.2021).

[2] Власти США будут отдавать IT-компании под суд за плохую киберзащиту [Электронный ресурс] URL: https://www.cnews.ru/news/top/2021-10-08_v_ssha_itkompanii_budut_otdavat (дата обращения 24.11.2021).

властей[1]. Данный закон исключает удаление террористических материалов, которые являются частью любых образовательных, художественных, журналистских или академических материалов.

В Германии действует закон «О мерах в отношении социальных сетей», вступивший в силу 1 января 2018 года, который обязывает крупные сетевые платформы («Facebook», «Instagram», «Twitter», «YouTube», оперативно удалять «незаконный контент»[2], признаваемый таковым по 22 разделам УК.

В октябре 2020 года правительство Германии одобрило законопроект, позволяющий предоставлять доступ спецслужбам к переписке пользователей мессенджеров, таким как «WhatsApp» и «Facebook Messenger, с целью сделать борьбу с терроризмом и киберпреступностью более эффективной.

В Ирландии ответственность за преступления в сфере технологий предусмотрена Актом о криминальном ущербе 1991 года. Субъекты, которые использует компьютер на территории государства с целью получения данных или нарушения личных прав других виновно в совершении преступления, несмотря на то, получило ли лицо определенную информацию[3]. При этом подобное деяние наказывается штрафом или заключением под стражу до трех месяцев.

Закон КНР от 2017 года «О кибербезопасности» регламентирует действия поставщиков сетевых продуктов и услуг по сбору, хранению и обработке пользовательских данных, он также регулирует обеспечение информационной безопасности в стратегически важных отраслях[4]. В законе провозглашается защита национального киберсуверенитета КНР, за нарушения предусмотрены штрафы до миллиона юаней в зависимости от тяжести киберпреступления.

В Великобритании с августа 1990 года действует Акт о компьютерных злоупотреблениях. Основой Акта является неуполномоченный доступ к компьютерным данным. Им установлено, что лицо совершившее преступление, при использовании компьютера с намерением обеспечить доступ к любой программе или данным, содержащимся в любом компьютере, если этот доступ заведомо неправомочен, признается виновным, и за совершение этого преступления предусматривается наказание в виде штрафа или заключения на срок до 6 месяцев.

В России к категории киберпреступлений относятся: неправомерный доступ к компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК); нарушение

---

[1]«IT-гиганты сами не справляются»: какова роль государств в обуздании соцсетей [Электронный ресурс] URL: https://news.rambler.ru/internet/46902467-it-giganty-sami-ne-spravlyayutsya-kakova-rol-gosudarstv-v-obuzdanii-sotssetey/ (дата обращения 24.11.2021).

[2]Германия: новый закон о соцсетях [Электронный ресурс] URL: https://www.hrw.org/ru/news/2018/02/14/314928 (дата обращения 24.11.2021).

[3] Законодательство о киберпреступлениях в зарубежных странах [Электронный ресурс] URL: https://ria.ru/20130809/955198703.html (дата обращения 24.11.2021).

[4] Закон о кибербезопасности к КНР [Электронный ресурс] URL: https://kartaslov.ru/ (дата обращения 23.11.2021).

правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК); мошенничество с использованием платежных карт (ст. 159.3 УК РФ);

Основными нормативными актами, затрагивающими вопросы борьбы с киберпреступлениями в России, остаются Федеральный закон № 187 от 01.01.20218 года «О безопасности критически важной информационной инфраструктуры Российской Федерации», Федеральный закон «О связи» от 07.07.2003 № 126, Федеральный закон «О безопасности» от 28.12.2010 № 390, Федеральный закон «Об электронной подписи» от 06.04.2011 № 63, Федеральный закон «О персональных данных» от 27.07.2006 № 152.

В настоящее время Россия выступила с предложением к Организации Объединенных Наций на международном уровне классифицировать киберпреступления на 23 вида и внесла проект конвенции, направленный на противодействие киберпреступлениям, который подразумевает увеличение количества составов подобного рода преступлений, совершающихся посредством сотовой связи и сети Интернет.

В данной конвенции нашли отражение следующие составы преступлений:

-несанкционированный доступ к персональным данным;

-незаконное распространение фальсифицированных лекарственных средств и медицинских изделий;

-терроризм;

-экстремизм;

-реабилитация нацизма;

-незаконный оборот наркотиков, оружия;

-вовлечение несовершеннолетних в противоправную деятельность.

В проекте делается особый акцент на процедурных аспектах и экстренных механизмах взаимодействия, повышающих скорость и эффективность работы правоохранительных органов в рамках расследований киберпреступлений трансграничного характера, которые требуют «мгновенной реакции».

Анализ зарубежного и российского законодательства показывает, что в современных условиях государства по-разному справляются с проблемами в сфере интернет-преступности, и единого алгоритма действия не выработано до сих пор, но во всем мире просматриваются тенденции к ужесточению регулирования сети Интернет, и возможно законопроект, предложенный Российской Федерацией, отвечающий проблемам и запросам настоящего времени, позволит более эффективно организовать борьбу с киберпреступностью, как на отечественном уровне, так и за рубежом.

Литература

1. Антивирусная правда [Электронный ресурс] URL: https://www.drweb.ru/pravda/issue/?number=646&lng=en (дата обращения 23.11.2021).

2. Власти США будут отдавать IT-компании под суд за плохую киберзащиту [Электронный ресурс] URL: https://www.cnews.ru/news/top/2021-10-08_v_ssha_itkompanii_budut_otdavat (дата обращения 24.11.2021).
3. Гридчин М.М. Проблемы влияния информационных технологий на молодежь [Электронный ресурс] URL: https://cyberleninka.ru/article/n/problemy-vliyaniya-informatsionnyh-tehnologiy-na-molodezh/viewer (дата обращения 24.11.2021).
4. Германия: новый закон о соцсетях [Электронный ресурс] URL: https://www.hrw.org/ru/news/2018/02/14/314928 (дата обращения 24.11.2021).
5. Законодательство о киберпреступлениях в зарубежных странах [Электронный ресурс] URL: https://ria.ru/20130809/955198703.html (дата обращения 24.11.2021).
6. Закон о кибербезопасности к КНР [Электронный ресурс] URL: https://kartaslov.ru/ (дата обращения 23.11.2021).
7. Исследование: количество кибератак в мире выросло на 0,3% во II квартале 2021 [Электронный ресурс] URL: https://tass.ru/ekonomika/12250541 (дата обращения 24.11.2021).

К.О. Даценко, В.Г. Кузина
Научный руководитель: **Скуковский А.Г.**

Определение местоположения технического средства участника уголовного судопроизводства, оборудованного приемными и передающими модулями систем GPS, ГЛОНАСС, по беспроводным сетям Wi- Fi и по базовым станциям сотовой связи

Аннотация. В данной статье рассмотрены методы определения географических координат с использованием технического средства участника уголовного судопроизводства, оборудованного приемными и передающими модулями систем GPS, ГЛОНАСС, беспроводных сетей Wi-Fi и базовых станций сотовой связи в процессе расследования преступлений.

Ключевые слова: расследование, система GPS, система ГЛОНАСС, спутниковые технологии навигации, беспроводные сети Wi-Fi.

Задача определения местоположения участника уголовного судопроизводства заключается в определении его координат на поверхности Земли.

В настоящее время применяются следующие системы определения местоположения: при помощи спутниковых навигационных систем (ГЛОНАСС, GPS); по беспроводным сетям Wi-Fi; системы определения координат по базовым станциям GSM.

В настоящее время существует две глобальных системы спутникового позиционирования: американская система глобального позиционирования GPS и российская система ГЛОНАСС. С помощью данных систем возможно определить местоположение абонентского оборудования, в роли которого может

выступать сотовый телефон, смартфон, навигатор, часы, планшетный компьютер или любое другое устройство с GPS или ГЛОНАСС приемником.[1]

Подобные системы активно разрабатываются в различных странах, хотя с технической точки зрения достаточно и одной системы для обслуживания.

В данной статье рассмотрен принцип работы системы спутникового позиционирования GPS, так как принцип работы у систем спутникового позиционирования GPS и ГЛОНАСС во многом схож.

При определении местоположения участника уголовного судопроизводства с помощью системы позиционирования GPS, используется трехмерная система координат под названием «WGS 84», которая охватывает всю планету Земля. Данная система спутникового позиционирования состоит из 31 спутника, которые вращаются на земной орбите в 6 плоскостях, в каждой плоскости находится от 4 до 6 космических аппаратов, располагающихся на высоте 20 350 км и передвигающихся со средней скоростью около 14 000 км в час.[2]

В любой точке планеты Земля в зоне приема GPS-навигатора будет находиться как минимум 4 космических спутника. GPS-спутники передают три навигационных сигнала на трех частотах: L1 (1575.42 МГц), L2 (1227.60 МГц) и L5 = 1176,45 МГц. Данные сигналы могут быть приняты обычной антенной в так называемой «зоне прямой видимости» и использоваться для вычисления местоположения абонентского устройства. Вычисление местоположения производит непосредственно абонентское оборудование при этом без необходимости передавать вычисления обратно на спутник.

Каждый космический спутник имеет на борту очень точные атомные часы, которые синхронизируются с такими же часами на Земле. Синхронизация часов необходима вследствие того, что в сутки из-за гравитационного замедления времени часы на спутнике начинают отставать на 38 микросекунд. Высокая точность секунд является необходимым критерием при определении географических координат абонентского устройства. Причина кроется в самом принципе определения местоположения приемника, который заключается в измерении разницы между временем передачи и временем приема, то есть вычисляется время, за которое сигнал от спутника дошел до абонента. Для вычисления координат приемника на местности необходимо знать точные координаты космических спутников, от которых принимаем сигнал, но так как спутники постоянно перемещаются и их координаты меняются, то это становится сложной задачей. Для оперативного расчета, а также уменьшения стоимости пользовательской аппаратуры вычисление максимально возможного объема данных возложено на наземный комплекс управления, в котором рассчитывается прогноз параметров орбиты спутников в фиксированные моменты времени. Иными словами, зная параметры орбиты и точные

[1] Калюжный А.Н. Использование возможностей средств сотовой связи в раскрытии и расследовании преступлений, посягающих на свободу личности // Вестник Восточно-Сибирского института МВД России. 2018. № 1(84). С. 118-124.

[2] Кукк К.И. Низкоорбитальная комбинированная спутниковая система связи и мониторинга, в том числе для Арктического региона // Спутниковая связь и вещание – 2014. Специальный выпуск журнала «Технологии и средства связи». С. 87-96.

координаты спутника можно вычислить точное расположение спутника в производный момент времени. Наземные станции передают спутникам навигационные сообщения, содержащие данные эфемерид и альманах. Датчики, находящиеся на спутнике в беспрерывном режиме, передают навигационные сообщения, содержащие эфемериды с метками времени и альманахом. Пользовательская аппаратура принимает такое навигационное сообщение и, опираясь на заложенный в памяти предыдущий альманах, максимально быстро и точно определяет собственные координаты.[1]

Для определения местоположения участника уголовного судопроизводства необходимо наличие четырех и более космических спутников, находящихся на данной территории. Для устранения неверного решения и уточнения местоположения необходимы данные четвертого спутника, после чего местоположение будет точно установлено.

На практике все обстоит намного сложнее. Например, существует влияние ионосферы и тропосферы, где скорость сигнала замедляется, а также существуют естественные и искусственные препятствия для прохождения радиоволн, сигнал имеет свойство отражаться от поверхности, что приводит к увеличению расстояния, которое он проходит до приемника, и соответственно вызывает погрешность в результатах. В связи со всеми погрешностями приходится корректировать сигнал от спутников с помощью наземных станций, в том числе наземных технологий Wi-Fi и GSM.

В процессе расследования преступлений активно используются данные GPS и ГЛОНАСС позиционирования. Так, полицейские установили, что А. добрался до работы, но оттуда вместе с другим мужчиной Б. выехал за пределы населенного пункта на заводском автобусе. Между Б. и А. возник конфликт. В ходе ссоры Б. выстрелил в мужчину А. из огнестрельного оружия. От полученных телесных повреждений А. скончался. Злоумышленник решил оставить тело А. за городом. При помощи системы спутникового позиционирования ГЛОНАСС был установлен маршрут заводского автобуса. Тело А. было обнаружено в сугробе на пути следования транспортного средства.[2]

Принцип действия GSM-позиционирования очень похож на работу спутниковых навигационных систем, только здесь роль спутников играют наземные базовые станции сотовой сети. Площадь, охватываемая сетью GSM, разбита на ячейки, каждую из которых обслуживает базовая приемопередающая станция. Базовая станция, как правило, имеет от 2 до 6 передатчиков, которые имеют антенны с диаграммой направленности 120 градусов и равномерно покрывают площадь. В малонаселенных пунктах используются 900 МГц станции, имеющие зону покрытия от 400 до 35 км. В густозаселенных районах

[1] Финогеев А.Г., Маслов В.А. Сравнительный анализ методов позиционирования в беспроводных системах связи // Телематика – 2009. Сборник трудов XVI Всероссийской научно-методической конференции. - М., 2009. - С. 283-284.

[2] Никитин А. Совмещенные приемные модули систем ГЛОНАСС/GPS производства КБ «Геостар Навигация» // Новости электроники. - Рыбинск, 2010. - №4. - С. 7.

дополнительно могут устанавливаться 1800 МГц станции, имеющие зону покрытия от 200 м до 1,5 км.[1]

Так же, как в спутниковых навигационных системах, для определения географических координат технического средства, необходимо определить расстояния между базовыми станциями и устройством, а затем решить систему уравнений. Существуют два метода определения расстояния – дальномерный и угломерный. При реализации дальномерного метода на базовых станциях измеряется время распространения сигнала от передатчика GSM, установленного на абонентском устройстве до базовой станции. Здесь можно выделить два способа определения координат UL-TOA (Up Link Time Of Arrival – от англ. время прибытия) и E-OTD (Enhanced Observed Time Difference – от англ. соблюдаемая разница во времени). Метод UL-TOA основан на измерении интервалов времени прохождения сигнала от мобильной станции до нескольких базовых станций. В системе работают мобильная и три базовые станции, координаты которых известны. При этом часы на всех базовых станциях должны быть строго синхронизированы. Передатчик GSM, установленный на мобильной станции, посылает сигнал, который принимают все базовые станции. Базовые станции, в свою очередь, определяют время получения сигнала и передают эти данные далее в вычислительный центр, где и рассчитываются координаты технического средства. В вычислительном центре решается система уравнений, в результате чего определяются координаты абонентского устройства. Недостатком этой системы является необходимость синхронизации часов всех базовых станций.

При определении координат методом E-OTD синхронизации часов базовых станций не требуется. Система состоит из мобильной станции, трех базовых станций и вычислительного центра. Координаты вычислительного центра и базовых станций известны. Часы мобильной станции и вычислительного центра не синхронизированы – на каждых часах свое время. Первая базовая станция посылает сигнал на мобильную станцию и в вычислительный центр. На мобильной станции определяется время прибытия сигнала, а затем его значение отправляется на вычислительный центр. При реализации угломерного метода измерения базовые станции определяют углы α, β направления прихода сигнала от GSM передатчика, установленного на абонентском устройстве относительно линии, соединяющей две сотовые станции сети. Пересечение пеленгов двух (или большего числа) базовых станций определяют положение устройства.[2]

При определении географических координат по беспроводным сетям Wi-Fi, в первую очередь служба геолокации смартфонов применяет для определения местоположения устройства модуль GPS. Если позиция успешно вычислена,

---

[1] Васильченко А.А., Кочуров А.В., Сорокин О.И. Формализация алгоритма установления соединения в сети сотовой связи GSM // Радиоэлектронные устройства и системы для инфотелекоммуникацион-ных технологий: сб. тр. междунар. конф. М.: Попов, 2016. Т. 2. С. 310-317.

[2] Головчанский А.В. Об использовании средств спутниковой навигации в целях установления и фиксации координат места происшествия // Вестник Воронежского института МВД России. 2015. №2. С. 62-69.

устройство сканирует Wi-Fi-эфир и отправляет через сеть Интернет данные о географическом положении близлежащих точек доступа Wi-Fi, которые собираются в общую базу данных производителя системы геолокации операционной системы: для смартфонов Android — в базу данных Google; для смартфонов iPhone — в базу данных Apple. Данная информация используется как приложениями Google и Apple, так и другими, установленными на смартфоне (фитнес-трекерами и др.).

У производителя операционной системы смартфона формируется и поддерживается в актуальном состоянии глобальная база данных о месторасположении всех точек доступа Wi-Fi. Она помогает определять местоположение персонального портативного устройства в случае, когда рядом есть Wi-Fi, но нет GPS-сигнала. Смартфон отправляет через Интернет данные о близлежащих точках доступа Wi-Fi и получает в ответ данные о своем местоположении. Польза для владельца смартфона в этом случае очевидна: смартфон быстро и точно определяет местоположение в любой точке Земли.[1]

Производитель ОС собирает и хранит историю перемещения каждого устройства. Сохраняются не только географические точки, но и детализированные маршруты. Передачу данных о местоположении можно отключить, но в этом случае маршруты перестанут сохраняться, а вот географические точки все равно будут отображаться.

Для установления местоположения участников уголовного судопроизводства следователи, в процессе расследования преступлений, чаще всего используют данные базовых станций. Одним из примеров является уголовное дело по обвинению сотрудника полиции Кухаркина в вымогательстве и получении взятки в крупном размере. Так, первую часть взятки он получил за шесть месяцев до того, как был задержан при получении второй части суммы. Кухаркин выдвинул алиби о том, что он не мог участвовать в получении первой части денег, так как в период с 27 февраля по 10 марта он находился в служебной командировке за пределами города, что подтверждалось командировочными документами. Следователем по постановлению суда была получена статистика соединений телефона Кухаркина в данный период с указанием базовых станций. При анализе статистики было установлено, что Кухаркин действительно до 6 марта находился в командировке за пределами города, о чем свидетельствовали базовые станции, с которыми связывался телефон. 6 марта было установлено передвижение абонента по трассе в город, а также последующие вызовы абонента с территории города. Также путем анализа статистики соединений в указанный период были установлены свидетели, которые подтвердили факт проезда Кухаркина в город с остановкой и ремонтом машины, а также установлена жительница города, у которой Кухаркин ночевал в ночь с 6 на 7 марта. Алиби обвиняемого было опровергнуто.[2]

---

[1] Романов В.И. Криминалистическая техника и потребности следственной практики // Рос. следователь. 2015. № 24. С. 13-16.

[2] Ковтун Ю.А., Рудов Д.Н. Проблемные аспекты расследования мошенничеств, совершаемых с использованием мобильной связи // Проблемы правоохранительной деятельности. 2013. № 2. С. 61-64.

Стоит отметить тот факт, что в 2020 году в Российской Федерации было продано рекордное количество смартфонов (порядка 31 млн. девайсов на сумму около 570 млрд. рублей[1]), что свидетельствует о распространенности данных электронных устройств с приемными и передающими модулями систем GPS, ГЛОНАСС, Wi-Fi среди населения, что предоставляет широкие возможности правоохранительным органам с точки зрения информационного обеспечения для раскрытия и расследования преступлений.

Литература

1. Калюжный А.Н. Использование возможностей средств сотовой связи в раскрытии и расследовании преступлений, посягающих на свободу личности // Вестник Восточно-Сибирского института МВД России. 2018. №1 (84). С. 118-124.
2. Кукк К.И. Низкоорбитальная комбинированная спутниковая система связи и мониторинга, в том числе для Арктического региона // Спутниковая связь и вещание – 2014. Специальный выпуск журнала «Технологии и средства связи». С. 87-96.
3. Финогеев А.Г., Маслов В.А. Сравнительный анализ методов позиционирования в беспроводных системах связи // Телематика – 2009. Сборник трудов XVI Всероссийской научно-методической конференции. - М., 2009. - С. 283-284.
4. Никитин А. Совмещенные приемные модули систем ГЛОНАСС/GPS производства КБ «Геостар Навигация» // Новости электроники. - Рыбинск, 2010. - №4. - С. 7.
5. Васильченко А.А., Кочуров А.В., Сорокин О.И. Формализация алгоритма установления соединения в сети сотовой связи GSM // Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий: сб. тр. междунар. конф. М.: Попов, 2016. Т. 2. С. 310-317.
6. Головчанский А.В. Об использовании средств спутниковой навигации в целях установления и фиксации координат места происшествия // Вестник Воронежского института МВД России. 2015. №2. С. 62-69.
7. Романов В.И. Криминалистическая техника и потребности следственной практики // Рос. следователь. 2015. № 24. С. 13-16.
8. Ковтун Ю.А., Рудов Д.Н. Проблемные аспекты расследования мошенничеств, совершаемых с использованием мобильной связи // Проблемы правоохранительной деятельности. 2013. № 2. С. 61-64.
9. ТАСС. Информационное агентство. Продажи смартфонов в России в 2020 году достигли рекордных 570 млрд рублей // [Электронный ресурс]. URL: https://tass.ru/ekonomika/10375261 (Дата обращения 26.11.2021).

[1] ТАСС. Информационное агентство. Продажи смартфонов в России в 2020 году достигли рекордных 570 млрд рублей // [Электронный ресурс]. URL: https://tass.ru/ekonomika/10375261 (Дата обращения 26.11.2021).

Е.А. Илларионова

Механизм следообразования при совершении кибермошенничества

Аннотация. В статье обращается внимание на проблемы, связанные с образованием, обнаружением, фиксацией и изъятием следов при совершении кибермошенничества. Исследование механизма следообразования рассматривается через призму установления наиболее характерного способа совершения такого рода преступления. Данная характеристика позволяет установить распространенные следовоспринимающие объекты преступного посягательства. В связи с этим, основной задачей определения механизма следообразования конкретного преступления является создание на первоначальных этапах расследования наиболее эффективной программы первоначальных следственных действий и оперативно-розыскных мероприятий.

Ключевые слова: кибермошенничество; механизм следообразования; следовоспринимающие объекты; следообразующие объекты; способ совершения преступления; виртуальный след; Интернет-пространство.

Механизм следообразования может быть определен как особая форма протекания процесса, имеющая своим итогом образование следа, обусловленного спецификой следового контакта, процесс воздействия на объекты окружающей обстановки (следовоспринимающие объекты).

При описании криминалистической характеристики преступлений выделяют несколько этапов, которые отражают типичные закономерности формирования действий преступников на определенных этапах, что позволяет смоделировать конкретное преступление, определить основные следовоспринимающие объекты, спрогнозировать процесс его раскрытия и расследования. Первый этап – подготовительный, большинство преступлений такого рода совершаются преступной группой, которая заранее разрабатывает план криминальной операции, способ совершения преступления, подготавливает средства совершения преступного посягательства. Второй этап – реализация преступного умысла, зависящая от избранного способа совершения преступления, но главным является незаконное завладение чужим имуществом путем использования интернет-ресурсов. Важным определяющим моментом считается получение возможности распорядиться полученным (вывод активов). Последний этап – использование результатов преступления, они могут быть распределены между участниками или направлены на создание другого совместного «бизнеса» либо на усовершенствование имеющегося. [1]

Механизм следообразования напрямую связан со способом совершения преступления. В научной литературе под способом преступления понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, составляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего события, своеобразии

[1] Вехов Б.В. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: монография / Б. В. Вехов. Волгоград, 2005. С. 276.

преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия и расследования преступления.[1] Способов совершения кибермошенничества существует множество, они постоянно прогрессируют в связи с увеличением темпа технического прогресса, но существуют наиболее типичные, которые лежат в основе совершения преступления, сочетаясь с новыми видами технических злоупотреблений. Зачастую для совершения мошенничества в сфере компьютерной информации используются различные вредоносные программы – программное обеспечение, которое предназначено для несанкционированного доступа к персональному компьютеру с целью похищения конфиденциальных данных, а также для нанесения связанного с его использованием ущерба. Все вредоносные программы в научной литературе делят на три группы: компьютерные вирусы – программы, способные «размножаться» и внедрять свои прототипы в иные программы, то есть заражают существующие файлы, которые становятся вредоносными; сетевые черви – это вредоносные программы, представляющие собой отдельный файл, то есть при размножении не становятся частью иных файлов; троянские программы, задачей которых является обеспечение злоумышленнику доступа к персональному компьютеру пользователя с целью управления техническим устройством.

С учетом анализа практики, нормативного и доктринального материала можно выделить самые распространенные виды интернет-мошенничества: интернет-попрошайничество – в сети Интернет появляются объявления с просьбами об оказании различного рода помощи, пользователи знакомятся с просьбой и перечисляют деньги на счета мошенников (могут быть ситуации, когда распространяются реальные истории, но настоящие пострадавшие не знаю о том, что их жизненная ситуация используется с целью незаконного получения выгоды); мошенничество с помощью Интернет-магазинов (можно отнести и торговлю товарами ненадлежащего качества), виновное лицо под видом менеджера магазина предлагает клиенту оплатить полную стоимость товара, а после оплаты, выполнив обязательства не в полном объеме или не выполнив их вовсе, не выходит на связь; уведомления о выигрыше – пользователь получает сообщение о выигрыше, но с условием, что для его получения необходимо перечислить на счет виновных лиц определенную сумму; фишинг – вид мошенничества, осуществляемый с целью получения реквизитов банковской карты либо электронного кошелька, электронной почты и иной конфиденциальной информации. Обычно реализуется путем рассылки сообщений от имени банков, платежных и других систем с просьбами авторизоваться, помочь системе в устранении неполадок и т.п., введя реквизиты, обеспечивающие доступ к интересующему злоумышленников ресурсу. Существуют и иные виды, но эти являются самыми распространенными.

[1] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: Автореф. Дис. М., 1970. С.10.

В целом действия интернет-мошенников сводятся к четырем этапам: информирование жертвы; процесс взаимодействия с жертвой; получение денежных средств; сокрытие совершенного преступления.

Свойство отражения присуще всей материи, оно присутствует, когда взаимодействует два и более объекта. Если в одном объекте происходят изменения, отражающие факт воздействия на него другого объекта, то можно говорить, что первый объект (следовоспринимающий – приемник информации) является носителем информации о втором (следообразующий – источник информации). Следовательно, любое преступление оставляет следы на соответствующих объектах. А.Л. Осипенко в одной из своих работ акцентирует внимание на то, что сложность обнаружения следов преступлений в сфере компьютерной информации связана, в первую очередь, с тем, что результаты преступных действий распределяются по множеству объектов (компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы и т.п.).[1] С этим связана особенность определения следовоспринимающих объектов.

Основные следы сохраняются на девайсе, который использует преступник для несанкционированного доступа к персональной информации потерпевшего лица, но чаще всего задействуется несколько устройств, которые вовлечены в преступный обмен полученной информации и находятся на больших расстояниях друг от друга.

Не менее значимым является техническое устройство потерпевшего лица, которое является источником информации и следов преступного воздействия. Обмен информацией происходит с помощью установления сетевой связи с устройством потерпевшего, которое используется для обнаружения системы подозреваемого (обвиняемого), можно с его помощью определить способ незаконного завладения. Все эти устройства взаимосвязаны между собой следовой картиной.

Интернет – это всемирная система объединенных компьютерных систем для хранения и передачи информации, не имеющая единого центра управления. Некоторые ученые говорят о наличии виртуальных следов[2], которые сохраняются, в том числе, в сети Интернет. Данный ресурс обычно используется для создания различного рода и вида сайтов (специализированная программа, дистанционно обеспечивающая ведение диалога между продавцом и покупателем). Эта программа содержит несколько управляемых по единой логике электронных страниц с текстовой, графической иногда звуковой информацией, на которых отражаются совершаемые манипуляции, то есть любое действие отражается в системе в виде закодированной информации.

Автоматизированная система расчетов банка комплекс аппаратно-программных средств, реализующих мультивалютную информационную систему, обеспечивающую современные финансовые и управленческие

[1] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009. С. 11.

[2] Мещеряков В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе // Воронежские криминалистические чтения: сб. науч. тр. 2008. № 9. С. 221-232.

технологии в режиме реального времени при транзакционной обработке данных. Любая расчетная операция, в том числе, списание и зачисление денежных средств проходит через такую банковскую систему и отражается на соответствующих носителях. Одобрение большинства банковских операций происходит автоматически, то есть их совершает компьютер, поэтому следы сохраняются на техническом устройстве банка, поэтому оно важно для поиска следов совершения преступления (необходимо получение банковской выписки).

Банкомат, отделение банка важны для расследования, потому что с их помощью можно обнаружить криминалистически значимую информацию. Банкомат - устройство для осуществления в автоматическом режиме наличных денежных расчетов и (или) расчетов с использованием платежных карт, передачи распоряжений кредитной организации об осуществлении расчетов по поручению физических лиц по их банковским счетам, а также для составления документов, подтверждающих передачу соответствующих распоряжений (ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт»). Значит, внутри системы сохраняются следы совершенных операций. Если преступник снимал денежные средства с банковской карты, то в банкомате могут сохраниться информационные данные по списанию, а также видеозапись; если виновное лицо приходило в отделение банка, то можно допросить сотрудников.

В рамках данной работы был рассмотрен механизм следообразования при совершении кибермошенничества через призму криминалистически значимого элемента – способ, определение которого позволяет выявить наиболее типичные следовоспринимающие объекты. Указанные данные ориентируют на поиск, фиксацию и изъятие определенных следов, используемых в процессе доказывания по уголовному делу.

Литература

1. Алесковский С.Ю., Аубакиров А.Ф. Нетрадиционная криминалистика: учеб. пособие. Алматы: АЮ-ВШП «Адилет», 2003. 127 с.
2. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. №4 (34). С. 209-216.
3. Вехов Б.В. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: монография / Б. В. Вехов. - Волгоград, 2005. – С. 276.
4. Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: Автореф. Дис. – М., 1970. – С.10.
5. Криминалистика: учебник / А.И. Александров [и др.]; под ред. С.П. Кушниренко, В.Д. Пристансков, Т.А. Седова. - М., 2019. - 334 с.
6. Мещеряков В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе // Воронежские криминалистические чтения: сб. науч. тр. 2008. № 9. С. 221-232.

7. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009. С. 11.
8. Тарасов, А.А. Безналичные денежные средства как предмет хищений в сфере финансовой деятельности воинских частей / А.А. Тарасов // Право в Вооруженных Силах. - 2005. - № 10. - С.1-9.

И.А. Зыков
Научный руководитель: **Санташов А.Л.**

Хулиганство в информационно-телекоммуникационной сети Интернет

Аннотация. В данной статье даются примеры хулиганских действий в интернете. Приводятся нормы российского законодательства, предусматривающие ответственность за хулиганство. Автором делается вывод о том, что учитывая цифровизацию различных сфер жизни, в том числе и «цифровизацию правонарушений», законодателю, несомненно, важно и необходимо «идти в ногу со временем».

Ключевые слова: хулиганство, мелкое хулиганство, общественное место, ответственность, законодательство, преступление.

Навязывание общения кому-либо в случае, когда человек опасается за свою безопасность, является противозаконным.

Современный человек проводит в Интернете много времени, из них значительную часть времени он тратит на социальные сети, общаясь с коллегами, друзьями, читает новости.

В соответствии с Указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» государство поставило своей целью обеспечить благоприятные условия для применения информационных и коммуникационных технологий, что также предполагает комплексное совершенствование законодательства[1].

За совершение преступлений и административных правонарушений, в том числе в сети Интернет, граждане подлежат привлечению к уголовной и административной ответственности.

Интернет-хулиганство имеет свои разновидности:

1) Троллинг, как культура является феноменом социальным и психологическим на просторах Интернета. Интернет тролли занимаются провокационными действиями на форумах, в чатах или в комментариях блогов, пытаясь настроить против себя пользователей этих социальных сетей. Проще говоря, занимаются хулиганством.

2) Кибермоббинг, представляет собой систематическое, повторяющееся в течение длительного времени третирование, оскорбление, унижение достоинства другого человека, например, в школе, в другом учебном заведении, на рабочем месте и так далее. Типичные действия, осуществляемые при

[1] Собр. законодательства Рос. Федерации. – 2017. – № 20, ст. 2901.

моббинге — это распространение заведомо ложной информации (слухов и сплетней) о человеке, насмешки и провокации, прямые оскорбления и запугивание, социальная изоляция (бойкот и демонстративное игнорирование), нападки, ущемляющие честь и достоинство человека, причинение материального или физического вреда.

В соответствии с ч.3 ст.20.1 КоАП РФ распространение в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, за исключением случаев, предусмотренных ст.20.3.1 КоАП РФ, если эти действия не содержат уголовно наказуемого деяния.

Таким образом, была достигнута цель по охране общественного порядка и уважения к обществу и государству в сети Интернет, в котором необходимо соблюдать правила допустимого поведения, а также формирование понимания того, что сеть Интернет запрещено использовать для совершения правонарушений.

Законодатель относит к распространению информации деяния, которые обладают рядом критериев:

- во-первых, распространяемая информация выражает явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации;

- во-вторых, неприличная форма, за которой скрывается циничное поведение, противоречащее установленным в обществе правилам поведения;

- в-третьих, данная информация оскорбляет человеческое достоинство и общественную нравственность.

Особенностью ч.3 ст.20.1 КоАП РФ является место совершения правонарушения - информационно-телекоммуникационные сети, в том числе сеть «Интернет».

10 января 2021 г. вступил в силу Федеральный закон, изменивший редакцию ст. 213 УК РФ об ответственности за хулиганство. Данный состав преступления был дополнен признаком применения насилия либо угрозы его применения, признак применения при хулиганстве оружия или предметов, используемых в качестве оружия, перенесен в ч.2 данной статьи.

Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области противодействия экстремизму» от 24 июля 2007 г. № 211-ФЗ[1] часть 1 ст. 213 УК РФ дополнена признаком с экстремистским мотивом.

Голик Ю.В. считает, что при понимании общественного места речь должна идти о месте общения людей, указывая, что давно существует «телефонное

[1] Российская газета.2007.1 августа.

хулиганство», к которому добавилось и хулиганство в социальных сетях и в Интернете, «расхожий термин «троллинг» отчасти покрывает этот тезис»[1]. Представляется, что, исходя из такого понимания общественного места, действия лица, совершившего хулиганство в информационно-телекомуникационной сети Интернет в процессе общения, может быть признано таковым, если действует с угрозой применения насилия, с экстремистским мотивом.

УК РФ предусматривает ответственность за преступления, совершаемые в том числе с использованием сети «Интернет»: -доведение до самоубийства (статья 110);-склонение к совершению самоубийства или содействие совершению самоубийства (статья 110.1);-организация деятельности, направленной на побуждение к совершению самоубийства (статья 110.2);-вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (статья 151.2);-незаконные организация и проведение азартных игр (171.2);-незаконные изготовление и оборот порнографических материалов или предметов (статья 242);-изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (статья 242.1);-использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (статья 242.2);-публичные призывы к осуществлению экстремистской деятельности (статья 280);-публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (статья 280.1);-возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (статья 282).

В настоящее время практика применения норм отечественного законодательства по привлечению лиц к ответственности за совершение преступлений и административных правонарушений, в том числе в сети Интернет только формируется. Учитывая цифровизацию различных сфер жизни, в том числе и «цифровизацию правонарушений», законодателю, несомненно, важно и необходимо «идти в ногу со временем».

А.А. Казаков
Научный руководитель: **Османова Н.В.**

Подследственность киберпреступлений

Аннотация. Данная статья посвящена вопросам установления территориальной подследственности преступлений, совершенных с использованием информационных и телекоммуникационных технологий. Рассмотрены основные положения уголовно-процессуального законодательства РФ, регламентирующие определение места совершения преступления.

Ключевые слова: киберпреступление, подследственность, правоохранительные органы, место совершения преступления, уголовное преследование.

[1] Голик Ю. Ответственность за хулиганство: изменение законодательства// Научное сообщение. 2017. № 8. С.162.

Киберпреступность — это продукт глобальной цифровизации передового общества, требующий принятия надлежащего противодействия со стороны страны. В ответ на это противодействие киберпреступники принимают меры к кропотливому сокрытию следов совершения преступления, сохранению анонимности, продумывают свое поведение так, дабы очень максимально осложнить сбор доказательств и избежать ответственности. Эти условия предназначают правовую и фактическую сложность доказывания по этим делам. Зачастую при совершении киберпреступлений используются способы цифровой маскировки: шифрование данных, в что количестве с внедрением предназначенных программ для конспирации Айпишников, выход в Сеть сквозь общественные точки доступа, внедрение учетных записей и идентифицирующих данных, являющихся собственностью других лиц, не ознакомленным об этом применении, и например дальше[1].

Правоохранительные органы не только РФ, но и иных государств, говорят о значительном ряде задач, с коим им приходится сталкиваться в борьбе с компьютерными правонарушителями, и одна из данных задач — заключение вопроса о юрисдикции киберпреступления.

В ч. 2 ст. 9 УК РФ закреплено понятие времени совершения преступления, которым признается время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий. Однако в связи с развитием новых способов совершения преступлений, обусловленных модернизацией информационных и телекоммуникационных технологий, вопрос о месте совершения подобных преступлений до сих не урегулирован в части определения места окончания преступления и территориальной подследственности органов, осуществляющих предварительное расследование подобных преступлений. Точное определение места совершения преступления необходимо для установления пределов действия уголовного закона, а также для верного установления органа, должного осуществлять предварительное расследование и избегания затягивания сроков предварительного следствия путем направления материалов по территориальной подследственности, что имеет большое значение для материального уголовного права. В научном обществе популярен взгляд, согласно которому, под местом совершения преступления следует понимать какую-либо территорию, на которой совершено преступление[2].

Общей особенностью всех преступлений, совершаемых с использованием высоких технологий, является их транснациональность (трансграничность). Она затрудняет установление места совершения подобных преступлений, что в свою очередь способствует затягиваю сроков предварительного расследования, а также усложняет процесс установления лица, совершившего преступление.

[1] СК: для решения проблемы «слива» баз данных в Сеть нужен новый законодательный подход // Информационное агентство ТАСС. URL: https://tass.ru/interviews/10461383 (дата обращения: 30.11.2021).

[2] Расулов Р.В. Некоторые спорные вопросы определения места совершения преступления // Актуальные проблемы российского права. 2011. №4 (21). С. 179.

Преступления в сфере компьютерной информации могут начинаться на территории одного государства, а оканчиваться на территории другого, что придает проблеме определения места совершения преступления международный характер[1].

23.11.2001 в Будапеште принята Конвенция о преступности в сфере компьютерной информации, согласно положениям которой, страна-участник самостоятельна в принятии мер уголовного преследования лиц, которые совершили преступные деяния на ее территории. Правомочия государства распространяется на граждан этого государства, при совершении ими наказуемого деяния в месте совершения преступления, либо если деяние совершено за пределами территориальной юрисдикции какого-либо государства. Если на юрисдикцию в отношении деяния претендуют одно или несколько государств, то они проводят консультации для установления наиболее подходящей юрисдикции для осуществления судебного преследования[2].

Следует отметить, что Российская Федерация участником данной Конвенции не является, в связи с чем ее положения не могут распространяться на территории РФ.

Согласно ч. 1 ст. 152 УПК РФ, предварительное расследование производится по месту совершения деяния, содержащего признаки преступления. Согласно ч. 2 ст. 152 УПК РФ если преступление было начато в одном месте, а окончено в другом месте, то уголовное дело расследуется по месту окончания преступления[3]. Несмотря на то, что положения ст. 152 УПК РФ достаточно конкретно определяют место совершения преступления, в случае совершения киберпреступления, определить это место проблематично. Можно утверждать, что, учитывая развитие информационных и телекоммуникационных технологий, нормы УПК РФ не могут четко ответить на вопрос относительно места окончания, и как следствие, место совершения подобного преступления.

В п. 5 постановления Пленума Верховного Суда РФ № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняется, что преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб[4].

---

[1] Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-р юрид. наук: 12.00.09. М., 2010. С. 114-115.

[2] Степанов-Егиянц Владимир Георгиевич. К вопросу о месте совершения компьютерных преступлений // Научно-информационный журнал «Армия и общество». 2014. №5 (42). С. 18.

[3] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

[4] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2

В постановлении Пленума идет речь о банковских счетах, и им не охватываются случаи перечисления денежных средств на счета мобильных телефонов, на виртуальные (электронные) счета и т.д.

Рассмотрим на примере типичное преступление, совершенное с использованием информационных и телекоммуникационных технологий. Потерпевшему звонят на телефон и в ходе разговора сообщают, что он является победителем лотереи, при этом для получения выигрыша ему необходимо перевести определенную сумму на счет, сообщенный злоумышленником. Потерпевший, не осознавая, что в отношении него совершаются противоправные действия, перечисляет требуемую сумму на сообщенный злоумышленниками счет, возможно даже открытый на территории другого государства.

В момент совершения преступления преступник мог находиться за тысячи километров от потерпевшего, а виртуальный счет был открыт с помощью компьютера, установленного в ином месте. Открытый злоумышленником виртуальный счет привязан к серверу, имеющему иную географическую привязку, нежели место нахождения оборудования, с которого открыт электронный счет.

В дальнейшем преступник, имея доступ к счету, может использовать полученные средства любыми способами, в том числе осуществлять транзакции на другие счета, как электронные, так и банковские.

Рассмотренная выше ситуация не охватывается нормами действующего законодательства, так как счета виртуальных кошельков не имеют географической привязки, в связи с чем определить точное место окончания преступления не представляется возможным[1].

На практике сотрудники правоохранительных органов прибегают к следующим вариантам: принимают процессуальные решения по месту нахождения банка, а именно: где открыт счет и куда поступили похищенные денежные средства, либо считают, что преступление окончено там, где злоумышленник снял денежные средства, после чего направляют материалы по территориальной подследственности, взяв за основание место нахождения банкомата, с помощью которого были обналичены похищенные денежные средства.

На наш взгляд, для решения подобных ситуаций, целесообразно использовать следующий механизм. В случае, если преступник находился в пределах территории РФ в момент совершения им деяния, то уголовное дело при наличии к тому оснований должно возбуждаться по месту обращения потерпевшего. Далее, после проведения первоначальных неотложных следственных действий, в том числе установления места, где было совершено компьютерное преступление, все материалы уголовного дела должны быть направлены по территориальной подследственности в правоохранительный орган по месту

[1] Хасанов Р.Р. О проблемах определения территориальной подследственности по уголовным делам о хищениях, совершенных с использованием информационно-телекоммуникационных технологий // Вестник Казанского юридического института МВД России. 2017. №1 (27). С. 114.

совершения преступления. Например, если потерпевший от компьютерного преступления обратился с заявлением в правоохранительные органы в г. Москве, а позднее будет установлено, что преступник совершил посягательство с компьютера, установленного в Пермском крае, то материалы уголовного дела должны быть переданы в правоохранительный орган Пермского края.

Литература

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2021) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.
2. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2.
3. Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-р юрид. наук: 12.00.09. М., 2010. С. 55.
4. Расулов Р.В. Некоторые спорные вопросы определения места совершения преступления // Актуальные проблемы российского права. 2011. №4 (21). С. 178-183.
5. Степанов-Егиянц Владимир Георгиевич К вопросу о месте совершения компьютерных преступлений // Научно-информационный журнал «Армия и общество». 2014. № 5 (42). С. 16-20.
6. Хасанов Р.Р. О проблемах определения территориальной подследственности по уголовным делам о хищениях, совершенных с использованием информационно-телекоммуникационных технологий // Вестник Казанского юридического института МВД России. 2017. №1 (27). С. 114.
7. СК: для решения проблемы «слива» баз данных в Сеть нужен новый законодательный подход // Информационное агентство ТАСС. URL: https://tass.ru/interviews/10461383 (дата обращения: 30.11.2021).

Л.Е. Королева
Научный руководитель: **Лебедева А.А.**

Способ нарушения неприкосновенности личной жизни с использованием информационных технологий, как элемент криминалистической характеристики

Аннотация. В статье рассматривается способ совершения нарушений неприкосновенности личной жизни, как элемент криминалистической характеристики. Условия бурного развития информационных технологий, обуславливают особые способы совершения указанных нарушений. Кроме того, способ совершения данного преступления непосредственно коррелируется с личностью преступника.

Ключевые слова: способ, неприкосновенность личной жизни, конфиденциальная информация, информационные технологии, распространение информации.

В настоящее время обширные массивы личных данных, сведений составляющих личную тайну, персональную информацию передаются людьми по средствам телекоммуникационного оборудования, мессенджеров, сети «Интернет» во время личной переписки или телефонного общения. Соответственно возникает и возможность перехвата и подключения с целью ознакомления с этими данными и дальнейшим распоряжением. Указанные незаконные действия в последнее время распространены и квалифицируются по статьям 137-138.1 УК РФ[1].

Выбор способа совершения преступления в некоторой степени определяет непосредственный предмет посягательства - конфиденциальную информацию, затрагивающую интересы определенного лица, не связанную с его профессиональной или общественной деятельностью, способную причинить вред данному лицу в случае ее разглашения.

В условиях развития информационных технологий как конфиденциальная информация, так другие сведения, хранятся в электронном виде, что обуславливает совершении преступлений с использованием информационно-коммуникационных средств и сетей.

Среди многообразия способов нарушения неприкосновенности личной жизни, представляется возможным выделить основные группы: 1) сбор, 2) хранение и обработка, 3) распространение сведений о личной жизни лица.[2]

Способы сбора конфиденциальной информации можно объединить в две группы: способы непосредственного доступа к источникам и носителям информации и способы опосредованного (удаленного) доступа.

Особые способы распространения конфиденциальных сведений о личной жизни, выражаются в адресном или безадресном направлении/пересылки информационных сообщений с приватными сведениями о конкретном лице третьим лицам. Адресное распространение сведений о личной жизни совершается при помощи направления сообщения знакомым потерпевшего. Кроме того, сведения о круге общения потерпевшего, содержатся на личной странице пользователя в социальной сети. В случаях безадресного распространения, информация размещается в популярных социальных сетях или на других сайтах, где она может стать доступна неограниченному числу интернет-пользователей.

Так, например, К. обнаружил в нетбуке с выходом в сеть «Интернет», который ранее находился в пользовании потерпевшей, незакрытые ею электронные сервисы. После чего, К. осуществил доступ электронным сервисам потерпевшей, и ознакомился с содержанием переписки с другими лицами. Затем скопировал содержания переписки на отдельный электронный носитель, после чего

[1] Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (действ ред.). URL: www.consultant.ru/document/cons_doc_LAW_10699 (дата обращения: 21.11.2021).

[2] Баринов В.С. Проблемы выявления и расследования преступных нарушений неприкосновенности частной жизни: дис. ... канд. юрид. наук: Саратов, 2006. С 35.

распространил скопированные им ранее данные, путем пересылки в программе обмена сообщениями знакомым потерпевшей.

Способ совершения преступления непосредственно коррелируется с личностью преступника. Так, в способе приготовления к преступлению и его реализации, действия по сокрытию его следов, встречаются признаки и качества, накопленные в течение его предшествовавшей совершению преступного деяния жизни. Вместе с тем, в данных действиях усматриваются профессиональные или иные специальные навыки, которые могут быть обусловлены должностным функционалом или сферой профессиональной деятельности преступника.

Широкое распространение так называемой «подвижной» связи сопровождается ростом количества нарушений тайны связи, совершаемых работниками организаций, предоставляющих соответствующие услуги. Указанные работники имеют в силу занимаемой должности беспрепятственный доступ к конфиденциальной информации, а именно: к персональным данным клиентов, номерам телефонов, сведениям о соединениях абонентов, объеме трафика.[1]

Так работники организаций, предоставляющих услуги сотовой связи, используя служебное положение неправоверно получают доступ к конфиденциальной информации, как правило детализации звонков конкретных клиентов данной организации. В последствии преступники фиксируют полученные сведения при помощи электронного устройства, затем используя данные конфиденциальные сведения в личных целях, либо распространяют третьим лицам, как правило также, используя при этом информационно-коммуникационные средства. Так при распространении конфиденциальной информации преступник может использовать мобильное устройство, персональной компьютер, а также социальные сети и мессенджеры.

Так, например, Б. являясь директором офиса ПАО «ВымпелКом», имея в силу должностных обязанностей доступ к специальной базе персональных данных абонентов, зашла в программу в программу в которой ввела данные мобильного телефона, а также период времени, за который необходимо было предоставить детализацию. После чего, полученные сведения она сфотографировала на телефон и переслала сведения о детализации телефонных и иных соединений абонентов У. и А. по средством мессенджера «Whatsapp».[2]

При незаконном сборе информации служебным положением также пользуются сотрудники правоохранительных служб. Как правило, ими являются сотрудники оперативных подразделений, которые в силу своих должностных полномочий неправомерно получают доступ к конфиденциальным сведениям при производстве оперативно-розыскных мероприятий.

Так, например, оперуполномоченный УУР ГУ МВД России имея доступ к действительным постановлениям судей, преследуя цель незаконного проведения

[1] Баринов С.В. Некоторые особенности выявления и расследования преступных нарушений неприкосновенности частной жизни, совершаемых работниками организаций, предоставляющих услуги подвижной (сотовой) связи. // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. №3. С. 115-122.

[2] Обвинительное заключение по уголовному делу №12002Х в производстве СК РФ за 2020 г.

оперативно-розыскных мероприятий, при помощи редактора фотографических изображений, внес в судебные постановления ложные сведения о лице и абонентском номере. После чего, нарушая установленный порядок, используя свое служебное положение, подготовил 14 заданий на проведение оперативно-розыскных мероприятий. Далее оперуполномоченный незаконно получал сведения о входящих и исходящих соединениях по абонентским номерам, которыми впоследствии распоряжался по своему усмотрению.[1]

При сборе сведений о другом лице, преступник также может применять различные технические средства, предназначенные для подобных целей (в том числе и специальные технические средства, если речь идет о сотрудниках оперативных подразделений, осуществляющих ОРД).

В связи с этим отдельно стоит рассмотреть незаконные производство, приобретение и сбыт специальных технических средств[2], предназначенных для негласного получения информации, за совершение которых предусмотрена уголовная ответственность ст. 138.1 УК РФ. Так например, преступником могут использоваться различные технические средства закамуфлированные под предметы другого функционального назначения,[3] что позволяет преступнику осуществлять бесконтрольное нарушение личной жизни и фиксировать полученную информацию.

Таким образом, способ нарушения неприкосновенности личной жизни является важнейшим элементом криминалистической характеристики рассматриваемого вида преступлений, а также основой частной методики расследования. Способы рассматриваемой группы преступлений различны и зависят от сложившейся обстановки, кроме того связаны с такими элементами криминалистической характеристики как предмет и личность преступника.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (посл. ред. от 27.10.2020). URL: www.consultant.ru/document/cons_doc_LAW_10699.
2. Постановление Правительства РФ от 16 апреля 2012 г. N 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность

[1] Приговор Воронежского областного суда от № 2-99/2017 от 12.12.2017 URL: https://sudact.ru/regular/doc/0hh461UIldL9/?regular-txt=&regular-case_doc=2-99%2F2017&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=1026&regular-court=&regular-judge=&_=1620052163804 (дата обращения: 21.11.2021).

[2] Постановление Правительства РФ от 16 апреля 2012 г. N 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» URL: https://base.garant.ru/70164730/ (дата обращения: 21.11.2021).

[3] Кузнецов А.Н. Доказывание по делам о незаконном оборотеспециальных технических средств. // Полицейское право. 2006. № 4. С. 51-55.

осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». URL: https://base.garant.ru/70164730/ (дата обращения: 21.11.2021).
3. Баринов В.С. Проблемы выявления и расследования преступных нарушений неприкосновенности частной жизни: дис. . канд. юрид. наук: Саратов, 2006. С 35.
4. Баринов С.В. Криминалистическая характеристика преступных нарушений неприкосновенности частной жизни, совершаемых в сети Интернет // Актуальные проблемы российского права. 2016. № 9. С. 137-141.
5. Баринов С.В. Некоторые особенности выявления и расследования преступных нарушений неприкосновенности частной жизни, совершаемых работниками организаций, предоставляющих услуги подвижной (сотовой) связи. // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. №3. С. 115-122.
6. Кузнецов А.Н. Доказывание по делам о незаконном оборотеспециальных технических средств. // Полицейское право. 2006. № 4. С. 51-55.
7. Приговор Октябрьского районного суда г. Архангельска № 1-22/2017 1-378/2016 от 13.02.2017. URL: https://sudact.ru/regular/doc/xSyYIgS0Ag6C/?page=8&regular-court=&regular-date_from=01.01.2017 (дата обращения: 21.11.2021).
8. Приговор Воронежского областного суда от № 2-99/2017 от 12.12.2017 URL: https://sudact.ru/regular/doc/0hh461UIldL9/?regular-txt=&regular-case_doc=2-99%2F2017&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=1026&regular-court=&regular-judge=&_=1620052163804 (дата обращения: 21.11.2021).
9. Обвинительное заключение по уголовному делу №12002XXX в производстве СК РФ за 2020 г.

П.Д. Левашова
Научный руководитель: **Кокорева Л.В.**

Некоторые проблемы участия специалиста при расследовании киберпреступлений

Аннотация. Статья посвящена актуальной проблеме расследования киберпреступлений. Рассматриваются некоторые особенности выбора и привлечения специалиста в сфере высоких технологий к производству следственных действий. Даются рекомендации по планированию расследования по уголовным делам, требующим использования специальных познаний. Раскрываются существующие проблемы регламентации правового статуса специалиста.

Ключевые слова: специалист, киберпреступность, информационные технологии, взаимодействие, следственное действие, специальные познания.

Среди серьезных изменений, произошедших на рубеже второго и третьего тысячелетия, можно заметить, что возросла степень открытости национальных

экономических систем, увеличился обмен капиталами и кадрами, товарами и услугами, выросла роль научных знаний[1]. Информационно-телекоммуникационные технологии прочно вошли в наш быт, и являются неотъемлемым атрибутом жизни каждого современного человека. Массовое использование глобальной сети Интернет способствует увеличению операций по обмену данными. В большом информационном потоке пользователь нередко утрачивает бдительность и избирательность внимания, что увеличивает его шансы стать жертвой IT преступления.

По официальным данным МВД России, в 2021 г. небольшой рост общего количества зарегистрированных преступлений (на 1,6 %) обусловлен тем, что существенная часть криминальных деяний совершается с применением IT-технологий. В период январь-май 2021 г. преступлений в сфере высоких технологий зарегистрировано на 25,7 % больше, чем год назад, в том числе совершенных при помощи сети Интернет – на 48,4 %, с использованием компьютерной техники – на 40,1 %. Если в январе-мае 2020 г. удельный вес преступности рассматриваемого вида составлял 21,7 %, то по итогам пяти месяцев текущего года он увеличился до 26,8 %[2].

Указанная статистика объясняется тем, что в связи с пандемией в отдельных регионах России периодически вводятся ограничительные меры по сокращению пребывания лиц в местах общего пользования. Лишившись возможности получать доход традиционным нелегальным способом посредством уличных краж, грабежей и разбоев, преступники стали искать новые пути обогащения, в том числе связанные с использованием информационных технологий в удаленном доступе[3].

В настоящее время к киберпреступлениям принято относить все общественно опасные деяния, совершаемые полностью или частично в виртуальном пространстве посредством использования информационно-коммуникационных технологий[4]. Очевидно, что для раскрытия и расследования преступлений указанного вида необходимо использование специальных знаний в области компьютерной техники и высоких технологий. Отсутствие у большинства лиц, ведущих производство по уголовному делу, дополнительного информационного образования[5] свидетельствует о необходимости привлечения к расследованию

---

[1]Левашова П.Д. Антиглобализм как политическое движение в современном обществе // Право, общество, государство: проблемы теории и истории: Сборник научных трудов межвузовской конференции / под. ред. К.Е. Размахова. 2019. С. 67.

[2] МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 г. URL: https://мвд.рф/news/item/24738876 (дата обращения: 17.11.2021).

[3] Валуев М.В., Левашова П.Д. Некоторые виды мошенничества в период пандемии // Современное состояние правоохранительной деятельности: проблемы организации, функционирования и перспективы развития: Сборник статей по итогам работы межведомственного, межрегионального круглого стола. 2021. С. 32.

[4]Русскевич Е.А. Преступления, совершаемые с использованием информационно-коммуникационных технологий: результат интерпретации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1(4). С. 101–106.

[5] Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед

иных участников уголовного судопроизводства. В связи с этим следователь (дознаватель) имеет право воспользоваться услугами специалиста и взаимодействовать с ним как в процессуальной, так и в непроцессуальной форме[1].

Приглашая специалиста принять участие в следственном действии, следователь (дознаватель) в соответствии со ст. 168 УПК РФ должен удостовериться в его компетентности и отсутствии заинтересованности в исходе уголовного дела. Тем не менее, законодателем не указаны критерии оценки соответствия профессиональных знаний необходимых на данном этапе расследования. На наш взгляд, документа об образовании в данном случае недостаточно. Целесообразно убедиться в опыте работы лица с интересующими следствие предметами преступления (в нашем случае с ЭВМ, смартфон и другими техническими средствами) посредством сбора характеризующего материала по месту работы. В случае необходимости производства следственного действия в организации, с которой связаны события преступления, не рекомендуется привлечение кого-либо из сотрудников предприятия. Несмотря на компетентность в рассматриваемом вопросе, «местный» специалист может иметь отношение к случившемуся, а потому подлежит отводу. По делам о киберпреступлениях целесообразно привлекать в качестве специалистов сотрудников отдела «К», ЭКЦ МВД России, работающих по данному профилю, в том числе и экспертов, которые, консультируя следователя (дознавателя), выступают в качестве специалистов.

В процессе профессиональной деятельности необходимо собирать контактные данные специалистов для того, чтобы взаимодействовать с ними в непроцессуальной форме в виде консультаций при расследовании уголовных дел повышенной сложности, в том числе и киберпреступлений.

При подготовке плана предстоящего следственного действия, следователь (дознаватель) должен определить в какой области необходимы специальные познания на данном этапе расследования[2]. Из-за объективной невозможности участия необходимого специалиста в производстве по уголовному делу правоохранительные органы теряют ценные данные, которые могли лечь в основу доказательственной базы. Привлечение специалиста в другой области

сотрудниками следственных органов // Вестник науки и образования. 2018. №8 (44). URL: https://cyberleninka.ru/article/n/problemy-rassledovaniya-kiberprestupleniy-kotorye-stoyat-pered-sotrudnikami-sledstvennyh-organov (дата обращения: 16.11.2021).

[1] Кокорева Л.В., Кокорев Р.А. О взаимодействии подразделений органов внутренних дел при раскрытии и расследовании преступлений // Органы предварительного следствия в системе МВД России: история, современность, перспективы (к 50-летию со дня образования следственного аппарата в системе МВД России): Сб. матер. всерос. науч.-практ. конф.: В 2-х ч. М.: Академия управления МВД России, 2013. Ч. 1. С. 176.

[2] Кокорева Л.В., Кокорев Р.А. Этапы взаимодействия следователя и специалиста при проведении следственных действий // Доклады международной научно-практической конференции «Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России» (г. Лиссабон (Португалия) – 5-12 мая 2012 г.) / под редакцией заслуженного деятеля науки Российской Федерации, д.ю.н., профессора А. М. Кустова и д.э.н., доцента Т. Ю. Прокофьевой. М.: Издательство «МЭЙЛЕР», 2012. С. 81.

специальных познаний может оказаться не только безрезультатным, но и повлечь нарушение процессуальных норм.

В свою очередь, следователю (дознавателю) необходимы знания именно основ компьютерных технологий при расследовании киберпреступлений, которые смогут помочь ему определить вопросы для производства судебной экспертизы. Так назначая компьютерно-техническую экспертизу, следователь сформулировал вопросы, не относящиеся к предмету исследования назначенной им экспертизы, выходящие за пределы специальных познаний эксперта, в итоге, экспертное заключение было признано судом недопустимым доказательством[1].

Разъясняя специалисту порядок производства следственного действия, следователь (дознаватель) должен обратить внимание участника уголовного судопроизводства на его права и обязанности. Если специалист не является сотрудником ведомственного подразделения и не имеет опыт участия в производстве следственного действия, руководитель следственно-оперативной группы должен провести профилактическую работу по пресечению возможных процессуальных нарушений.

Обращаясь к правовому статусу специалиста, обратим внимание на мнение Л. Г. Татьяниной и Е. И. Кузнецова, указывающих на необходимость дополнить ст. 58 УПК РФ правом давать показания[2]. На наш взгляд, дача показаний по вопросам, входящим в компетенцию специалиста является его обязанностью, что следует из ч. 1 (разъяснение сторонам и суду вопросов, входящих в компетенцию – форма дачи показаний) и 4 (обязанность являться по вызовам дознавателя, следователя или в суд) ст. 58 УПК РФ. В соответствии с п. 17 ППВС РФ от 19 декабря 2017 г. № 51[3], в судебном заседании допрос специалиста проводится по правилам допроса свидетеля. Иными словами, отказ от дачи показаний специалиста равносилен отказу от дачи свидетеля и влечет ответственность в соответствии со ст. 308 УК РФ. Однако в отличие от свидетеля, специалист может как выйти за рамки поставленных ему вопросов, давая разъяснение, так и сослаться на необходимость проведения специального исследования для формирования окончательного вывода.

Несмотря на то, что для производства отдельных следственных действий технических знаний следователя (дознавателя) может быть достаточно, например, при осмотре смартфона, законодатель в ст. 164.1 УПК РФ обозначил необходимость участия специалиста при изъятии электронных носителей информации или копировании с них информации. Велика вероятность того, что

---

[1]Апелляционное определение Судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 20.04.2017 по делу № 22-2649/2017. URL: https://base.garant.ru/147142847/ (дата обращения 17.11.2021).

[2] Татьянина Л.Г., Кузнецов Е.И. Допрос специалиста в уголовном судопроизводстве // Вестник ЮУрГУ. Серия: Право. 2006. № 13. URL: https://cyberleninka.ru/article/n/dopros-spetsialista-v-ugolovnom-sudoproizvodstve (дата обращения: 17.11.2021).

[3] Постановление Пленума Верховного Суда Российской Федерации от 19 декабря 2017 г. № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)». URL: https://rg.ru/2017/12/29/postanovlenie-dok.html (дата обращения: 17.11.2021).

злоумышленник, ожидая визит правоохранительных органов, мог применить средства шифрования информации на своем компьютере, в связи с чем, при осмотре техники необходимы знания в области криптографии и снятия парольной защиты. Тактически целесообразно проведение обыска по месту жительства подозреваемого при сохранении фактора внезапности, однако и в случае отсутствия такого преимущества эффективности и законности предстоящего следственного действия будет способствовать участие специалиста по делам о киберпреступлениях.

В заключение отметим, что раскрытие и расследование киберпреступлений в настоящее время невозможно без участия в производстве по уголовному делу специалиста. Тем не менее, в регламентации правового статуса указанного участника уголовного судопроизводства имеются особенности, которые необходимо закрепить единой правоприменительной практикой.

Литература

1. Постановление Пленума Верховного Суда Российской Федерации от 19 декабря 2017 г. № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)». URL: https://rg.ru/2017/12/29/postanovlenie-dok.html.
2. Валуев М.В., Левашова П.Д. Некоторые виды мошенничества в период пандемии // Современное состояние правоохранительной деятельности: проблемы организации, функционирования и перспективы развития: Сборник статей по итогам работы межведомственного, межрегионального круглого стола. 2021. С. 32.
3. Кокорева Л.В., Кокорев Р.А. О взаимодействии подразделений органов внутренних дел при раскрытии и расследовании преступлений // Органы предварительного следствия в системе МВД России: история, современность, перспективы (к 50-летию со дня образования следственного аппарата в системе МВД России): Сб. матер. всерос. науч.-практ. конф.: В 2-х ч. М.: Академия управления МВД России, 2013. Ч. 1. С. 175–179.
4. Кокорева Л.В., Кокорев Р.А. Этапы взаимодействия следователя и специалиста при проведении следственных действий // Доклады международной научно-практической конференции «Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России» (г. Лиссабон (Португалия) – 5-12 мая 2012 г.) / под редакцией заслуженного деятеля науки Российской Федерации, д.ю.н., профессора А. М. Кустова и д.э.н., доцента Т. Ю. Прокофьевой. М.: Издательство «МЭЙЛЕР», 2012. С. 80–83.
5. Левашова П.Д. Антиглобализм как политическое движение в современном обществе // Право, общество, государство: проблемы теории и истории: Сборник научных трудов межвузовской конференции / под. ред. К.Е. Размахова. 2019. С. 67.
6. Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и

образования. 2018. №8 (44). URL: https://cyberleninka.ru/article/n/problemy-rassledovaniya-kiberprestupleniy-kotorye-stoyat-pered-sotrudnikami-sledstvennyh-organov.
7. Русскевич Е.А. Преступления, совершаемые с использованием информационно-коммуникационных технологий: результат интерпретации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1(4). С. 101–106.
8. Татьянина Л.Г., Кузнецов Е.И. Допрос специалиста в уголовном судопроизводстве // Вестник ЮУрГУ. Серия: Право. 2006. № 13. URL: https://cyberleninka.ru/article/n/dopros-spetsialista-v-ugolovnom-sudoproizvodstve.
9. Апелляционное определение Судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 20.04.2017 по делу № 22-2649/2017. URL: https://base.garant.ru/147142847.
10. МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 г. URL: https://мвд.рф/news/item/24738876.

В.И. Малик

О некоторых мерах противодействия наркопреступлениям, совершаемых несовершеннолетними с использованием сети Интернет

Аннотация. В статье актуализирована проблема распространения наркотических средств через сеть Интернет. В цифровую эпоху несовершеннолетние являются наиболее активными пользователями «Всемирной паутины». Автор акцентирует внимание на профилактике наркопреступлений в подростковой среде, как одного из важнейших направлений правоохранительных органов. Обоснованы оптимальные меры предупреждения преступлений, связанных с незаконным оборотом наркотических средств в сети Интернет.

Ключевые слова: противодействие наркопреступлениям, несовершеннолетние, незаконный оборот наркотических средств, информационные технологии, сеть Интернет.

На сегодняшний день, Интернет – это не только самая востребованная площадка для распространения наркотиков, но и для вербовки несовершеннолетних граждан. В связи с этим усложняется процесс проведения оперативно-розыскных мероприятий и следственных действий, направленных на выявление фактов незаконного оборота наркотиков.

Увлечение компьютерными технологиями свойственно подросткам, то есть лицам от 14 до 19 лет. Именно эта категория населения является самыми уязвимыми и внушаемыми, что и выгодно фигурантам. В контексте сказанного следует согласиться с суждением О.В. Овчинниковой, которая говорит о том, что

«сеть Интернет выступает коммуникативным полем, поскольку большинство сайтов предусматривает блог для общения пользователей»[1].

Члены организованных групп и организованных преступных сообществ все чаще дают о себе знать, направляя в социальные сети вакансии о работе, где посредством совершения простых действий человек сможет заработать большие деньги. Как правило, ответы на подобные сообщения приходят от молодых людей, подростков, которые подвержены вербовке.

В результате, подростки не понимая - какую ответственность им придется нести, вступают на преступный путь. Для вербовки несовершеннолетнего «операторы» просят сделать что-то совсем незначительное, но прилично платят. «Сделав несколько закладок, он думает, что так будет всегда, ничего не произойдет. И потом, когда ему дают действительно опасное задание, он этого уже не осознает»[2]. Министерство внутренних дел РФ обеспокоено сложившейся ситуацией, именно поэтому родителей просят насторожиться, если ребенок покупает дорогие вещи, имеет несколько электронных или банковских карт на разных владельцев. На официальном сайте МВД России содержится полезная информация для родителей, чтобы уберечь своих детей от негативного влияния со стороны наркодилеров[3]. Там же находятся рекомендации и советы поведения для родителей в том случае, если они обнаружили, что их ребенок имеет отношение к наркотическим веществам.

Следует подчеркнуть, что среди задач и функций, которые осуществляют сотрудники органов внутренних дел, присутствуют такие как осуществление профилактики употребления и сбыта наркотических средств несовершеннолетними.

Отметим, что профилактика в вопросах борьбы с незаконным оборотом наркотиков – на одном из первых мест в ведомстве, потому, как известно, преступление легче предупредить, чем остановить. Одной из форм профилактики в сфере оборота наркотических средств являются беседы, лекции, проведение родительских собраний в школах и других учебных заведениях совместно с обучающимися.

Приказ МВД России от 27.12.2018 № 886 устанавливает основные направления взаимодействия подразделений по контролю за оборотом наркотических средств с другими подразделениями органов внутренних дел при осуществлении деятельности по предупреждению, выявлению, пресечению

---

[1] Овчинникова О.В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет // Правопорядок: история, теория, практика. 2018. № 1. С. 95.

[2] Самоделова С. На темной стороне Сети: вербовка школьников в наркокурьеры стала эпидемией // Московский комсомолец.RU от 21.02.2019. [Электронный ресурс]. URL: https://www.mk.ru/social/2019/02/21/na-temnoy-storone-seti-verbovka-shkolnikov-v-narkokurery-stala-epidemiey.html (дата обращения 17.11.2021).

[3] Официальный сайт МВД РФ. Это должен знать каждый. Несколько правил, позволяющих предотвратить потребление психоактивных веществ вашим ребенком. [Электронный ресурс] https://мвд.рф/mvd/structure1/ Glavnie_upravlenija/gunk/родителям-и-детям/это-должен-знать-каждый

и раскрытию правонарушений, связанных с незаконным оборотом наркотических средств[1].

Так, сотрудники подразделений по контролю за оборотом наркотиков в делах с участием несовершеннолетних в большей мере взаимодействую с подразделениями по делам несовершеннолетних, которые оказывают в пределах своей компетенции содействие в выявлении мест возможного сбыта, приобретения и потребления наркотических средств и психотропных веществ либо новых потенциально опасных психоактивных веществ.

Среди первоочередных мероприятий в указанном направлении стоит регулярное проведении плановых и внеплановых мероприятий для проверки мест массового отдыха молодежи. Операции и рейды сотрудников в вечерние клубы, бары, рынки, подвалы, чердаки и иные заведения и места, где с высокой вероятностью могут распространяться наркотические и психотропные вещества, являются весьма продуктивными направлениями деятельности правоохранительных органов по предупреждению, выявлению и пресечению наркопреступлений среди несовершеннолетних.

К мерам противодействия рассматриваемого негативного явления следует отнести проведение комплексного анализа состояния работы подразделений по делам несовершеннолетних по линии незаконного оборота наркотических средств и психотропных веществ среди несовершеннолетних.

На основе полученных результатов, контролирующими подразделениями вносятся предложения руководителю территориального органа МВД России о необходимости проведения профилактических мероприятий, а также необходимые предписания в органы и учреждения системы профилактики безнадзорности и правонарушений несовершеннолетних граждан.

К другим, не менее эффективным, формам профилактики относится контроль, осуществляемый сотрудниками полиции, по месту жительства несовершеннолетних, родителей, либо законных представителей, которые отрицательно влияют на воспитание детей, ненадлежащим образом исполняют свои родительские обязанности по воспитанию несовершеннолетних, тем самым склоняя их к девиациям, употреблению наркотиков и т.д. Для этого составляется график внезапных проверок по месту жительства сотрудниками ПДН, ОУУП, ОУР совместно с представителями системы профилактики.

Как было уже сказано, интернет-пространство имеет широкие коммуникационные возможности для расширения сферы бесконтактных способов распространения наркотических средств. Технические возможности информационных ресурсов по соблюдению анонимности их пользователей делают раскрытие такого рода преступлений чрезвычайно трудоемким и весьма сложным. В данной связи, для того, чтобы повысить раскрываемость преступлений в сфере оборота наркотиков с использованием сети Интернет и

[1] Приказ МВД России от 27.12.2018 №886 (ред. от 01.03.2021) «Об утверждении положения о взаимодействии при осуществлении деятельности по предупреждению, выявлению, пресечению и раскрытию правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, сильнодействующих или ядовитых веществ» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru.

соответствовать новым методам и преступным формам, правоохранительные органы нацелены на принятие всевозможных мер, изобличающих виновных лиц, а именно:

1) прохождение специализированного обучения сотрудниками ОВД[1];

2) мониторинг подозрительных сайтов в сети Интернет;

3) международное сотрудничество по оказанию правовой помощи в сфере государственного контроля за оборотом наркотических средств и психотропных веществ[2], в том числе в делах с участием несовершеннолетних и т.д.

Усложнение преступных методов и способов совершения преступлений требует модификацию тактики раскрытия и расследования преступлений в сфере оборота наркотических средств. Сегодня МВД оценивает интернет-контент о способах изготовления, использования и культивирования наркотических средств, психотропных веществ и их прекурсоров и принимает решение о включении ресурсов в список запрещенных сайтов. В России устанавливается ответственность операторов связи за обеспечение устойчивого, безопасного и целостного функционирования интернета. С принятием внесенных в Госдуму поправок в КоАП России операторы могут быть оштрафованы за неисполнение Федерального закона № 90-ФЗ. По данным Роскомнадзора, только в 2020 году противоправный контент был удален на 18 тысячах сайтов с пропагандой наркотиков[3].

Проведенный анализ показал, что для предупреждения и пресечения преступлений, связанных с незаконным оборотом наркотических средств в сети Интернет, в том числе с участием несовершеннолетних граждан, необходимо предпринять следующие меры:

1. Процесс регистрации пользователей должен быть максимально достоверным в целях исключения анонимных персон. Для этого следует усовершенствовать систему идентификации, а в частности, запрашивать паспортные данные при регистрации.

2. Блокирование интернет-ресурсов, тематикой которых является пропаганда потребления наркотических средств, их полезные свойства и вся информация, относящаяся к приготовлению и ингредиентам.

3. Ограничение доступа к сайтам, имеющим информацию о наркотических средствах категории граждан, не достигших 18 лет.

4. Отслеживание запросов интернет пользователей, относящихся к наркотическим средствам и психотропным веществам.

---

[1] Мельцов В.М. Противодействие сотрудниками ОВД «бесконтактным» методам сбыта наркотиков / В.М. Мельцов, М.А. Бекмешова // Научное и образовательное пространство: перспективы развития: материалы VI Международной научно-практической конференции / под ред. О.Н. Широкова. – Чебоксары: ЦНС «Интерактив плюс», 2017. С. 365-367.

[2] Васюков В.Ф., Панферов Р.Г. Расследование контрабанды наркотических средств, перемещаемых в международных почтовых отправлениях. Учебное пособие. М.: Изд-во Прометей, 2021. С.114-116.

[3] Доклад Государственного антинаркотического комитета о наркоситуации в Российской Федерации в 2020 году [Электронный ресурс] https://drugmap.ru/wp-content/uploads /2020/08/ Doklad-GAK-2019-KMM.pdf. (дата обращения 19.11.2021).

Таким образом, указанные меры должны сократить количество сайтов с информацией о распространении наркотических средств. Тем самым снизится число несовершеннолетних пользователей, вовлеченных в сферу виртуальной наркопреступности.

Подводя итог, следует заключить, что, основой системы профилактики наркопреступлений, особенно среди молодежи, должно выступать формирование психологического иммунитета и нетерпимости к потреблению наркотиков еще с ранних лет жизни, стимулирование здорового образа жизни.

Целью индивидуальной профилактики преступлений, совершаемых несовершеннолетними, являются исправление и перевоспитание несовершеннолетнего, либо изменение его криминогенной ориентации.

Литература

1. Васюков В.Ф., Панферов Р.Г. Расследование контрабанды наркотических средств, перемещаемых в международных почтовых отправлениях. Учебное пособие. М.: Изд-во Прометей, 2021. – 332 с.
2. Доклад Государственного антинаркотического комитета о наркоситуации в Российской Федерации в 2020 году [Электронный ресурс] https://drugmap.ru/wp-content/uploads /2020/08/ Doklad-GAK-2019-KMM.pdf.
3. Мельцов В.М. Противодействие сотрудниками ОВД «бесконтактным» методам сбыта наркотиков / В.М. Мельцов, М.А. Бекмешова // Научное и образовательное пространство: перспективы развития: материалы VI Международной научно-практической конференции / под ред. О.Н. Широкова. – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 365–367.
4. Овчинникова О.В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет // Правопорядок: история, теория, практика. 2018. № 1. С. 94–98.
5. Приказ МВД России от 27.12.2018 № 886 (ред. от 01.03.2021) «Об утверждении положения о взаимодействии при осуществлении деятельности по предупреждению, выявлению, пресечению и раскрытию правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, сильнодействующих или ядовитых веществ» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru
6. Самоделова С. На темной стороне Сети: вербовка школьников в наркокурьеры стала эпидемией // Московский комсомолец.RU от 21.02.2019. [Электронный ресурс]. URL: https://www.mk.ru/social/2019/02/21/na-temnoy-storone-seti-verbovka-shkolnikov-v-narkokurery-stala-epidemiey.html

А.А. Магомедов
Научный руководитель: **Бертовский Л.В.**

К вопросу расследования уголовных дел о преступлениях, совершенных должностными лицами, обладающими особым правовым статусом с использованием криптовалюты

Аннотация. В статье проводится анализ действующего законодательства в части предварительного расследования уголовных дел, возбужденных в отношении должностных лиц, обладающих особым правовым статусом о преступлениях с использованием криптовалюты. Рассматриваются некоторые уголовно-процессуальные проблемы, связанные с расследованием уголовных дел указанной выше категории, в которых криптовалюта является предметом преступления. Предлагаются варианты решения проблем, связанных с расследованием исследуемой категории уголовных дел.

Ключевые слова: криптовалюта; должностные лица, обладающие особым правовым статусом; предварительное расследование; доказательства; конфискация имущества.

Уголовно-процессуальная деятельность сложилась таким образом, что доказывание вины должностных лиц, обладающих особым правовым статусом, в процессе расследования связано с получением правоохранительными органами информации о движении денежных средств по счетам (вкладам) в кредитных организациях. Однако при расчете с должностными лицами при совершении преступлений, помимо денежных средств, могут применяться альтернативные платежные системы. Указанная платежная система представляет новую форму электронных денег, это биткоин и другие криптовалюты. Такие системы функционируют только в виртуальном пространстве, основываются на принципе децентрализации, не имеют единого органа управления и функционируют автономно, вне зависимости от национальных денежно-валютных систем. Таким образом, создание электронных денег сопровождается выходом денежной массы из под контроля государств. В связи с этим отношение к денежным инструментам подобного рода должно строиться, исходя из потенциальной опасности их для денежного суверенитета государств.

Кроме этого, по коррупционным преступлениям доказать связь взяткодателя и взяткополучателя, расчеты между которыми произведены в криптовалюте, зачастую не представляется возможным без проведения соответствующих оперативно-розыскных мероприятий.

На территории Российской Федерации складывающиеся общественные отношения, связанные с оборотом криптовалюты остаются не до конца урегулированными. Даже с учетом тех изменений, которые были внесены в действующее законодательство.

Верховным судом Российской Федерации 26 февраля 2019 года были внесены изменения в постановление Пленума Верховного суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных

преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». Данные изменения приравняли криптовалюту к денежным средствам по уголовным делам.

Анализ действующего уголовно-процессуального законодательства выявил некоторые проблемы, связанные с расследованием уголовных дел в отношении должностных лиц, обладающих особым правовым статусом, в которых криптовалюта является предметом преступления.

Уголовно-процессуальные проблемы состоят в следующем:

1. Возникает сложность в определении стоимости криптовалюты, выступающей предметом преступного посягательства.

2. Проблема в конфискации криптовалюты или наложения ареста в соответствии с требованиями Уголовно-процессуального кодекса

Российской Федерации.

3. Отражение в обвинительном заключении размера и характера вреда, причиненного потерпевшему преступлением.

Указанные проблемы носят системный характер. Можно предположить, что законодательные изменения могли бы решить указанные проблемы, однако этого не произошло в связи со следующим обстоятельствами.

Понятие криптовалюты до недавнего времени не имела правового статуса, в связи с чем правоприменитель понимал сделки с криптовалютой как сделки с сомнительным финансовым инструментом, однако вступивший в силу Федеральный закон от 31 июля 2020 года № 259 ФЗ «О цифровых финансовых активах, цифровой валюте и внесении изменений в отдельные законодательные акты Российской Федерации» (далее - Федеральный закон № 259 – ФЗ) она приобрела правовой статус.

С 1 января 2021 года вступил в силу Федеральный закон № 259 – ФЗ. На основании пункта 3 статьи 1 данного закона криптовалюта относится к цифровой валюте – совокупности электронных цифровых данных, содержащихся в информационной системе и предлагаются либо могут быть приняты в качестве средств платежа. В то же время цифровая валюта не является денежной единицей ни России, ни иностранного государства. Не смотря на это криптовалюта может быть использована в качестве расчетной денежной единицы. Следовательно, криптовалютная транзакция может являться доказательством получения выгоды должностным лицом, обладающими особым правовым статусом. Фиксация указанного доказательства осуществляется путем скриншота монитора.

При этом стоимость криптовалюты в рублевом эквиваленте должна быть отражена в обвинительном заключении. Ее стоимость можно определить следующим образом. Надо зайти на сайт соответствующей биржы, на которой данная валюта приобреталась, с помощью графических инструментов сайта, указать время и дату перевода криптовалюты должностному лицу, обладающему особым правовым статусом, и сделать скриншот для приобщения к уголовному делу.

Еще один спорный вопрос заключается в том, как фактически конфисковать или наложить арест на криптовалюту.

Существует два варианта.

Первый - это перевод денежных средств из криптокошелька обвиняемого, обладающего особым правовым статусом, в специально открытый криптокошелек для хранения денежных средств под контролем следователя.

Следует иметь в виду, что криптомонеты признаются вещественным доказательством, и в данном случае криптокошелек может открывать только следователь.

Второй способ предполагает оставление криптомонет в криптокошельке обвиняемого, с заменой кода доступа, необходимого для авторизации кошелька.

Данные варианты возможны только при наличии пароля доступа у следователя. Технические возможности взлома криптокошелька, по мнению IT-специалистов являются невозможными.

Таким образом можно сделать выводы, что Федеральный закон № 259 – ФЗ урегулировал правовой статус цифровой валюты. Криптовалютная транзакция может являться доказательством получения выгоды должностным лицом, обладающими особым правовым статусом. Стоимость криптовалюты в рублевом эквиваленте должна быть отражена в обвинительном заключении.

Стоимость можно определить следующим образом. Необходимо зайти на сайт соответствующей биржы, на которой данная валюта приобреталась, с помощью графических инструментов сайта, указать время и дату перевода криптовалюты должностному лицу, обладающему особым правовым статусом, и сделать скриншот который необходимо приобщить к уголовному делу.

Литература

1. Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».
2. Информационное письмо Банка России от 14 августа 2018 г. N ИН-014-12/54 «О национальной оценке рисков ОД/ФТ».
3. Багмет А.М. К вопросу о совершенствовании курсов повышения квалификации по криминалистической тактике в Академии Следственного комитета Российской Федерации / А.М. Багмет // Вестник Академии Следственного комитета Российской Федерации. 2015. N 3. С. 23 - 26.
4. Дубянский А.Н. Теории происхождения денег и криптовалюты // Деньги и кредит. 2017. № 12. С. 99.
5. Долгиева М. Легализация криптовалюты: судебная практика // Законность. 2021. N 3.С. 50-54.
6. Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru.

П.О. Мироненкова
Научный руководитель: **Глушков М.Р.**

Социальная инженерия как объект криминалистического изучения

Аннотация. В статье дается определение социальной инженерии, а также рассматриваются различные ее техники. Автором анализируются возможные причины широкого распространения преступлений, совершенных с применением методов социальной инженерии, а также рассматриваются основные способы противодействия и защиты от преступлений данного вида.

Ключевые слова: социальная инженерия, методики мошенничества, техники социальной инженерии, фишинг, претекстинг, «троянский конь».

На сегодняшний день мы являемся свидетелями грандиозного явления, называемого техническим прогрессом. Компьютеризация практически всех сфер общественной жизни открывает новые возможности в развитии экономики, медицины, образования. Вместе с тем, создание новых информационных технологий, расширение возможностей интернет-контента порождает и комплекс отрицательных последствий, связанных с ростом уровня преступности, появлением ее новых форм и методов.

На сегодняшний день одной из основных тенденций развития преступности в сфере информационно-телекоммуникационных технологий является использование методов социальной инженерии при совершении противоправных деяний. По словам заместителя председателя правления Сбербанка России С.В. Кузнецова, более 80% случаев мошенничеств в Российской Федерации совершается при помощи методов социальной инженерии. А согласно данным статистики Центрального банка РФ, количество атак с использованием социальной инженерии в 2020 году выросло на 147% по сравнению с 2019 годом[1].

Что же представляет из себя эта «социальная инженерия», в чем заключается ее сущность?

Социальная инженерия представляет собой систему «различных психологических методик и мошеннических приемов, целью которых является получение конфиденциальной информации о человеке обманным путем»[2]. Иными словами, это своеобразный метод несанкционированного доступа к информации или системам хранения информации с помощью техник, основанных на использовании слабостей человеческой натуры. На сегодняшний день социальная инженерия стала чрезвычайно эффективным оружием в руках мошенников. Это обусловлено тем, что человек более уязвим, чем система. Поэтому главной целью использования социальной инженерии в преступных

[1] Количество атак с использованием социальной инженерии выросло на 147% в 2020 году - SecurityLab.ru by Positive Technologies [Электронный ресурс] URL: https://www.securitylab.ru/news/515178.php. (дата обращения 27.11.2021).

[2] Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. – М.: Международные отношения, 2020. – 288 с.

действиях является побуждение человека к раскрытию конфиденциальной информации для совершения действий, направленных в обход систем безопасности: как говорится, «самая эффективная тактика сетевых атак — это атака на нейросеть, уютно расположившуюся между монитором и спинкой офисного кресла». На рынке программных средств доступно огромное количество продуктов для обеспечения информационной безопасности, но именно человек, как носитель информации является самым уязвимым звеном и владеет «ключами от всех дверей»: комбинацией учетных данных (логин и пароль), номером кредитной карты, данными для доступа к онлайн-банку и т.д.[1]

Техники социальной инженерии представляют собой совокупность приемов и методов, которые являются вспомогательными средствами неправомерного доступа к конфиденциальной информации пользователей для достижения корыстных целей. Рассмотрим некоторые из наиболее распространенных техник социальной инженерии:

1. Фишинг (термин образован от игры слов «password harvesting fishing» - ловля паролей) – является наиболее распространенной и одной из самых эффективных техник социальной инженерии. Фишинг представляет собой массовую рассылку писем по электронной почте. Зачастую письма отправляются с почтовых адресов, похожих на адреса известных компаний, банков, сервисов (например, ВКонтакте, mail.ru и др.), и содержат в себе ссылку на фальшивую web-страницу. Такая страница содержит логотип организации и специальную форму с вводом персональных данных (например, данные банковской карты). Таким же образом происходит мошенничество при покупке товаров через сеть «Интернет». На электронную почту жертвы приходит письмо якобы от Интернет-магазина (например, AliExpress.com) с информацией о действующих на текущий период акциях и купонах с ссылкой на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержимым. Жертва оформляет и оплачивает заказ, но не получает его, т.к. деньги перечислены на счет злоумышленника, а не продавца. Разновидностью фишинга является смишинг–атака с использованием текстовых сообщений посредством SMS-рассылок.

2. Претекстинг – это набор действий злоумышленника, который проводится по определенному, заранее подготовленному сценарию (претексту), в результате которого жертва должна выдать какую-либо информацию или совершить определенное действие. Эта техника требует от мошенника некоторой подготовки и выяснения информации о жертве (выяснение имени человека, его даты рождения, последних цифр счета), с тем, чтобы обеспечить доверие жертвы. Этот вид атак применяется обычно по телефону. Например, звонки от так называемых сотрудников банка, с сообщением о том, что банковская карта или счет заблокированы или о том, что с карты был совершен крупный денежный перевод.

[1]Шумский И.Н. Социальная инженерия как искусство взлома человека // Международный студенческий научный вестник. – 2018. – № 1. – С. 62-64.

3. Квипрокво (от лат. Quidproquo — «услуга за услугу»). Суть данной техники заключается в том, что мошенники звонят по случайному номеру телефона компании и, представляясь сотрудниками техподдержки, опрашивают, есть ли какие-либо технические проблемы. При наличии проблем, в процессе их «решения» жертва под диктовку вводит команды, которые позволяют злоумышленнику запустить вредоносное программное обеспечение.

4. «Троянский конь». Эта техника основывается на любопытстве жертвы, ее доверчивости и желании получить выгоду. Злоумышленником в адрес жертвы направляется сообщение, которое содержит в себе интересное вложение, например, о выигрыше крупной суммы денег, бесплатного апгрейда программы, «громкой» новости и т.д. Пройдя по этой ссылке, пользователь вместо обещанного официального приложения или просмотра интересующей страницы скачивает себе на устройство вредоносную (троянскую) программу, которая способна, при наличии подключенной услуги «Мобильный банк», без участия абонента запрашивать баланс и выводить денежные средства с лицевого счета абонента на электронные кошельки злоумышленников.

5. «Дорожное яблоко» - этот метод является, своего рода, адаптацией «троянского коня» и требует обязательного применения какого-то физического носителя информации. Хакеры могут подбрасывать (в машину на парковке, в сумку) или оставлять в общественных местах загрузочные флеш-карты или диски, подделанные под носители с интересным и/или уникальным контентом. Атака мошенников рассчитана на то, что лицо, обнаружившее накопитель, подсоединит его к компьютеру, после чего произойдет кража персональных данных. Однако широкого распространения данная техника не имеет.

6. Взлом данных для входа на популярный социальный Интернет-ресурс. Так, мошенники, взломав страницу в социальных сетях, изучают переписку владельца аккаунта с определенными контактами, и делают им рассылку от имени владельца с просьбой занять определенную сумму денег. В данном способе мошенничества для достижения преступной цели комбинируются методы технического хакерства (подбор пароля) и социальной инженерии (рассылка сообщений друзьям жертвы с просьбой занять денег).

Как отмечает В.С. Овчинский, социальная инженерия превратилась в один из самых распространенных векторов атак на информацию, от которых сложнее всего защититься[1].

Почему же использование техник социальной инженерии мошенниками так распространено? На то есть несколько причин. Во-первых, получить доступ к технической системе безопасности, усовершенствованной новейшими средствами защиты информации, намного сложнее, чем получить ту же информацию от обычного пользователя обманным путем. Во-вторых, мошеннические схемы с использованием социальной инженерии являются более результативными, дешевыми и эффективными. В-третьих, степень вероятности быть пойманным, применяя методы психологического воздействия на жертву,

[1] Овчинский В.С. Мафия. Новые мировые тенденции «Коллекция изборского клуба». – М.: Книжный мир, 2016. – 369 с.

для их инициаторов несколько ниже, нежели вероятность, возникшая в связи с взломом технического средства.

В 2020 году в связи с ослаблением экономики, вызванным эпидемиологической обстановкой в стране, повысился уровень безработицы в стране, и как следствие произошел всплеск мошенничества с использованием компьютерных технологий. Мошенничество во втором квартале 2020 года в основном осуществлялось с помощью рассылки электронных писем (фишинга), причем мошенники незамедлительно среагировали на животрепещущие изменения в обществе. В письмах (якобы из официальных учреждений) гражданам предлагалось получить различные льготы и выплаты в связи с пандемией, взять кредит с низкой процентной ставкой. А когда в марте 2020 года на территории России начали вводить режим самоизоляции, и в некоторых регионах для посещения общественных мест от граждан требовалось оформить специальный QR-пропуск через электронный портал гос.услуг, злоумышленники немедленно среагировали на это созданием фишингового сайта для сбора персональных данных жертв. От посетителя подделанного сайта требовалось указать номер паспорта, цель поездки и отправить SMS на короткий номер. В результате таких действий с мобильного счета потерпевшего списывалась определенная сумма, а его личные данные попадали в базу мошенников, а пропуск оставался неоформленным.

В качестве вывода можно сказать, что социальная инженерия на сегодняшний день является одной из самых серьезных проблем, угрожающих сетевой и компьютерной безопасности, поскольку она использует естественную доверчивость человека и его подверженность манипулированию. Техники социальных инженеров разнообразны, но их объединяет одно — в их основе лежат когнитивные искажения, человеческая глупость и невнимательность[1].

Средства и способы защиты от социальной инженерии подразделяются на антропогенные и технические. 95% всех нарушений безопасности объясняются человеческим фактором. Поэтому важно, чтобы пользователи стали первой линией защиты, а для этого необходимо повышать уровень грамотности населения в области компьютерной безопасности[2], своевременно информировать граждан о новых способах и методах интернет-мошенничества – в этом и заключается сущность антропогенных способов защиты.

К программно-технической защите относятся средства, затрудняющие неправомерный доступ к информации. Поскольку одной из самых «популярных» техник атаки социальных хакеров в Интернете является фишинг (то есть направление электронные писем и сообщений с подложных адресов), программисты создают специальное ПО (например, Solar от «Ростелеком», Bluecoat, Websense, а также встроенные средства защиты браузеров), позволяющее анализировать и фильтровать все поступающие на электронный

[1] Бирюков М. Социальная инженерия или как не стать обманутым // Международный журнал прикладных наук и технологий «Integral». — 2018. — № 2. — С. 22–24.

[2] Tadviser. Государство. Бизнес. Технологии. [Электронный ресурс] URL: https://www.tadviser.ru/index.php/ (дата обращения 27.11.2021).

почтовый ящик данные. Фильтры анализируют тексты входящих и исходящих сообщений. Предполагается, что это позволит своевременно выявить подозрительное сообщение и не допустить утечки личных данных пользователя. Однако никакое, даже самое современное программное обеспечение не может предусмотреть всех вариаций написания потенциально опасных сообщений.

В завершение нужно отметить, что способы совершения преступлений в сфере информационных технологий постоянно совершенствуются. При этом противодействие им должно состоять в повышении компьютерной грамотности населения, а также разработке адекватных технологий защиты, чему, в свою очередь, способствует широкое обсуждение затронутых проблем на разного рода научно-представительских мероприятиях, одним из которых является сегодняшняя конференция.

Литература

1. Бирюков М. Социальная инженерия или как не стать обманутым // Международный журнал прикладных наук и технологий «Integral». — 2018. — № 2. — С. 22–24.
2. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. – М.: Международные отношения, 2020. – 288 с.
3. Овчинский В.С. Мафия. Новые мировые тенденции «Коллекция изборского клуба». – М.: Книжный мир, 2016. – 369 с.
4. Шумский И.Н. Социальная инженерия как искусство взлома человека // Международный студенческий научный вестник. – 2018. – № 1. – С. 62-64.

М.С. Орлова

Деструктивный интернет-контент как криминогенный фактор насильственных преступлений, совершаемых с применением оружия учащимися и студентами в образовательных учреждениях

Аннотация. В работе поднимается проблема деструктивного интернет-контента и его влияния, как криминогенного фактора, на совершение вооруженных нападений на образовательные учреждения. Автором приводятся практические примеры скулшутинга, где одним из факторов совершения преступления выступает увлечение учеником (студентом) запрещенными материалами, находящимися на просторах интернет-пространства. В связи с этим, автор предлагается обратить внимание на усовершенствование профилактических и предупредительных мер, направленных на борьбу с деструктивным интернет-контентом.

Ключевые слова: интернет-контент, насильственная преступность, причины и условия, колумбайн, скулшутинг.

В современном мире проблема деструктивного интернет-контента является одной из наиболее актуальных. Уже давно жизнь современного человека

невозможно представить без участия в ней информационно-телекоммуникационных технологий. Информационный контент, содержащийся на просторах интернета, не всегда оказывает только положительное влияние на его потребителей. Зачастую он носит весьма агрессивный, а порой и разрушительный характер, что в дальнейшем может привести к последствиям. Ученые уже давно бьют тревогу, что распространение деструктивного контента в сети несет в себе большую опасность для общества. Особую опасность такое явление представляет для несовершеннолетних, что обусловлено их психологическими и физиологическими особенностями. Отсутствие жизненного опыта, неспособность к категорическому мышлению, отсутствие четких установок и взглядов на окружающие их ситуации, неумение выстраивать границы между реальностью и виртуальным пространством – все это часто приводит к негативным последствиям.

В последнее десятилетие проблема вооруженных нападений учащихся и студентов на образовательные учреждения привлекла особое внимание со стороны ученых и правоохранителей, а также общества в целом. Еще в XX веке американский исследователь Глен Мачерт ввел термин, характеризующий вооруженное нападение на образовательное учреждение – скулшутинг[1]. Первый громкий инцидент, вооруженного нападения на образовательное учреждение, произошел в конце 90-х в школе «Колумбайн (округ Джефферсон, штат Колорадо, США). Двое школьников Эрик Харрис и Дилан Клибболд убили 13 человек (12 учеников и одного учителя) и ранили ещё 23 человека, после чего покончили жизнь самоубийством[2].

Спустя годы данный феномен получил свое распространение в сети-интернет. Современным фактором популяризации идей скулшутинга в России становятся интернет-сообщества, фан-аккаунты в рамках которых активно распространяются, идеологически оправдываются идеи массового убийства[3]. Только за последние восемь лет в России произошло более 30 случаев нападений учащихся и студентов на образовательные учреждения. Первый случай вооруженного нападения упомянутый в средствах массовой информации относится к ситуации, произошедшей 3 февраля 2014 года в школе № 263 мкр. Отрадное. Десятиклассник Сергей Гордеев пришел в учреждение с отцовским карабином. В результате произошедшего 2 человека погибли, 1 пострадал.[4]

Одно из наиболее резонансных вооруженных нападений на школу, произошёл 5 сентября 2017 года в Подмосковье. Девятиклассник из Ивантеевки Михаил Пивнев проник в школу, вооружённый кухонным топориком, пневматическим

---

[1] Пастыка Е. А., Питанова М. Е. Проблема вооруженных нападений подростков в образовательных учреждениях // Вестник ПензГУ. 2020. №3 (31). С. 116.

[2] Массовое убийство в школе «Колумбайн». Википедия [Электронный ресурс]. - URL: https://ru.wikipedia.org/ wiki/ (дата обращения: 11.10.2021).

[3] Пучнин А.В., Пучнина М.Ю. Влияние деструктивного интернет-контента на формирование колумбайн-идей среди несовершеннолетних // Вестник Санкт-Петербургского университета МВД России. 2021. №3 (91). С. 21

[4] Стрельба в школе № 263. Википедия [Электронный ресурс]. - URL: https://ru.wikipedia.org/ wiki/ (дата обращения: 10.10.2021).

оружием и самодельными взрывпакетами. В результате случившегося пострадало 4 человека.

Одно из наиболее масштабных по количеству жертв преступлений произошло 17 октября 2018 года в Керченском политехническом колледже. Студент Владислав Росляков через запасной вход пронёс сумку с самодельной взрывчаткой, которая была начинена металлическими поражающими элементами. Парень оставил её в буфете, и как только началась перемена взрывчатка детонировала. Затем преступник вернулся в буфет и открыл беспорядочный огонь из помпового ружья по людям. После стрельбы он совершил самоубийство. Погибли 20 человек, ещё 67 пострадали.

В ходе расследования преступлений, правоохранительными органами было установлено, что лица, совершавшие нападения на образовательные учреждения интересовались идеями «Колумбайна», состояли в интернет-сообществах, читали литературу, посвященную данной тематики, изучали материал, в той или иной мере, касающийся темы вооруженного насилия в образовательных учреждениях.

Решение данной проблемы было обозначено в конце 2018 года, Федеральным законом «О внесении изменений в статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации»[1] и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию». Так в перечень оснований включенных в "Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено был включен новый пункт касающийся информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц. При этом устанавливается, что блокировка таких сайтов должна производится незамедлительно.

Однако данные меры, нельзя считать полностью действенными. Во-первых, блокирование интернет-сообществ и интернет-групп по-прежнему требует значительного количества времени несмотря на пометку «незамедлительно». В первые дни обнаружения угрозы происходит блокирование лишь 1/3 части таких групп. Остальная часть интернет-сообществ прекращает свое существование лишь на 7- 10 день. Существуют случаи, когда информация, содержащаяся в группе, требует тщательной проверки, которая затягивает процесс блокирования на неопределенный срок. Во-вторых, блокирование интернет-контента как правило происходит лишь в тех группах, в которых освещают исключительно резонансные случаи нападения. Так, например, в рамках блокировки деструктивного интернет-контента посвященного «Колумбайну» регулярно

[1]Федеральный закон «О внесении изменений в статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»» № 472 // Парламентская газета. - 2018 г. - № 52. - Ст. 8101 с изм. и допол. в ред. от 18.12.2018.

происходит блокировка групп посвященных Эрику и Дилану (стрелкам школы «Колумбайн») однако, данный случай является не единичным ввиду чего следует обратить внимание на блокировку контента посвященного менее ярким и известным вооруженным нападениям.

Деструктивный интернет-контент является одним из наиболее важных криминогенных факторов, влияющих на совершение вооруженных нападений на образовательные учреждения учащимися и студентами. Меры, которые принимались государством нельзя назвать эффективными. О данном факте свидетельствует ежегодное увеличение численности вооруженных нападений на образовательные учреждения, а также показатели тяжких и особо тяжких преступлений, носящих насильственных характер среди молодежи.

Следующий значимый шаг на пути к борьбе с деструктивной информацией, содержащейся в сети-интернет, был сделан в сентябре 2021 года. 9 крупнейших интернет-компаний учредили Альянс по защите детей в цифровой среде, в мероприятии по видео-связи принял участие президент Российской Федерации В.В. Путин. Основной задачей, обсуждаемой на совещании, стал вопрос необходимости саморегулирования интернет-платформ для защиты детей от деструктивного контента, фейков и других интернет-угроз. По мнению участников альянса введение возрастного фильтр на фильмы ужасов, кровавые сцены и прочий контент «+18» является хорошим способом ограждения подрастающего поколения от негативного и агрессивного потока информации интернет среды. Альтернативой такого контента могут послужить комедии, фантастика и приключения, которые привлекут интерес молодого зрителя. Однако специалисты в данной обрати также отмечают, что положительную динамику в данном направлении получится достичь только при согласованном взаимодействии с родителями.

Таким образом, комплексное обеспечение информационной безопасности учащихся и студентов, путем введения новых профилактических и предупредительных мер в сфере защиты прав несовершеннолетних и молодежи от информации, причиняющей вред их здоровью, нравственному и духовному развитию, снизит число насильственных преступлений (в том числе в образовательных учреждениях), совершаемых под воздействием деструктивных интернет-контентов, а также повысит уровень правосознания обучающихся.

Литература

1. Федеральный закон «О внесении изменений в статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» от 18.12.2018 № 472-ФЗ // Парламентская газета. - 2018 г. - № 52. - Ст. 8101 с изм. и допол. в ред. от 18.12.2018.
2. Пастыка Е. А., Питанова М. Е. Проблема вооруженных нападений подростков в образовательных учреждениях // Вестник ПензГУ. 2020. №3. С. 21.

3. Пучнин А.В., Пучнина М.Ю. Влияние деструктивного интернет-контента на формирование колумбайн-идей среди несовершеннолетних // Вестник Санкт-Петербургского университета МВД России. 2021. №3. С.116.
4. Официальный интернет-портал Википедия. URL: https://ru.wikipedia.org.

А.О. Пантелеева, С.О. Ламыкина
Научный руководитель: **Скуковский А.Г.**

Извлечение доказательственной и ориентирующей информации из мобильных устройств с помощью криминалистической техники в ходе осмотра предмета и особенности ее оформления

Аннотация. При расследовании преступлений мобильный телефон становится источником доказательственной и ориентирующей информации. Для извлечения и исследования данных мобильного устройства необходимо использовать специальную криминалистическую технику. При этом особое значение имеет процессуально и тактически правильное производство следственного действия – осмотра предметов, фиксирующего криминалистически значимую информацию, извлекаемую из мобильного устройства с применением криминалистической техники.

Ключевые слова: мобильное устройство, доказательственная и ориентирующая информации, криминалистическая техника, осмотр предметов, извлечение криминалистически значимой информации.

При расследовании большинства видов преступлений мобильное устройство является важным источником доказательственной и ориентирующей информации.

Доказательственная информация — это информация, связанная с событием происшествия и обстоятельствами его совершения, которая может служить средством доказывания и быть использована в процессе доказывания в ходе доследственной проверки преступления, расследования и судебного рассмотрения уголовных дел.

При этом доказательственная информация одновременно может быть также и ориентирующей. К ориентирующей информации относят сведения о возможных носителях доказательственной информации (их характере, местах нахождения и т. д.); сведения об обстоятельствах, подлежащих доказыванию, позволяющие в последующем выбрать наиболее эффективные средства доказывания; сведения, способствующие правильно оценить всю совокупность собранных по уголовному делу доказательств. Стоит отметить, что ориентирующая информация носит вспомогательный характер по отношению к процессу оценки преступления, так как она позволяет правоприменителю ориентироваться в установленных по делу событиях и фактах, которые связаны с самим событием преступления.

Так, например, в мобильных устройствах, используемых в ходе совершения преступлений в сфере информационных технологий, сохраняются специфические следы, которые могут носить как доказательственную, так и

ориентирующую информацию, значимую для предварительного следствия. Условно данные следы можно разделить на следующие виды:

1. электронные динамические следы, т. е. следы соединениях с другими абонентами или устройствами (временя, частота, характер и содержание);

2. электронные следы, содержащиеся на устройстве, т. е. записи в телефонных книгах, заметках, данные об установленных приложениях, фотографии, электронные файлы и т.д.;

3. следы на SIM-карте, т. е. следы, оставленные непосредственно на чипе карты или в его памяти.

Таким образом, из мобильного устройства может быть извлечена следующая информация:

- о взаимодействии определённых лиц по средствам сотовой связи или приложений и мессенджеров, а также даты и времени переписки;
- о месте нахождения лица в определённое время;
- о передвижениях лица в определенное время;
- о круг интересов и увлечениях по средствам осмотра данных приложений, подписок, галереи;
- о использовании для возможных переводов приложений мобильного банка (части приложения банка имеется на телефоне);
- о наличии определенных файлов на мобильном телефоне или планшете и т.д.

Стоит отметить, что приведенный перечень извлекаемой информации не является исчерпывающим в связи с неизбежным развитием возможности техники и программного обеспечения.

Для извлечения из мобильного устройства и исследования криминалистически значимой информации следователю необходимо применять специальную криминалистическую технику, позволяющую оперативно, качественно и беспрепятственно извлечь, аккумулировать и проанализировать все данные, содержащиеся на мобильном устройстве, которые могут представлять интерес для предварительного следствия.

На сегодняшний день в следственных управлениях Следственного комитета России имеются мобильные комплексы с программным обеспечением по сбору и анализу цифровых данных, которые позволяют в короткие сроки извлечь важную (включая удаленную) информацию из памяти мобильных устройств связи, карт памяти, SIM-карт участников уголовного процесса при производстве следственных действий. К таким видам криминалистической техники сегодня относятся: Мобильный криминалист, UFED, XRY, MOBILedit, CellXtrac.

Извлекаемая информация из мобильного устройства может представлять собой важное доказательственное значение. Однако для признания полученной информации доказательством необходимо соблюдение процессуальной формы и требований, установленных ст. 88 УПК РФ, об относимости, достоверности, допустимости и достаточности. В связи с этим актуальным является процессуально правильное оформление и тактически верное производство следственного действия – осмотра предметов, в ходе которого данная информация обнаруживается, анализируется и фиксируется.

Главной особенностью осмотра мобильных устройств является то, что основная часть информации, в отличие от осмотра обычных предметов, не может быть воспринята следователем при непосредственном осмотре, в связи с чем требуется использование специальной криминалистической техники.

Как отмечают А.М. Багмет и С.Ю. Скобелин, в ходе предварительного следствия основной проблемой является процессуальный порядок оформления извлечения и анализа данных из мобильных устройств с использованием криминалистической техники. Это обусловлено тем, что в уголовно-процессуальном законодательстве не предусмотрено отдельное следственное действие по извлечению вышеуказанной информации из мобильных устройств.

На сегодняшний день в уголовно-процессуальном законодательстве и правоприменительной деятельности сложилась практика использования криминалистической техники для извлечения информации из мобильных устройств, ее анализ и фиксация в следующих процессуальных формах: назначение и проведение судебной экспертизы и осмотр предметов.

В следственной практике извлечение, анализ и фиксация информации из мобильных устройств осуществляется в рамках осмотра предметов. В результате применения криминалистической техники и (или) программного обеспечения для изъятия данных, например, UFED или Мобильный криминалист, формируется «Отчет об извлечении», в котором в аккумулированном и классифицированном виде представлены данные (в том числе удаленные, скрытые), извлеченные из осматриваемого устройства. Именно эти извлеченные данные представляют криминалистически значимую информацию и признаются доказательствами по делу. Однако имеется разная следственная практика отражения в протоколе осмотра предметов информации, содержащейся в сформированном и прилагаемом отчете.

В ходе анализа следственной практики следственных органах Следственного комитета Российской Федерации имеются следующие варианты закрепления (фиксации) криминалистически значимой информации, полученной в ходе извлечения и анализа данных из мобильного устройства при осмотре.

1. В протоколе осмотра предметов (мобильного устройства) отражается факт применения технико-криминалистического средства с указанием на приложение – сформированный отчет, в котором выделяются фрагмент (часть) данных, представляющих интерес для следствия и носящих криминалистически значимый характер. При этом в последующем в постановлении о признании и приобщении к уголовному делу в качестве вещественного доказательства - мобильного устройства с указанием на значимую информацию, содержащуюся в отчете, и обоснованием оснований приобщения.

2. Отдельный осмотр документов - отчета, полученного в ходе осмотра предметов - телефона с применением криминалистической техники, в котором отражается вся значимая для предварительного следствия информация.

3. В протоколе осмотра предметов – мобильного устройства – подробно фиксируются данные из мобильного устройства, которые представляют собой криминалистически значимую информацию.

Из приведённых выше вариантов фиксации данных, полученных из мобильного устройства, наиболее тактически и процессуально правильным, на наш взгляд, является третий вариант. В связи с тем, что основным назначением протокола следственного действия является «фиксация определенных сведений, которые устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию по уголовному делу».

Для процессуально правильного оформления и тактически верного производства осмотра предметов с применением криминалистической техники нами был составлен алгоритм производства осмотра мобильного устройства.

1. Указание на получение согласия владельца мобильного устройства или судебного решения на его осмотр.

Данное процессуальное требование вытекает из конституционного права, закреплённого ст. 13 УПК РФ: ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений (в том числе SMS-сообщения) допускается только на основании судебного решения. Позиция о необходимости судебного решение излагается и в определении Конституционного Суда Российской Федерации от 28.02.2017 № 338-О, от 25.01.2018 № 189-О, в которых отмечается, что, если в ходе осмотра мобильного телефона владелец возражает против проведения исследования имеющейся в телефоне информации, то производство осмотра без судебного решения нарушает его конституционные права.

2. Отметка о правах, обязанностях и ответственности участвующих лиц. Обязательное предупреждение понятых и иных участвующих лиц о недопустимости разглашения сведений, полученных в ходе исследования мобильного устройства, что отдельно отражается в протоколе следственного действия или оформляется подпиской о неразглашении данных предварительного расследования, которая прилагается к протоколу осмотра.

3. Указание на применение технических средств, а также кем они применяются.

4. Фотографирование мобильного устройства в упаковке и после вскрытия, а также основные этапы производства осмотра.

5. Предварительный осмотр устройства на наличие на внешних элементах иных следов, подлежащих фиксации и изъятию (следов пальцев и ладоней рук, биологических следов, микрочастиц и других).

6. Указание на объект осмотра – мобильный телефон со всеми идентифицирующими наименованиями (марка, модель и т.д.).

7. Внешний осмотр мобильного устройства и описание (цвет, форма, индивидуальные признаки, из чего выполнен, составные части, разъемы и их место нахождение; имеющиеся обозначения, маркировка).

8. Отметка о всех манипуляциях с устройством (включение, подзарядка и т.д.), введение пароля (который может быть получен от владельца при изъятии устройства), подключение к криминалистической технике с указанием способа, средства подключения субъектом применения технического средства.

9. Действия, направленные на изъятие физических и логических данных с мобильного устройства при помощи криминалистической техники. Все

производимые в ходе осмотра действия отражаются в протоколе осмотра в соответствии с требованиями УПК РФ. При этом для подтверждения получения данной информации с данного мобильного устройства с применением криминалистической техники необходимо фиксировать все этапы ее получения с помощью видео- или фотосъемки.

10. Указание на факт формирования и получения отчета по результатам применения технического средства и его приобщения к осмотру предмета. Результаты применения криминалистической техники в виде отчета прикладывает к соответствующему осмотру в печатанном или в электронном виде на CD-диске.

11. Внесение в протокол данных, извлечённых с мобильного устройства и отраженных в отчете, которые представляют интерес для следствия, с указанием категории данных, вида, времени и места (при наличии) создания (сохранения), места расположения на устройстве, содержания и т.д. Подробное описание криминалистически значимой информации.

12. Указание и описание упаковки, в которую помещается объект после осмотра (с вложением в нее первоначальной упаковки).

13. Составление и приложение фототаблицы.

14. Отметка о приложении: фототаблицы, отчета об изъятии (в электронном или печатном виде), CD-диска и т.д.

15. Внесение замечаний и дополнений от участвующих лиц, к производству следственного действия и составлению протокола.

Данный алгоритм отражает основные процессуальные и тактические аспекты производства осмотра мобильного устройства с применением технических средств.

Таким образом, осмотр мобильного устройства с применением криминалистической техники и программного обеспечения позволяет получить криминалистически значимую информацию доказательственного и ориентирующего характера. При этом стоит учитывать, что неправильное процессуальное оформленное протокола следственного действия без учета соблюдений конституционных прав и свобод влечет признание его как недопустимого доказательства. При осмотре мобильных устройств необходимо исходить из следующих требований: своевременность, законность, объективность и полнота.

Литература

1. Багмет А.М., Скобелин С.Ю. Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств // Материалы межд.научно-практ.конференции «Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях». Т.: ТГАМЭУП. №10. 2013.
2. Уголовно-процессуальное право: учебник для бакалавриата и магистратуры / В. М. Лебедев [и др.]; под общей редакцией В. М. Лебедева. — 2-е изд.,

перераб. и доп. - М.: Издательство Юрайт, 2014. URL: https://www.urait.ru/bcode/380745
3. Шхагапсоев К.З. Понятие доказательственной информации и производства следственных действий по ее проверке в районах вооруженного конфликта // Пробелы в российском законодательстве. 2017. № 2.
4. Яковлева О.А. Классификация криминалистически значимой информации и ее роль в досудебном уголовном производстве // Вестник Волгоградского государственного университета. 2016. № 5.

А.И. Рахимов

Учёт возрастных изменений при получении информации, содержащейся в идеальных следах преступления

Аннотация. В статье представлен анализ влияния возрастных изменений на процесс формирования идеальных следов преступления. Отмечено влияние возраста человека на процессы восприятия и обработки информации. Описаны особенности тактики получения и проверки информации, содержащейся в идеальных следах преступления, с учётом изменений, происходящих в психике их носителя в зависимости от возраста.

Ключевые слова: идеальный след, формирование идеальных следов, возрастные изменения в психике человека, достоверность информации, тактика получения и проверки информации.

Одной из актуальных проблем органов следствия и дознания остаётся проблема получения объективных и достоверных сведений о совершённом преступлении. Вместе с тем, значительная часть поучаемой информации это свидетельства людей, непосредственно воспринимавших преступное событие в ходе его подготовки, совершения либо сокрытия, то есть это та информация, которая содержится в идеальных следах преступления.

По своей сути идеальные следы представляют собой образы и понятия, сформировавшиеся в сознании человека во время преступного события и сохранившиеся в его памяти, использование которых, в интересах следствия, возможно только после их трансформации в доступную для восприятия другими людьми форму. Идеальные следы обладают большим информационным потенциалом, однако подвержены влиянию различных объективных и субъективных факторов, которые могут изменить их информационную составляющую. Как известно, процесс формирования идеальных следов является сложной психофизиологической деятельностью человеческого организма, который проходит несколько этапов, начиная с непосредственного восприятия конкретных объектов, предметов, действий явлений и т.д. до воспроизведения информации о них в устной, графической или иной форме. При этом происходит постоянная переработка информации, содержащейся в памяти человека. Одним из факторов, оказывающим существенное влияние на все стадии процесса формирования идеальных следов является возраст человека. Возрастные изменения проявляются во всех функциях человеческого организма,

которые развиваются с момента его рождения и, достигая своего пика, плавно угасают с приближением старости[1].

Так, например, в возрасте 3-5 лет, ещё не полностью сформирована система восприятия, а произвольное внимание ребёнка легко замещается непроизвольным. Процессы внимания совершенствуются только на 9-10 год жизни человека. У подростков к 14 годам возрастают возможности категориального и понятийного аппарата, однако при этом они могут проявлять ошибочное понимание явлений в связи с их чрезмерно расширенной, либо наоборот крайне ограниченной трактовкой. Считается, что все когнитивные функции человека выходят на оптимальный уровень своего развития к 18–20 годам [2]. Вместе с тем опираясь на научную литературу по психологии, в том числе и геронтопсихологии, можно сказать, что возрастные проблемы с процессами восприятия и памяти возникают у людей примерно с 65 лет и далее индивидуально усугубляются с возрастом.

Таким образом, достоверность получаемых от участников и очевидцев преступного события сведений обусловлена, в том числе их возрастом, который влияет на формирование идеальных следов в памяти человека, их сохранение и воспроизведение, что в свою очередь определяет эффективность проведения таких следственных действий, как допрос, очная ставка, предъявление для опознания и других вербальных следственных действий.

Кроме того, практический опыт показывает, что в своём большинстве лица малолетнего возраста и пожилые люди чаще всего являются потерпевшими или очевидцами преступного события, а работа с ними протекает в условиях бесконфликтной ситуации. Также опрос следственных работников показал, что менее всего склонны к даче ложных показаний малолетние лица (до 14 лет) и лица пожилого возраста (старше 65 лет).

Исходя из вышесказанного полагаем, что тактика получения и проверки информации, содержащейся в идеальных следах преступления должна корректироваться в соответствии с изменениями, происходящими в психике их носителя в зависимости от возраста.

Так, например, в связи с замедлением процессов обработки информации в пожилом возрасте, более чётко проявляются вербальные и невербальные признаки лжи, что облегчает выявление наличия конфликтной ситуации и позволяет своевременно применить тактические приёмы, направленные на разоблачение ложных показаний. В тоже время следует учитывать и тот факт, что противоречия в показаниях лиц пожилого возраста могут быть вызваны не

---

[1] См., например, Кагермазова Л.Ц. Возрастная психология (Психология развития) / Электронный учебник. 276 с. URL: https://chukotkabezsirot.chao.socinfo.ru/media/2019/01/25/1274339953/Vozrastnaya psixologiya_uchebnik.pdf (дата обращения 24.12.2021); Дорогина О. И. и др. Геронтопсихология: учеб. пособие.: под общ. ред. Ю.В. Лебедевой. Екатеринбург: Изд-во Урал. ун-та, 2020. 131 с.

[2] См, например, Общая психология. В 7 т. : учебник для студ. высш. учеб. заведений / под ред. Б. С. Братуся. Т.3. Память / В. В. Нуркова. М.: Издательский центр «Академия», 2006. 320 с.; Купцова А.М. и др. Физиологические основы внимания. Развитие внимания у детей и подростков. Учебно-методическое пособие. Казань. КФУ. 2017. 35 с.

только намеренной ложью, но и особенностями их восприятия, сохранения и воспроизведения обстоятельств события. Исходя из этого, считаем необходимым, при подготовке следственных действий, предварительно получать информацию о состоянии их здоровья, в том числе о состоянии органов чувств (зрения, слуха и т.д.) и когнитивных функций.

Учитывая психологические и социальные аспекты старения, первостепенное значение при работе с лицами пожилого возраста приобретает такой этап как установление психологического контакта, от которого зависит успех не только конкретного следственного действия, но и других последующих действий. Чем прочнее установлен контакт, тем охотнее люди пожилого возраста вступают в диалог, и напротив, отсутствие психологического контакта может стать причиной полного отказа от общения. Исходя из этого, при подготовке к следственному действию с участием лиц пожилого возраста, следует особое внимание уделять предварительному изучению их личности. Так, например, отношение пожилого человека к его собственным воспоминаниям «составляет значительную часть его психической жизни»[1] и может быть эффективно использовано при построении беседы. Также, не менее полезным для выбора линии поведения будет наличие информация о характере будущего собеседника, поскольку с возрастом происходит сдвиг черт характера в негативную сторону[2].

Кроме того, планируя место и время проведения следственных действий с лицами пожилого возраста целесообразно учитывать их зависимость от медицинских приборов и препаратов, возможность их перемещения, также оптимальное время напряжённой умственной работы, которое приходится на первую половину дня[3]. Учитывая вышеизложенное, а также тот факт, что лица данной категории труднее адаптируются к новым условиям, считаем более эффективным проведение с ними следственных действий, по возможности, в привычной для них обстановке, при условии отсутствия противодействия с их стороны. Определяя продолжительность следственного действия, следует исходить из состояния здоровья и самочувствия человека в конкретных условиях.

Анализ научной литературы, посвящённой проблемам старения человека, показывает, что с возрастом повышается внушаемость человека, что обуславливает необходимость выяснять факты обсуждения обстоятельств расследуемого события с другими людьми, давления со стороны заинтересованных лиц, ознакомление с публикациями в средствах массовой информации, в целях выявления и нейтрализации возможного искажения идеальных следов под влиянием внушения. Кроме того, для обеспечения наиболее полного припоминания обстоятельств исследуемого события,

---

[1] Бертовский Л. В. Особенности допроса лиц старших возрастных групп // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 4. С. 1100-1121.

[2] Дорогина О. И. и др. Геронтопсихология: учеб. пособие.: под общ. ред. Ю.В. Лебедевой. Екатеринбург: Изд-во Урал. ун-та, 2020. С. 35.

[3] Прохорова Э. М. Биологические ритмы и здоровье // Сервис +. 2010. №3. С. 20-26.

рекомендуем заранее планировать и проводить дополнительный допрос (опрос) людей пожилого возраста с перерывом в 2-3 дня.

Вместе с тем, не стоит забывать, что общение с представителями правоохранительных органов вызывает эмоциональное переживание у любого человека, особенно если оно связано с преступным событием, а для человека пожилого возраста повышенная психоэмоциональная нагрузка, с учётом состояния его здоровья, может привести к необратимым последствиям. Исходя из этого, считаем целесообразным при работе с лицами пожилого возраста иметь аптечку первой медицинской помощи и уметь правильно оказать её до прибытия квалифицированных специалистов. Кроме того, считаем необходимым обязательное применение средств видеозаписи при проведении следственных действий с участием подозреваемых (обвиняемых), потерпевших и ключевых очевидцев, относящихся к лицам пожилого возраста.

Резюмируя вышеизложенное, можно констатировать, что возрастные изменения, происходящие в психике человека, вносят определённые коррективы в тактику получения информации, содержащейся в идеальных следах преступления и должны учитываться при выстраивании линии поведения при работе с лицами пожилого возраста.

Литература

1. Бертовский Л. В. Особенности допроса лиц старших возрастных групп // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 4. С. 1100-1121.
2. Дорогина О. И. и др. Геронтопсихология: учеб. пособие. : под общ. ред. Ю.В. Лебедевой. Екатеринбург: Изд-во Урал. ун-та, 2020. 131 с.
3. Кагермазова Л.Ц. Возрастная психология (Психология развития) / Электронный учебник. 276 с. URL: https://chukotkabezsirot.chao.socinfo.ru/media/2019/01/25/1274339953/Vozrastnayapsixologiya_uchebnik.pdf (дата обращения 24.12.2021)
4. Купцова А.М. и др. Физиологические основы внимания. Развитие внимания у детей и подростков. Учебно-методическое пособие. Казань. КФУ. 2017. 35 с.
5. Общая психология. В 7 т. : учебник для студ. высш. учеб. заведений / под ред. Б. С. Братуся. Т.3. Память / В. В. Нуркова. М.: Издательский центр «Академия», 2006. 320 с.
6. Прохорова Э. М. Биологические ритмы и здоровье // Сервис +. 2010. №3. С. 20-26.

А.М. Рудаков

Самосознание и самоопределение личности как особый объект для защиты от криминальных манипуляций в интернет пространстве

Аннотация. В статье автором сделан акцент на необходимости формулирования понятий «самосознание» и «самоопределение» для практики правоприменения в целях обеспечения государственной безопасности, представлены результаты опросов, осужденных о самоопределении, предложены фундаментальные поправки в федеральный закон «О свободе совести и религиозных организациях».

Ключевые слова: убеждения, осужденные, самосознание, самоопределение.

«Проблема индивидуальности – главная психологическая и более того – политическая проблема XX века»[1] - это мнение врача-нарколога, психиатра Данилина А.Г. и мы его полностью разделяем. Попытки разрушить границы самосознания предпринимались политическими лидерами (например, лидерами фашистских режимов в Европе в начале XX века), политическими организациями (например, проекты ЦРУ по контролю за сознанием «MK ULTRA»[2], «Артишок»[3] и др.), тоталитарными сектами (например, секта «Храм Народов», по приказу лидера которой 909 человек совершили самоубийство[4]) и иными субъектами общественных отношений (например, Джордж Сорос[5]). Ставилась цель разрушить границы «Я», свести индивидуальность к нулю, дабы подчинить личность человека различным влияниям, и, в конечном итоге, личным корыстным интересам.

В XXI веке прежде скрытие и засекреченные проекты по лишению человека самосознания вышли в открытый формат. Так, в Министерстве обороны Российской Федерации заявили о развязанной против России ментальной войны. Об этом заявил советник министра обороны РФ Ильницкий А.М. «Целью новой войны является уничтожение самосознания, изменение ментальной основы общества противника», - объяснил Ильницкий А.М. Для отражения агрессивных атак на Россию необходимо перехватить инициативу, заявил другой военный эксперт Мураховский В.И., слова которого приводит РИА Новости[6].

---

[1] Данилин А.Г. - LSD. Галлюциногены, психоделия и феномен зависимости – М.: ЗАО Изд-во Центрполиграф, 2001. - 521 с. С. 240-241.

[2] Проект ЦРУ «МК-Ультра» - эксперименты над сознанием // https://topwar.ru/20913-proekt-cru-mk-ultra-eksperimenty-nad-soznaniem.html (дата обращения: 15.09.2021).

[3] Как ученый Сидни Готлиб стал «главным отравителем в ЦРУ» // https://rg.ru/2019/12/08/kak-uchenyj-sidni-gotlib-stal-glavnym-otravitelem-v-cru.html (дата обращения: 21.09.2021).

[4] Трагедия в Джонстауне. Массовое самоубийство 909 человек. // [Электронный ресурс]. URL: https://laberinti.ru/трагедия-в-джонстауне-массовое-самоу/ (дата обращения: 06.09.2021).

[5] Переписанные учебники и оранжевые революции: как миллиардер Сорос десятилетиями влияет на дела государств. https://tvzvezda.ru/news/20208162244-qn1hs.html (дата обращения: 23.08.2021).

[6] В Минобороны заявили о развязанной против России ментальной войне. https://rg.ru/2021/03/25/v-minoborony-rasskazali-o-novom-tipe-vojny-protiv-rossii.html?utm_source=yxnews&utm_medium=desktop (дата обращения: 12.09.2021).

По состоянию на 01.12.2021 в 643 исправительных колониях отбывало наказание 353 295 осужденных, в 18 воспитательных колониях для несовершеннолетних – 848 человек[1]. Смеем предположить, что бóльшая часть осужденных реализует сценарий криминального поведения, который им был навязан социально-информационным окружением, следовательно и их «самоопределение» не является аутентичным, самостоятельным, а передано на определение той социальной группе, членом которой они являются, с целью выживания в суровых, зачастую агрессивных, социальных условиях. Иными словами свобода самоопределения либо вынуждено передана группе взамен на безопасность и выживание, либо внушена в раннем возрасте, либо насильно навязана. Изложенное в частности проявляется в присвоении прозвищ в криминальной среде и в последующем в местах лишения свободы, определение групповой принадлежности осужденных, которой предписываются нормы поведения в процессе отбывания наказания в виде лишения свободы.

Наше предположение находит отражение в ответах осужденных на предложенные им вопросы. Так, на наш взгляд примечательным является мнение осужденных относительно влияния социального окружения на совершенное преступление. По мнению 11 % осужденных социальное окружение оказало 100 % влияние на их криминальное поведение, 10 % осужденных – 75 %, 27 % осужденных – 50 %, 20 % осужденных – 25 %. По мнению 6,1 % осужденных информационное окружение (средства массовой информации, Интернет) оказало 100 % влияние на совершенное ими преступление, 10,5% - 75 %, 17% - 50 %, 17% - 25 %. Абстрактное соотношение можно раскрыть на примере формирования мотивации употребления алкоголя. 80,3 % осужденных указали на влияние друзей в самом начале употребления алкоголя; 2,7 % осужденных – на подражание персонажам из фильмов, 5,4 % осужденных такое решение приняли самостоятельно. Важно отметить, что самостоятельное решение употреблять алкоголь осужденные приняли в возрасте от 6 до 18 лет (преобладающий возраст: от 14 до16 лет). Вместе с тем 51,2% осужденных утверждают, что у них был выбор иного пути, которым они не воспользовались, 21% полагают, что выбор скорее был, и 7,5% затруднились ответить.

Важно обратить внимание на последствия влияния социально-информационного окружения: самоопределение личности, ее самосознание.

В основе любых убеждений (религиозных и нерелигиозных) первично лежит вера (вера ученым, политикам, идеологам, богословам и иным субъектам, распространяющим убеждения), которую можно сформулировать в юридическом аспекте как поиск самоопределения и реализацию «свободы *само*определения»: право человека *самостоятельно* определять себя, ассоциировать свое «Я» с тем, что он считает аспектом истины, образ которой он реализует, положениям которой он следует, исповедует. В представленном аспекте представляет интерес определение своего «Я» осужденными. Так, 5,1%

[1] Краткая характеристика уголовно-исполнительной системы Российской Федерации. https://fsin.gov.ru/structure/inspector/iao/statistika/Kratkaya%20har-ka%20UIS/ (дата обращения: 16.11.2021).

осужденных полагают, что «Я» человека – это набор молекул и атомов, 3,4% – совокупность клеток, 5,1% – что-то нематериальное в теле, 13,6% – душа, 5,1% – дух. 18,6% осужденных полагают, что «Я» находиться где-то в мозге, 15,3% – считают, что «Я» – это сам мозг; 5,1% – где-то в теле, 10,2% – само тело. 15,3% осужденных затруднились ответить. Эти размышления показались не интересными 3,4% осужденным. Какие выводы можно сделать из изложенной информации? Волевой акт инициируется личностью человека: тем что она определяет как свое «Я», в том числе под воздействием физиологических процессов. На основании того, что человек понимает под своим «Я», строится обоснование и оправдание его поступка. Трагедия в Казани является подтверждением того, что значит заложить в конструкт «Я» деструктивные алгоритмы самоопределения и как следствие – криминальная самореализация[1].

В последнее время основным информационным пространством становится интернет. Наиболее активно вопросы самосознания и самоопределения как личного так и национального обострились после 2014 года (политический кризис в соседствующем государстве), особенно в период с 2020 года и по настоящее время – период распространения коронавирусной инфекции, кризисный период, провоцирующий людей сместить приоритеты, выйти из зоны комфорта, задуматься о личном самосознании и политическом самоопределении. Изложенные процессы вынудили большую часть населения сместить внимание в новостные ленты и иные информационные ресурсы интернет пространства, чем воспользовались и криминальные элементы, усилив свою деструктивную активность. Об этом можно судить по заголовкам новостей: «Деревенский школьник сам сделал себе обрезание и подался в террористы»[2]; «Экстремисты вербовали молодежь в свои ряды через соцсети»[3]; «Как туляков вербуют на работу наркодилерами - «закладчиками»»[4]; «ФСБ пресекла деятельность интернет-вербовщиков «Исламского государства»»[5]; ««Я буду везде, где разжигают ненависть» Вербовщик «Правого сектора» — о том, как российскую молодежь превращают в опасных радикалов»[6]; «Бесконтактная вербовка: как террористы заманивают молодежь через соцсети»[7].

Таким образом, мы предлагаем разделить федеральный закон «О свободе совести и о религиозных организациях» на два закона «О свободе совести и

---

[1] Казанский стрелок назвал себя богом, который ненавидит всех [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4803171 (дата обращения: 30.11.2021).

[2] См.: [Электронный ресурс]. URL: http://www.ntv.ru/novosti/831842/ (дата обращения: 30.11.2021).

[3] См.: [Электронный ресурс]. URL: http://www.ntv.ru/novosti/984656/ (дата обращения: 30.11.2021).

[4] См.: [Электронный ресурс]. URL: https://myslo.ru/news/criminal/2017-07-25-kak-tulyakov-verbuyut-na-rabotu-narkodilerami (дата обращения: 30.11.2021).

[5] См.: [Электронный ресурс]. URL: https://www.ntv.ru/novosti/1650249/ (дата обращения: 30.11.2021).

[6] См.: [Электронный ресурс]. URL: https://lenta.ru/articles/2020/11/30/verbovka/ (дата обращения: 30.11.2021).

[7] См.: [Электронный ресурс]. URL: https://ria.ru/20180228/1515459761.html (дата обращения: 30.11.2021).

сомоопределения» и «О религиозных организациях» (аналогично «О политических партиях», отчасти регулирующий политические убеждения). В федеральном законе «О свободе совести и свободе сомоопределения» предусмотреть организационно-правовой механизм регулирования общественных отношений по формированию убеждений и самоопределения личности в аспекте функционирования федеральных законов «О религиозных организациях», «О политических партиях», «О средствах массовой информации», «О защите детей от информации, причиняющей вред их здоровью и развитию».

В федеральном законе «О свободе совести и сомоопределения» необходимо перечислить «иные убеждения» и отразить такие понятия как: «Самосознание», «Образ «Я»», «Сознание». Важно отметить, что такие понятия, как «бессознательное», «образ «Я», «самосознание», «мышление», уже определены в ГОСТ Р 43.0.21-2020. «Национальный стандарт Российской Федерации. Информационное обеспечение техники и операторской деятельности. Сознание и самосознание», утвержденного и введенного в действие Приказом Росстандарта от 24.07.2020 № 403-ст. Для того, чтобы указанные понятия были задействованы в обеспечении государственной безопасности, их необходимо включить в предлагаемый нами федеральный закон и определить порядок функционирования организационно-правового механизма фильтрации информации, обучения граждан в сфере критического восприятия получаемой информации на подобие такого, который действует в настоящее время в отношение информации о коронавирусной инфекции (правовая ответственность за заведомо ложную информации об инфекции, повышенная информационная активность средств массовой информации с целью просвещения и пропаганды).

Литература

1. Бесконтактная вербовка: как террористы заманивают молодежь через соцсети. [Электронный ресурс]. URL: https://ria.ru/20180228/1515459761.html (дата обращения: 30.11.2021).
2. В Минобороны заявили о развязанной против России ментальной войне // «Российская газета». [сайт]. URL: https://rg.ru/2021/03/25/v-minoborony-rasskazali-o-novom-tipe-vojny-protiv-rossii.html?utm_source=yxnews&utm_medium=desktop (дата обращения: 12.09.2021).
3. Данилин А.Г. Homo servus: человек зависимый. - М. Зебра Е, - 2018. - 576 с.
4. Деревенский школьник сам сделал себе обрезание и подался в террористы.[Электронный ресурс]. URL: http://www.ntv.ru/novosti/831842/ (дата обращения: 30.11.2021).
5. Как туляков вербуют на работу наркодилерами - «закладчиками». [Электронный ресурс]. URL: https://myslo.ru/news/criminal/2017-07-25-kak-tulyakov-verbuyut-na-rabotu-narkodilerami (дата обращения: 30.11.2021).

6. Как ученый Сидни Готлиб стал «главным отравителем в ЦРУ» // «Российская газета»: [сайт]. URL: https://rg.ru/2019/12/08/kak-uchenyj-sidni-gotlib-stal-glavnym-otravitelem-v-cru.html (дата обращения: 21.09.2021).
7. Казанский стрелок назвал себя богом, который ненавидит всех [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4803171 (дата обращения: 30.11.2021).
8. Краткая характеристика уголовно-исполнительной системы Российской Федерации // «Официальный сайт ФСИН России». [сайт]. URL: https://fsin.gov.ru/structure/inspector/iao/statistika/Kratkaya%20har-ka%20UIS/ (дата обращения: 16.10.2021).
9. Переписанные учебники и оранжевые революции: как миллиардер Сорос десятилетиями влияет на дела государств // Сетевое издание «Телеканал «Звезда». [сайт]. URL: https://tvzvezda.ru/news/20208162244-qn1hs.html (дата обращения: 23.08.2021).
10. Проект ЦРУ «МК-Ультра» - эксперименты над сознанием // «Военное обозрение»: [сайт]. URL: https://topwar.ru/20913-proekt-cru-mk-ultra-eksperimenty-nad-soznaniem.html (дата обращения: 15.09.2021).
11. Трагедия в Джонстауне. Массовое самоубийство 909 человек. // [Электронный ресурс]. URL: https://laberinti.ru/трагедия-в-джонстауне-массовое-самоу/ (дата обращения: 06.09.2021).
12. ФСБ пресекла деятельность интернет-вербовщиков «Исламского государства». [Электронный ресурс]. URL: https://www.ntv.ru/novosti/1650249/ (дата обращения: 30.11.2021).
13. Экстремисты вербовали молодежь в свои ряды через соцсети.[Электронный ресурс]. URL: http://www.ntv.ru/novosti/984656/ (дата обращения: 30.11.2021).
14. «Я буду везде, где разжигают ненависть» Вербовщик «Правого сектора» — о том, как российскую молодежь превращают в опасных радикалов. [Электронный ресурс]. URL: https://lenta.ru/articles/2020/11/30/verbovka/ (дата обращения: 30.11.2021).

М.И. Сайфуллина

Нормативно-правовое регулирование в сфере борьбы против детской и молодежной порнографии в сети Интернет (на примере Федеративной Республики Германии)

Аннотация. В научной статье раскрываются особенности становления уголовного законодательства в сфере противодействия детской и молодежной порнографии. Анализу подвернулись отдельные составы - § 176a § 184, 184b с УУ ФРГ содержащее термин «Контент». Автор исследовал особенности работы правоохранительных органов ФРГ в сфере противодействия детской и молодёжной порнографии в сети Интернет.

Ключевые слова: детская и молодежная порнография, цифровые медиа и даркнет, порнографический контент, Федеральное управление уголовной полиции.

Рост преступлений в сфере незаконного оборота порнографических материалов и предметов с использованием «всемирной паутины», т.е. сети Интернет, сегодня является одной из главных угроз национальной безопасности любого государства, потому что посягает на нравственные и духовные устои общества, на развитие будущего поколения.

Так, по данным Британского фонда наблюдения за Интернетом (Internet Watch Foundation (IWF)), в период пандемии COVID-19 за 2020 год, 33% веб-сайтов с детской порнографией содержали сцены изнасилования или сексуальных пыток с участием детей, где 55% показанных детей были в возрасте младше 10 лет и 2% младше 2 лет[1]. Одним из негативных последствий развития Интернета стало возникновение таких новых форм как - секс-вымогательство, дикпик, кибергрумин, секстинг.

По данным полиции ФРГ, в 2020 г. был зарегистрирован 18761 случай детской порнографии, что на 53% больше чем в 2019 г. (соответственно 12 262 случая). Комиссар федерального правительства по борьбе со злоупотреблениями Йоханнес-Вильгельм Рёриг подчеркнул, что «Защита должна быть там, где есть дети и подростки! Это все больше влияет на социальные сети и онлайн-Игры»[2]. Для правоохранительных органов ФРГ использование цифровых медиа и даркнет при создании и распространении детской и молодежной порнографии в Сети - Интернет стало серьезным вызовом, потому что особенность раскрытия преступлений в сфере незаконного оборота порнографии в сети «Интернет» заключается в высокой степени латентности и транснациональном характере негативного явления. Это вызывает определенные сложности в доказывании, потому что создатели и распространители порнографии активно используют возможности Интернета для создания каналов быстрого распространения порнопродукции, сокрытия следов, и конечно же получения денег.

Законодательство в сфере защиты детей и молодежи от сексуального насилия ФРГ подвергалась серьезным изменениям в 1969; 1973; 1993; 1998 годах, но начиная с начала 2000-х годов в Германии была развернута беспрецедентная компания по борьбе с детской порнографией[3]. Существенные изменения в сторону расширения уголовно-правовых составов и повышения пределов наказания были внесены в Уголовное уложение ФРГ (далее УУ ФРГ) в декабре

[1]Полиция регистрирует все больше случаев жестокого обращения с детьми// [Электронный ресурс] URL: https://www.tagesspiegel.de/politik/hier-ist-ein-kipppunkt-erreicht-polizei-registriert-mehr-faelle-von-kindesmissbrauch/27224198.html (Дата обращения 03.05. 2021).

[2] Представление количества детей-жертв насилия - оценка полицейской статистики преступности (PKS) 2020 // [Электронный ресурс] URL: https://www.bka.de/DE/Presse/Listenseite_ Pressemitteilungen /2021/Presse2021/210526_pmkindgewaltopfer.html (Дата обращения 011.05. 2021).

[3] Сайфуллина М. И., Аммар А. К. Становление уголовного законодательства ФРГ об ответственности за преступления против полового самоопределения детей и молодежи // Современная наука: актуальные проблемы теории и практики. Серия: ЭКОНОМИКА и ПРАВО. -2020. -№12. -С. 173-177 DOI 10.37882/2223.

2003 года[1]. В отдельных составах - § 184a, 184b, 184c УУ ФРГ законодатель выделил «простую» и «жесткую» порнографию, отнеся к последней детскую и молодежную порнографию.

В ходе реформы 2015 года в отдельные составы были выделены §184d, §184e, §184g УУ ФРГ предусматривающие уголовное наказание за:

- обеспечение доступа к порнографическому содержанию посредством вещания или телекоммуникаций средств массовой информации:

- за получение детьми-молодежью порнографического контента через Телемедиа[2].

Значимые изменения в УУ ФРГ произошли в январе и марте 2020 года. Так, стали криминализированы попытки связаться с несовершеннолетними онлайн через Интернет с целью сексуального насилия[3]. Законодатели расширили полномочия сотрудников полиции в рамках уголовного расследования. С разрешения судьи полицейским дано право использовать сгенерированные детские порнографические материалы для получения доступа к соответствующим интернет-платформам[4].

Незаконное распространение детской порнографии практически полностью перешло во «Всемирную патину», широкое же использование контента не только позволяло молниеносно передавать файлы, но и затрудняло правоохранительным органам раскрывать преступления. С 1 января 2021 года в диспозиции § 184 УУ ФРГ законодатель ввел термин «содержание», под которым понимается «порнографический контент».

Контент (в переводе от англ. Content означает «содержание, содержимое») обозначает любую информацию на сайте. Это может быть журналы, фотографии, фильмы, тексты, звуковая графическая информация. В соответствии с § 11 УУ ФРГ «Личные и материальные условия» под содержанием понимается то, что содержится в письменной форме, на носителях звука или изображения, на носителях данных, изображениях или других вариантах осуществления, или передается независимо от хранения посредством информационных или коммуникационных технологий. Таким образом, законодатель не только изменил название статей, но и расширил понятие.

16 июня 2021 года Бундестаг ввел в УУ ФРГ ст. § 176a. «Сексуальное насилие над детьми без физического контакта с ребенком», в соответствии с которой уголовному преследованию сегодня подвергаются лица использующие

[1] Gesetz zur Änderung der Bestimmungen über Verbrechen gegen die sexuelle Identität und zur Änderung anderer Bestimmungen vom 27. Dezember 2003, Federal Law Bulletin, Teil I 2003 Nr. 67 vom 30. Dezember. 2003. S. 3007-3012.

[2] Neunundvierzigstes Strafverfolgungsgesetz nach dem Strafgesetzbuch - Politische oder politische Richtlinien zum sexuellen Strafrecht 21. Januar 2015, Federal Law Bulletin, Teil I, Nummer 2 vom 26. Januar 2015, Seiten 10-15.

[3] 57. Gesetz zur Änderung des Strafgesetzbuches – Strafrechtliche Haftung für Cyber-Grooming vom 3. März 2020, Bundesanzeiger, Teil I 2020 Nr. 11 vom 12. März 2020, Seiten 431-432

[4] Siebenundfünfzigstes Gesetz zur Änderung des Strafgesetzbuchs - Cyber-Verbrechen, 3. März 2020, Federal Law Bulletin, 2020 Teil I Nr. 11, 12. März 2020. S. 431-432.

информационные или коммуникационные технологии с целью побудить ребенка:

- к половым актам, которые он или она должен совершить с виновным либо с третьим лицом;

- совершить действия, предусмотренные § 184b абзац «Распространение, приобретение и хранение детской порнографии»[1].

К иным нормативно-правовым актам, регулирующим защиту детей от детской порнографии необходимо отнести:

- Закон «Об охране молодёжи» в ред. от 10 марта 2017 г. (JuSchG) - § 15 параграф 2 № 4;

- Договор о защите человеческого достоинства и защитах несовершеннолетних в радиовещании и TeleMedia (JMStV) - 4 Параграф 1 № 9[2], нормы которых запрещают изображать несовершеннолетних в неестественно гендерно-чувствительном положении.

В июне 2013 года вступил в силу Закон «Об усилении прав жертв сексуальных надругательств» (StORMG)[3]. Серьезным изменениям подвергся институт срока давности. Так, начало срока давности по уголовному праву стал течь с момента достижения потерпевшим 21 года, а не 18 лет как ранее. Срок давности по серьезным сексуальным преступления стал истекать не раньше, чем жертва достигнет 41 года. Срок давности по гражданскому праву с 3 лет (начиная отсчет с 21 года) законодатель увеличил до 30 лет. Это распространилось не только на иски о возмещении ущерба из-за умышленного нарушения права на сексуальное самоопределение, но также и на умышленные посягательства на жизнь, тело, здоровье и свободу.

22 декабря 2015 года вступил в силу Закон об усилении прав жертв в уголовном судопроизводстве (3-Закон «О реформе прав потерпевших»), укрепивший информационные права жертв уголовных правонарушений в уголовном судопроизводстве и законное право на поддержку психосоциального процесса, данное право стало действовать с 1 января 2017 года[4].

Правоохранительные органы ФРГ активно противодействуют распространению детской и молодежной порнографии. Так, в период с 2000 по 2021 г. правоохранительными органами ФРГ на всей территории были проведены такие общенациональные операции как «Марси» (2003 г.); «Микадо» (2007 г.) «Суси» и «Сион» (2009 г. Бавария). В 2017 году в Германии была

---

[1] Gesetz über sexuellen Missbrauch von Kindern vom 16. Juni 2021, Bundesgesetzblatt Teil I, 2021, Nummer 33 vom 22. Juni 2021, Seiten 1810-1818.

[2] Vertrag über den Schutz der Menschenwürde und den Schutz Minderjähriger in Rundfunk und TeleMedia (JMStV) vom 1. April 2003 (geändert am 1. Oktober 2016).

[3] Федеральный Закон ФРГ «О реализации прав потерпевших» // [Электронный ресурс] URL: https://www.bgbl.de /xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_ id%3D%27 bgbl113s 1805. pdf%27%5D#__bgbl__ %2F%815590 (Дата обращения 14.07. 2021).

[4] Gesetz zur Stärkung der Opferrechte im Strafverfahren (3. Opferrechtsreformgesetz) // Gesetz vom 21. Dezember 2015 - Bundesgesetzblatt I für 2015, Nr. 55 vom 30. Dezember 2015, S. 2525[Электронный ресурс] URL: https://dip.bundestag.de/vorgang/.../65145 (Дата обращения 17.08. 2021).

закрыта крупнейшая платформа детской порнографии «Элизиум» у которой было около 90000 пользователей. В мае 2021 года Федеральное управление уголовной полиции совместно с Центральным управлением по борьбе с Интернетом и компьютерными преступлениями при прокуратуре г. Франкфурта-на Майне закрыли платформу «Бойстаун» которой пользовались 400000 человек. Данная платформа была создана в июне 2019 года, с целью международного обмена жесткой детской порнографии. Доступ возможен был только через Darknet.

В целях противодействия детской и молодежной порнографии в рамках программы «Police 2020» в январе 2020 г. на территории Нижней Саксонии в качестве пилотного проекта стало действовать программное обеспечение на основе искусственного интеллекта (ИИ). Данный проект был разработан ИТ-экспертами Государственного управления криминальной полиции Нижней Саксонии[1].

Таким образом, детская и молодежная порнография является глобальной проблемой для ФРГ. На протяжении многих десятилетий правоохранительные органы ищут оптимальные механизмы борьбы с этим злом, однако появление новых цифровых форм преступности в сети Darknet стало очередной серьезной угрозой для немецкого общества. Правительству ФРГ необходимо предпринимать срочные комплексные (политические, социально-экономические, законодательные) меры в противодействии детской и молодежной порнографии в сети Интернет. Поэтому полагаем, что законодательные изменения 2020 и 2021 года помогут более детально и профессионально правоохранительным органам ФРГ противодействовать данным преступлениям.

Литература

1. Strafgesetzbuch des Deutschen Reiches vom 15. Mai 1871 // [Электронный ресурс] URL: https://www.google.com/search?q(Дата обращения 01.09. 2020).
2. Представление количества детей-жертв насилия - оценка полицейской статистики преступности (PKS) 2020 // [Электронный ресурс] URL: https://www.bka.de/DE/Presse/Listenseite_ Pressemitteilungen /2021/Presse2021 /210526 _pmkindgewaltopfer.html (Дата обращения 01.09. 2020).
3. Сайфуллина М. И., Аммар А. К. Становление уголовного законодательства ФРГ об ответственности за преступления против полового самоопределения детей и молодежи // Современная наука: актуальные проблемы теории и практики. Серия: ЭКОНОМИКА и ПРАВО. -2020. -№12. -С. 173-177.

[1] Искусственный интеллект: LKA Niedersachsen предоставляет программное обеспечение для борьбы с детской порнографией по всей стране //[Электронный ресурс] URL: https://www.lka.polizei-nds.de/a/presse/pressemeldungen/kuenstliche-intelligenz-lka-niedersachsen-stellt-software-zur-bekaempfung-von-kinderpornografie-bundesweit-zur-verfuegung-114750.html(Дата обращения 04.10. 2021)

А.Л. Санташов
Ю.Ю. Собина

Использование информационных технологий в противоправной экономической деятельности

Аннотация. В статье рассматриваются проблемы использования информационных технологий в противоправной экономической деятельности. Особое внимание автор уделяет наиболее распространенным в настоящее время в Российской Федерации схемам уклонения от платы налогов. Делается вывод о том, что научно-технический прогресс, являясь существенным фактором экономического роста, всегда будет обсуживать интересы нелегального сектора экономики, что ставит перед органами государственной власти новые задачи по созданию механизмов реагирования на возникающие вызовы современности.

Ключевые слова: информационные технологии, интернет, налоги, юридическое лицо, уголовная ответственность.

Применение информационных технологий в настоящее время является обыденным и повсеместным, их стремительное развитие оказывает существенное влияние на все области человеческой деятельности, в том числе на экономику, бизнес, криминалитет и, соответственно, правоохранительную систему.

В 1998 году в России специалистами Автобанка разработан «Интернет Сервис Банк», получивший название «интернет-банкинг» - программное обеспечение, основанное на западных банковских финансовых инструментах, предназначенных для дистанционного предоставления своих услуг посредством сети интернет.

Использование данного продукта основано на заключении кредитным учреждением с клиентом договора с последующей передачей последнему ключа «клиент-банк» для доступа в систему, используя который клиент получает возможность оперативно дистанционно управлять расчетным счетом своей организации с любого компьютера или мобильного устройства, имеющего выход в систему интернет-банкинга.

Заключение договора и выдача ключа «клиент-банк» кредитным учреждением осуществляется с единоличным исполнительным органом организации, то есть лицом, имеющим в силу закона или на основании доверенности право на осуществление организационно-распорядительных, административно-хозяйственных и управленческих полномочий в юридическом лице.

Схожую по своей природе услугу предлагают операторы сдачи налоговой отчетности, которые специализируются на разработке и внедрении систем защищенного электронного документооборота для представления электронной отчетности через Интернет. Принцип взаимодействия юридических лиц с налоговыми органами аналогичен описанному выше и также осуществляется с использованием электронного ключа, который оформляется оператором и

выдается представителю организации, имеющему в силу закона или на основании доверенности право на предоставление налоговой отчетности.

Федеральным законом от 06.04.2011 № 63-ФЗ (ред. от 02.07.2021) "Об электронной подписи"[1] нормативно урегулированы отношения в области использования электронных подписей, что предоставило физическим и юридическим лицам возможность совершать гражданско-правовые сделки, получать государственные и муниципальные услуги, реализовывать свои права при исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Указанные инструменты безусловно упростили работу и существенно оптимизировали процессы хозяйственной и обыденной деятельности граждан и организаций, однако наряду с законопослушными субъектами гражданских правоотношений эти же инструменты предоставили представителями криминальной среды возможность по расширению сфер противоправной деятельности.

В настоящее время эти возможности активно используются недобросовестными лицами, преследующими цели по незаконной оптимизации налогообложения, в том числе с использованием номинальных руководителей и подставных лиц; лицами, осуществляющими незаконную банковскую деятельность; лицами, оказывающими услуги по изготовлению и предоставлению заказчикам документов формального документооборота; лицами, осуществляющими неправомерный оборот средств платежей; лицами, вовлеченными в противоправную деятельность по образованию (созданию, реорганизации) юридических лиц через подставных лиц; лицами, квалифицирующимися на осуществлении рейдерских захватов предприятий, а также легализации денежных средств или иного имущества и др.

Ряд выгодоприобретателей бизнеса, заинтересованных в положительных финансовых результатах хозяйственной деятельности предприятия за счет незаконной налоговой оптимизации, в целях конспирации своих противоправных действий используют возможности информационных технологий при назначении в качестве единоличного исполнительного органа организации номинального руководителя, с которым кредитными учреждениями, операторами сдачи налоговой отчетности и удостоверяющими центрами заключаются договоры дистанционного обслуживания и которым выдаются электронные ключи для доступа в системы. Данные ключи впоследствии передаются и фактически используются конечными выгодоприобретателями, принимающим решения и осуществляющим юридически значимые действия.

Наиболее распространенная в настоящее время в Российской Федерации схема уклонения от платы налогов также основана на использовании реквизитов фиктивных организаций, которые регистрируются уполномоченными органами

[1] См.: СПС «КонсультантПлюс».

на подставных лиц с оформлением на их имя документов и выдачей необходимых ключей, которые ими в дальнейшем не используются.

Наличие большого количества таких фиктивных организаций необходимо и при осуществлении незаконной банковской деятельности, в ходе которой посредством счетов данных компаний осуществляется «транзит» и «обналичивание» денежных средств заказчиков, а также при оказании незаконных услуг по предоставлению «бумажного» НДС.

Только по официальным данным департамента финансового мониторинга и валютного контроля Банка России за 9 месяцев 2020 года незаконно обналичено 21 млрд. руб., что практически вдвое меньше, чем за аналогичный период 2020 года, когда было незаконно обналичено чуть больше 41 млрд. руб.

Сама по себе деятельность по незаконному созданию образованию (созданию, реорганизации) юридических лиц через подставных лиц является уголовно-наказуемой, как для лиц, которые данные организации регистрируют, так и для подставных лиц, на которых они регистрируются (ст.ст. 173.1, 173.2 УК РФ).

Осуществление рейдерских захватов предприятий путем фальсификации данных ЕГРЮЛ также не обходятся без использования современных информационных технологий и дистанционного предоставления в орган, осуществляющий государственную регистрацию юридических лиц, недостоверных сведений.

Совершение финансовых операций и других сделок с денежными средствами или иным имуществом, приобретенных преступным путем, традиционно сопровождается использованием описанных инструментов.

Кроме того, в связи с внедрением ФНС России системы АИС «Налог-3» и программных комплексов АСК НДС-2, АСК НДС-3, которые способны эффективно выявлять не только «налоговые разрывы», но и налоговых выгодоприобретателей, широкое распространение на «сером» финансово-технологическом рынке получают услуги по незаконному изготовлению через удостоверяющие центры дубликатов ключей ЭЦП на имя руководителей предприятий, фактически об этом не осведомленных. В последующем путем их применения в сети интернет в налоговые органы от имени юридических лиц предоставляются налоговые деклараций с, например, исчисленным к уплате налогом на добавленную стоимость по правоотношениям с организацией, с которой фактически гражданско-правовых отношений никогда не имелось. Тем не менее, данная организация получает возможность на применение налогового вычета, который программный комплекс АСК НДС-3 не распознает как «разрыв».

Также в ряде Telegram каналов и иных публичных источниках можно найти информацию об услугах по уводу программных комплексов ФНС России от конечных выгодоприобретателей в незаконных схемах налоговой оптимизации путем создания целой цепочки финансовых операций и документооборота с применением современных информационных технологий.

Дубликаты ключей ЭЦП зачастую используются для внесения в ЕГРЮЛ недостоверных сведений о юридическом лице, будь то недостоверные сведения

об учредителях (участниках) юридического лица, данные о его юридическом адресе или состоятельности (банкротстве).

Согласно данным, приведенным на сайте Банка России, чистый отток капитала из Российской Федерации в 2021 году вырос до $72 млрд. против $50,4 млрд. в 2020 году.

Существенная часть этого колоссального объёма денежных средств выведено вследствие совершения валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов и уклонения от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации.

Закономерно указанные противоправные действия совершаются с применением ранее описанных механизмов современных информационных технологий, в том числе предоставляющих возможность по дистанционному открытию счетов в российских и заграничных кредитных учреждениях (без их фактического посещения), использованию подложных ЭЦП хозяйствующих субъектов, оказанием услуг по изготовлению обосновывающих подложных документов, дистанционному таможенному декларированию и т.д.

Обеспокоенность государственных органов текущей ситуацией не раз являлась предметом расширенных обсуждений. Процедура администрирования, оформления и выдачи ЭЦП специализированными удостоверяющими центрами (УЦ) в силу изложенных и иных обстоятельств продемонстрировала свою несостоятельность, в связи с чем в 2021-2022 году в силу вступили и вступают поправки к Федеральному закону № 63-ФЗ «Об электронной подписи» и появляются подзаконные акты.

С 1 июля 2021 года ФНС стала выдавать электронные подписи руководителям коммерческих организаций и ИП.

После 1 июля 2021 года многие УЦ не могут выдавать электронные подписи любым лицам и организациям, поскольку не прошли аккредитацию по обновленным требованиям 63-ФЗ. На рынке осталось несколько десятков УЦ.

Если до 31 декабря 2021 года УЦ, аккредитованный по новым требованиям 63-ФЗ, выдал электронную подпись, то такая подпись продолжит действовать до 31 декабря 2022 года, если не закончится раньше. После этого ее нужно будет заменить по новым правилам.

Необходимо отметить, что не только представители преступного сообщества активно используют современные информационные технологии в целях достижения своих целей. Разумеется, правоохранительными органами наработан большой объём знаний и технологий по выявлению и документированию противоправной деятельности подозреваемых (обвиняемых). В зависимости от характера и вида осуществляемой противоправной деятельности могут быть задействованы инструменты по деанонимизации в сети интернет, фиксации однородных признаков цифровых портретов злоумышленников и их взаимосвязи с использованными предметами и средствами совершения преступления. При получении первичных отправных данных из кредитных, налоговых и иных учреждений, по-прежнему остаются эффективными

традиционные способы получения доказательств путем постепенного и последовательного установления обстоятельств произошедшего методом дедукции, поскольку в отличие от вещественных документальных доказательств незаконной финансовой деятельности, которые преступники могут уничтожить, информация о совершенных операциях через сеть интернет сохраняется навсегда или на протяжении длительного периода времени.

Научно-технический прогресс, являясь существенным фактором экономического роста, всегда будет обсуживать интересы нелегального сектора экономики, что ставит перед органами государственной власти задачи по созданию механизмов реагирования на возникающие вызовы, с которыми в Российской Федерации справляются своевременно и эффективно.

В.С. Танцюра
Научный руководитель: **Санташов А.Л.**

Противодействие киберпреступлениям в сфере обращения лекарственных средств, медицинских изделий и биологически активных добавок

Аннотация. В статье рассматриваются вопросы международного сотрудничества по борьбе с преступностью в сфере обращения лекарственных средств, медицинской продукции, пищевых добавок. Уделяется внимание вопросам функционирования государственных и межгосударственных органов по вопросам пресечения преступности в области фармацевтики. Приводится положительный опыт проведения мероприятий, направленных на пресечение криминальных проявлений в сфере обращения лекарственных средств и медицинской продукции, в том числе через интернет-пространство. Рассматриваются вопросы совершенствованию деятельности органов государственной власти и негосударственных образований с целью эффективного противодействия преступности в сфере оборота лекарственных средств, медицинских изделий и биологически активных добавок.

Ключевые слова: международное сотрудничество, лекарственные средства, медицинские изделия, биологически активные добавки, интернет-пространство, фармацевтический фальсификат, правоохранительная деятельность.

В настоящее время большинство государств и мировое сообщество испытывает беспрецедентный рост преступности на фармацевтическом рынке, что представляет глобальную проблему всего человечества в текущем столетии. Сложившаяся обстановка в большей степени связана с ежегодно увеличивающемся спросом на медицинские изделия, лекарственные препараты, биологически активные добавки, что продиктовано распространением во всем мире пандемии COVID-19, которая вызвала бум интернет-мошенничества, как на национальном, так и международном уровне. Распространение поддельных лекарств через Интернет давно стало одним из постоянных источников дохода трансконтинентальных преступных группировок. Безусловно, данная ситуация не остается без внимания как мирового сообщества, так и национальных правоохранительных структур, так как объектом преступного посягательства является жизнь и здоровье человека. Решение рассматриваемой проблемы

требует согласованных активных действий, как на национальном уровне, так и на уровне международного сотрудничества, что заложено в Конвенции Совета Европы «О борьбе с фальсификацией медицинской продукции и сходными преступлениями, угрожающими здоровью населения» (Конвенция «MEDICRIME»). Конвенция «MEDICRIME» предусматривает включение в структуру национального уголовного законодательства норм, предусматривающих ответственность за оборот лекарственного и медицинского фальсификата.

В силу данного обстоятельства с целью пресечения недоброкачественной медицинской и фармацевтической продукции объективно активизировалась деятельность общественных организаций, фармацевтических компаний, государственных структур, как в рамках отдельных государств, так и на международном уровне. Проблемы транснационального распространения фармацевтического и медицинского фальсификата неоднократно рассматривались на парламентских ассамблеях Совета Европы, заседаниях Европейского Совета, Международной фармакологической федерации (FIP), постоянно обсуждаются на Ассамблеях Всемирной организации здравоохранения (ВОЗ). По оценкам экспертов Всемирной организации здравоохранения, оборот поддельных медикаментов составляет около 430 млрд долларов в год, ежегодно по всему миру от приема фальсифицированной лекарственной продукции умирают сотни тысяч людей.

Первичная роль в международном противодействии преступности в фармацевтической сфере отводится Международной организации уголовной полиции в лице Национального центрального бюро Интерпола МВД России. Подразделениями НЦБ Интерпола МВД России совместно с органами ФТС России, Росздравнадзора на регулярной основе проводятся беспрецедентные операции «Фармаколог» и «Аптека», направленные на пресечение преступлений в сфере оборота фармацевтической продукции, в том числе в сети Интернет. На постоянной основе ежегодно в рамках международной операции «Пангея» в течении более 10 лет НЦБ Интерпола МВД России осуществляются мероприятия, направленные на координацию и повышение эффективности взаимодействия правоохранительных органов более 90 стран-участниц по борьбе с преступностью в сфере обращения медицинских изделий, лекарственных средств, биологически активных добавок.

Так, в период с 18 по 25 мая 2021 года НЦБ Интерпола МВД России на территории России было организовано проведение операции «Пангея», в которой приняли участие территориальные подразделения МВД России, ФТС России, Роспотребнадзора, Росздравнадзора. В ходе проведения операции было проведено около 17 тысяч оперативно-профилактических мероприятий. В результате предпринятых мер было выявлено более 1,2 тысяч правонарушений в сфере оборота незарегистрированных и контрафактных лекарственных средств и медицинских изделий, составлено более 600 протоколов об административных правонарушениях, возбуждено 85 уголовных дел, задержано 72 лица, подозреваемых в совершении преступлений, принято решение о блокировании

более тысячи интернет-сайтов, часть из которых принадлежит сегментам зарубежных государств.

Следует обратить внимание на вопрос расширения взаимодействия с фармацевтическими предприятиями, коммерческими и общественными организациями по вопросам пресечения распространения медицинского фальсификата. В частности, в 2021 году представители общественной организации «Общественная потребительская инициатива» направили в правоохранительные органы России обращение по факту обнаружения на онлайн-площадках AliExpress, «СберМегаМаркет», «Сбераптека» и «Яндекс.Маркет» 90 продавцов биологически активных добавок, в составе которых содержатся психотропные, наркотические, сильнодействующие или ядовитые вещества.

В ходе проведения ежегодных оперативно-профилактических мероприятий «Аптека» и «Фармаколог» сотрудниками правоохранительных органов необходимо привлекать специалистов Росздравнадзора, Роспотребнадзора для объективной и правильной оценки проверяемых фактов. На постоянной основе следует проводить мероприятия по обмену информацией с сотрудниками структурных подразделений по контролю и надзору за обращением лекарственных средств, медицинских изделий, биологически активных добавок с целью своевременного реагирования на факты противоправной деятельности в фармацевтической сфере. Вопросы организации взаимодействия правоохранительных органов с контрольно-надзорными структурами объективно обусловлены высокой степенью латентности правонарушений и преступлений в сфере обращения лекарственных средств, изделий медицинского назначения, биологически активных добавок.

Литература

1. Пособие для парламентариев. Конвенция Совета Европы о борьбе с фальсификацией медицинской продукции и сходными преступлениями, угрожающими здоровью населения (Конвенция «МЕДИКРИМ». СДСЕ № 211. [электронный ресурс] // URL: https :/ / rm . coe. int/16806a9676 (дата обращения 14.12.2021).
2. Терехов А. Ю. Международно-правовые средства предотвращения оборота фальсифицированных лекарственных препаратов: Автореф. дис. … канд. юрид. наук. М., 2011.
3. Российские полицейские приняли участие в международной операции Интерпола «Пангея». [электронный ресурс] // URL: https://www.rbc.ru/rbcfreenews/ 6139b1519a7947c71ae425b6 (дата обращения 28.12.2021).
4. «Подмешивают яды»: чем рискуют покупатели, заказывая БАД за рубежом. [электронный ресурс] // URL: https://ria.ru/20211005/dobavka-1753049831.html (дата обращения 28.12.2021).

М.Г. Терехов
Научный руководитель: **Шаронов С.А.**

Гражданско-правовые аспекты возникновения и развития института криптобанкинга в контексте использования цифровых активов (криптовалют)

Аннотация. Складывающиеся самостоятельные технологические тенденции по цифровизации в обществе – затрагивают достаточно большое количество общественных отношений в их числе экономические и гражданско-правовые аспекты правоотношений возникающих в сети «Интернет» при использовании цифровых активов (криптовалют) в определенных целях, в частности, как средство расчета, либо финансового инструмента в криптобанкинге. Феномен криптобанкинга и финансово-экономической деятельности последнего не имеет соответствующего гражданско-правового режима, исследован в науке юриспруденции достаточно слабо и неоднозначно, исходя из чего, автор настоящей научной статьи ставит перед собой основополагающую цель – тезисно разъяснить читателям и финансово-экономические свойства и гражданско-правовые основы режима криптобанкинга в Российской Федерации.

Ключевые слова: криптобанкинг, цифровые активы, криптовалюта, киберпреступность, цифровизация, цифровое право, гражданское право, стейблкоины, биткоины, цифровая среда.

В настоящее время отсутствует обширная научная литература на тему цифровых активов и деятельности криптобанкинов в условиях активного развития законодательства в системе российского права, что побуждает автора настоящей статьи осветить на теоретическом уровне, что представляет из себя феномен криптобанкинга.

Устоявшееся в научном обществе мнение о том, что зарождается и активно развивается новое направление в науке – отрасль «Цифровое право»[1], которое затрагивает широкую сферу правоотношений имеющих, как экономический, так и гражданско-правовой характер в «цифровой среде (сети Интернет)»[2].

Важнейшее место в складывающейся на сегодняшний день структуре такой отрасли играет – возникновение множественности различных межотраслевой институтов в основе которых использование цифровых активов (различных токенов: криптовалюты, NFT токены и т.д.). Одним из таких межотраслевых институтов цифрового права является – межотраслевой *институт криптобанкинга*, под которым понимается, что – это группа однородных и упорядоченных норм права регулируемых законом, в частности связанных с такими функциями как:

[1] Цифровое право: учебник / под общ. ред. Блажеева В. В., Егоровой М. А. М.: Проспект. 2021. С. 18-19.

[2] Примечание: автор настоящей статьи разъясняет, что «цифровая среда (сеть «Интернет»)» – это совокупность информационных технологий и (или) технологических устройств, используемых в материальном мире с альтернативной возможностью использования программного, технического взаимодействия в сети «Интернет».

- оборот цифровых активов;
- использование в качестве финансового инструмента.

Автор настоящей статьи отмечает, что достаточно очевидный факт формирования однородной группы отношений для возникающего института права – это наличие нормативно-правого акта (ов) регулирующего однородно возникающие правоотношения.

В рассматриваемом случае Российская Федерация[1] регулирует правоотношения неразрывно связанные с гражданско-правовым оборотом цифровых активов в цифровой среде (сети «Интернет») – федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ[2].

В продолжение данной темы, неоднократно отмечается автором настоящей статьи и другими современниками в сфере научных изысканий на тему цифровых правоотношений, что данный нормативно-правовой акт, безусловно, является историческим и системообразующим для системы права РФ в условиях цифровой трансформации общества, но, к большому сожалению не соответствующим правовой действительности, фактически являющийся «мертвым законом»[3].

Таким образом, все экономические процессы связанные с гражданско-правовым оборотом цифровых активов (в частности криптовалют) осуществляются в настоящее время в РФ на основании обычаев складывающихся в цифровой среде (сети «Интернет»), а также устанавливаемых владельцами (интернет ресурсов и цифровых финансовых платформ в различном формате, здесь же *криптобанкинг*) внутренних правил поведения, что предопределяет проблему для законодательной власти РФ на ближайшие годы.

Исходя из чего, автор настоящей статьи обращает внимание правоприменителей на особую значимость определяемого факта об регулировании возникающих правоотношений при использовании цифровых активов (криптовалюты) в цифровой среде (сети «Интернет»), в частности при обращении к сервисам криптобанкинга.

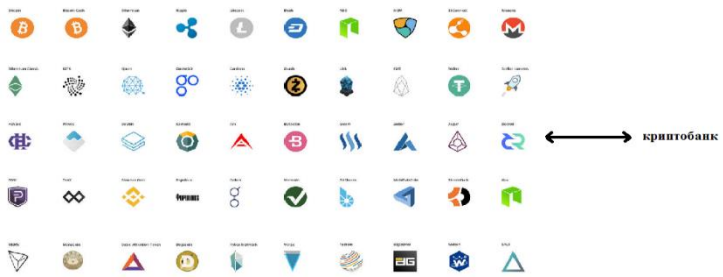


Рис. 1. Деятельность криптобанка с цифровыми активами (криптовалюты)

[1] Далее – РФ.

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // Собр. законодательства. 03.08.2020. № 31 (ч. 1). Ст. 5018.

[3] Примечание: нормы права, которые не работают.

Автор настоящей статьи, определив проблему, определив частные аспекты для правоприменителей, далее предлагает читателям вернуться от более практических аспектов к теоретическим.

Сущность данного межотраслевого института криптобанкинга и естественным образом быстро формирующихся подинститутов служит основополагающим и незаменимым фундаментом для развития цифровых правоотношений[1] в сфере криптобанкинга.

Криптобанкинг – это криптовалютно-кредитная деятельность организации в цифровой среде (сети «Интернет»)[2], которая регулирует платежный оборот цифровых активов в безналичной форме.

Криптобанк, как правило, предоставляет услуги по обороту (всем характерным для традиционных банков видам деятельности) большинства криптовалют, которые торгуются на лидирующих криптовалютных биржах. Активно в практике является эмитентом собственных цифровых активов (криптовалюты, которая может быть в форме видового ответвления – стейблкоинов[3]) используя их в качестве финансовых инструментов.

В последнее время в развитие отрасли криптобанкинга интегрированы десятки платежных систем в сферу цифровых правоотношений связанных с оборотом цифровых активов, среди множества платежных систем по всему миру – существуют и такие платежные системы как VISA, MasterCard и другие. Данный процесс предоставляет большие возможности для пользователей криптобанкинга по обороту цирфовых активов (криптовалют и иных) в повседневной жизни с использованием обычных платежных пластиковых кард с поддерживающими оборот цифровых активов – платежными системами.

Имея возможность по осуществлению операций в рамках популярных платежных систем, пользователь криптобанкинга получает достаточно обширную сферу для оборота цифровых активов в повседневной жизни, выводя криптовалюту в банки, далее в иные платежные системы регионального характера по своему усмотрению.

---

[1] Примечание: автор настоящей статьи разъясняет, что цифровые правоотношения –это гражданско-правовые отношения, которые осуществляются исключительно в цифровой среде (сети «Интернет).

[2] Зюзин Р.Г., Розалиев В.Л., Драгунов С.Е., Тюков А.П. Перспективы развития онлайн-платформ с помощью систем веб-аналитики // МНИЖ. 2017. №5-3 (59). URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-onlayn-platform-s-pomoschyu-sistem-veb-analitiki (дата обращения: 13.01.2021).

[3] Цифровой актив обеспеченный ценностями – рубль, юань, доллар, евро, золото, нефть и др.

Рис. 2. Оборот цифровых активов с использованием платежных систем международного уровня и федерального уровня

Основные признаки криптобанкинга:

- Коммерческая организация (как правило, имеет международную организационно-правовую структуру и статус);
- Создано для извлечения прибыли;
- Децентрализовано;
- Автоматизированные процессы заключения гражданско-правовых сделок (смарт-контракты);
- Стремится получиться разрешительную лицензию (в зависимости от расположения штаб-квартиры криптобанка);
- Наиболее часто разработан свой цифровой актив, с помощью которого осуществляются финансовые операции;
- Использование искусственного интеллекта;
- отсутствие третьей стороны (прямая связь криптобанка с пользователем).

Основные функции криптобанкинга, которые частично дублируют положения профильного законодательства в банковской деятельности[1]:

- Купля-продажа цифровых активов;
- Привлечение драгоценных металлов физических и юридических лиц во вклады;
- Транзакции по цифровым активам (переводы);
- Приобретение права требования от третьих лиц исполнения обязательств в форме цифровых активов;
- Открытие и ведение личных счетов пользователей;
- Обмен цифровых активов;
- хранение/ выдача цифровых активов;
- инвестиционные площадки в рамках криптобанкинга;
- вклады;
- криптобанкинговое обеспечение смарт-контрактов в коммерческой среде, которая, как правило, связана с осуществлением деятельности в сети-интернет;
- прямое инвестирование ICO - проектов;
- деятельность на рынке ценных бумаг.

[1] Федеральный закон от 02.12.1990 N 395-1 (ред. от 30.12.2020) «О банках и банковской деятельности», статья 5 // СПС Консультант Плюс (дата обращения 13.01.2021).

Достаточно подробное характеризующее описание криптобанкинга в сфере цифровых правоотношений указывает на глобальную трансформацию классической модели банковской деятельности. Добавляется достаточно большое количество преимуществ в отличие от традиционных банков:

- Отсутствие участия третьих лиц в операциях криптобанка;
- Автоматизированный процесс деятельности криптобанкинга (пример смарт-контракты);
- Более быстрые транзакции при обороте цифровых активов;
- Система безопасности постоянно модернизируется, дополнительным критерием защиты являются сами цифровые активы, это указывает на то, что криптобанкинг не уступает традиционным банкам;
- Интеграция с другими финансовыми площадками.

Во многом деятельность криптобанкинга, что следует из его функций и основных характеризующих признаков, достаточно сильно привязана к цифровым активам, как основополагающего и основообразующего элемента данной сферы цифровых правоотношений – это позволяет сделать вывод о том, что правовое регулирование данных областей правоотношений имеет достаточно однородную правовую природу – оборот цифровых активов.

В свою очередь оборот цифровых активов регламентирован основными правовыми положениями в профильном законе, а для отдельных видов деятельности, в частности деятельность криптобанкинга – в настоящее время не регламентирована законодательно.

Существующее законодательство в сфере финансового права, банковского права, гражданского права – указывает на межотраслевую правовую природу института криптобанкинга в цифровом праве.

По мнению автора, в сущность признания научным обществом новой сформировавшейся отрасли цифрового права – вкладывается типовой формат принятия действительности, как следствие – только отдельные институты цифрового права находят свое теоретическое закрепление и подтверждение, а иные институты данной отрасли существуют в «формальном» подходе при исследовании тематики цифровых активов и криптобанкинга.

Промежуточный итог такой действительности указывает на замедление темпов развития цифрового права в системе российского законодательства, что повлечет негативные финансовые, политические и экономические последствия в последующем для государства в секторе криптобанкинга.

Вывод, связанный с развитием цифровых правоотношений в сфере криптобанкинга неоднозначен. Присутствие законодательного регулирования оборота цифровых активов и признания их статуса указывает на комплексно сформировавшуюся отрасль права с различными межотраслевыми институтами, которые необходимо регулировать в рамках правового поля. Потребительский спрос пользователей цифрового оборота растет, как следствие - возрастает количество предложений по оказанию услуг в сфере криптобанкинга. Вопрос качества оказания услуг связанных с оборотом цифровых активов остается в настоящее время под большим вопросом из-за отсутствия органичного и сбалансированного национального законодательства, которое должно в лице

государства защищать, обеспечивать и регулировать гражданско-правовые процессы, которые возникают в сети-интернет.

Острая необходимость в гражданско-правовом регулировании данной сферы правоотношений - однозначно требуется в силу национального законодательства, предписывающего строгий порядок ведения финансово-кредитной деятельности на территории России, на основании чего разумным шагом для законодательной власти станет принятие в ряд федеральных законов дополнений касающихся сферы криптобанкинга и правоотношений складывающихся в данной сфере.

Литература

1. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // Собр. законодательства. 03.08.2020. № 31 (ч. 1). Ст. 5018.
2. Федеральный закон от 02.12.1990 «395-1 (ред. от 30.12.2020) «О банках и банковской деятельности», статья 5 // СПС Консультант Плюс
3. Зюзин Р.Г., Розалиев В.Л., Драгунов С.Е., Тюков А.П. Перспективы развития онлайн-платформ с помощью систем веб-аналитики // МНИЖ. 2017. №5-3 (59). URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-onlayn-platform-s-pomoschyu-sistem-veb-analitiki (дата обращения: 13.01.2021).
4. Цифровое право: учебник / под общ. ред. Блажеева В. В., Егоровой М. А. М.: Проспект. 2021. С. 18-19.

А.А. Холмогорова
Научный руководитель: **Скуковский А.Г.**

Использование информационно-телекоммуникационных систем при совершении криминальных взрывов и современные возможности экспертного исследования в сети «Интернет» при расследовании криминальных взрывов

Аннотация. В данной статье рассматриваются возможности использования данных из открытых источников при расследовании преступлений, совершенных и использованием взрывчатых веществ и взрывных устройств, также изучены информационные следы, которые могут быть оставлены преступниками при совершении и подготовке криминальных взрывов.

Ключевые слова: террористический акт, самодельные взрывные устройства, цифровые следы, информационно-телекоммуникационные системы, облачные данные.

Использование информационно-телекоммуникационных систем при совершении криминальных взрывов и современные возможности экспертного исследования в сети «Интернет» при расследовании криминальных взрывов.

По причине того, что в нашей стране на современном этапе широко распространены информационно-коммуникационные технологии, происходит изменение характера преступности. Сейчас увеличивается количество преступлений, совершаемых через различные информационно-телекоммуникационные сети.

Наше общество находится в постоянном динамическом развитии. Чтобы значительно облегчить жизнь человека на помощь приходят новейшие технологические разработки. И, напротив, в момент появления данных достижений, они зачастую используются для того, чтобы с их помощью упростить протекание незаконной деятельности преступников. В современное время в открытом доступе в сети «Интернет» в открытых источниках (социальные сети, открытые базы, реестры и др.) представлено много информации, это огромная база данных, в которых можно найти информацию практически про всех граждан Российской Федерации и других стран. Если собрать все открытые данные, то можно составить портрет человека, узнать, чем он увлекается, где работает. Также существует сеть «Tor», в которой в открытом доступе работают анонимные сайты, на которых в может быть расположена информация, запрещенная к распространению на территории Российской Федерации, в том числе, информация террористического характера. Из открытых источников можно узнать следующую информацию о человеке, в том числе, террористе: профиль поведения, интересы, геолокации, уровень дохода, связи между людьми, уровень информационного влияния. В процессе расследования преступления террористического характера, в частности, криминальных взрывов, в границах осмотра места происшествия и возможных путях подхода террористов-смертников, путях отхода (при закладывании «ловушек», мин) устанавливается наличие и проводится анализ записей с камер видеонаблюдения. В ходе осмотра видеозаписи в рамках видеотехнической судебной экспертизы экспертом, осмотра трупа или осмотра предметов следователем можно распознать лица в социальных сетях, проанализировать личность лица, подготовившего криминальный взрыв или непосредственного исполнителя, найти возможных соучастников, установить другие обстоятельства уголовного дела.

В таких ситуациях возникает вопрос: в какое экспертное учреждение обратиться за консультационной помощью или экспертным исследованием и анализом данных из открытых источников (так называемые «Big DATA»)?

В настоящее время в Российской Федерации существует компания Tazeros Global System (ex Social Data Hub), которая по нескольким фотографиям может создать трехмерную модель человека по фотографиям, в распоряжении компании одна из самых масштабных баз данных из открытых источников с помощью которой устанавливается информация о личности преступника (в том числе, хранится историческая копия информации из социальных сетей, так, компанией установлено, что Акбар Джалилов за три дня до совершения террористического акта в петербургском метро удалил аккаунт в социальной

сети «ВКонтакте», по историческим связям и общим группам найдены еще три аккаунта террориста[1]).

Следователи Следственного комитета при расследовании таких преступлений могут направить запрос в данную организацию (ООО «ТАЗЭРОС»), в течение 5 дней будет подготовлен ответ на запрос[2]. Таким образом можно оперативно получить информацию следующего характера: точную геопозицию пользователя перед совершением преступления (данная информация позволит установить место покупки составляющих частей самодельного взрывного устройства; возможных свидетелей; лиц, которые не сообщили в правоохранительные органы о подготавливаемом террористическом акте), данные о публичном профиле в социальных сетях (для последующего анализа полученной на основании судебного решения переписки в социальной сети), данные о подключениях (IP адрес, Версия клиента, Сессия, MAC адреса), уникальная цифровая подпись встроенного браузера телефона (Fingerprint ID, извлекаемые паттерны взаимодействия с интерфейсом, включающие все касания экрана, набор текста и переходы по экранам (для установления обстоятельств по инициировании взрыва при помощи кодирования самодельного взрывного устройства в сети «Интернет» и обстоятельств подготовки к совершению взрыва, например, поиск преступником информации об изготовлении детонатора).

Однако, указанная компания не является экспертным учреждением и результаты, полученные по запросу в данной организации, обладают ориентирующим характером при расследовании криминальных взрывов, способствуют установлению доказательств, подтверждающих причастность лица к совершению преступления. Придать вид доказательственной информации и получить подробные данные позволит назначение следователем компьютерно-технической экспертизы в ФГКУ «Судебно-экспертный центр Следственного комитета Российской Федерации».

В настоящее время возможно применение системы «Интернет» для кодирования самодельных взрывных устройств. Также новые технические возможности делают доступным управление производственными объектами, и машинами с помощью обычного смартфона, обладают встроенными модулями передачи данных. Следует привести пример, как в 2015 году в США программисты взломали электронную систему бортового компьютера автомобиля Jeep Cherokee и удаленно смогли управлять всеми системами автомобиля, внедряя новый год в программу движения автомобиля. Практически у каждого гражданина в сети «Интернет» хранится информация, в которых хранятся новые цифровые следы - «облачные данные» – данные, хранящиеся на внешних устройствах, сервисах, хранилищах, серверах (то есть «в облаке»), которые непосредственно связаны с мобильным устройством или компьютером путем специфичных идентификационных данных, таких как: данные аккаунта (логин, пароль), токен авторизации, электронный сертификат. Обмен данными между мобильным устройством и «облаком» происходит посредством

[1] Официальный сайт компании Tazeros Global Systems// URL: https://tazeros.com/info.
[2] Официальный сайт компании Tazeros Global Systems// URL: https://tazeros.com/info.

коммуникационных информационных сетей, наиболее распространенной из которых является сеть «Интернет»[1].

Мы не можем исключать использование террористами информационных технологий, в связи с чем, установление данных из облачных хранилищ позволяет установить обстоятельства, подлежащие доказыванию по уголовным делам о преступлениях, совершенных и использованием взрывчатых веществ и взрывных устройств. В настоящее время преступники могут использовать возможности информационно-телекоммуникационных сетей не только при инициировании взрыва, но и при подготовке к нему. Как ранее упоминалось, в сети «Интернет» существует достаточное количество открытых сайтов, «Телеграмм-каналов», анонимных сайтов в закрытой сети «Tor», на которых может быть представлена информация об изготовлении самодельных взрывных устройств. Так, Главным Следственным управлением Следственного комитета России расследовалось уголовное дело, по которому 18 летний гражданин из Тамбовской области -посредством сети «Интернет», с использованием мессенджеров изучил литературу по изготовлению самодельных взрывных устройств, изготавливал взрывные устройства, подготавливался в совершении взрыва в общежитии в Тамбовской области. Его деятельность пресечена, он не довел преступный умысел до конца, сотрудниками правоохранительных органов предотвращен террористический акт.

В Главном управлении криминалистики Следственного комитета Российской Федерации (Криминалистическом центре) проанализирована практика получения следственными органами информации, хранящейся в мессенджерах, информационно-телекоммуникационной сети «Интернет», сведений из открытых источников, по результатам которого выявлено, что при выдвижении версий и проверки их следственным путем, получении информации о потерпевшем или свидетелях, причастных к совершению преступления лицах, установлению обстоятельств, подлежащих доказыванию имеет значение получение доступа к закрытым аккаунтам в соцсетях и облачным хранилищам информации[2].

В практике следственных органов Следственного комитета России наиболее распространен поиск данных из открытых источников путем осмотра предметов - Интернет ресурса. Необходимо отметить, что такой осмотр целесообразнее проводить с участием специалистов, обладающих высокими познаниями в области информационной безопасности и занимающихся изучением данных из открытых источников, например, сотрудников организации ООО «ТАЗЭРОС» или привлечением инспектора или следователя-криминалиста отдела криминалистического сопровождения следствия Главного управления

[1] А.В. Гончаров. Использование возможностей современных инновационных технологий при исследовании цифровых устройств мобильной связи и компьютерных носителей информации при расследовании преступлений// Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: материалы Международной научно-практической конференции (Москва, 17 октября 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 188.

[2]Вестник Главного управления криминалистики. 2021. № 1. С. 19.

криминалистики Следственного комитета России. Это необходимо делать в связи с тем, что в системе Следственного комитета формируются внутренние базы данных криминалистически значимой информации на основе сведений из открытых источников - из Интернета, мессенджеров, облачных хранилищ, в том числе при осуществлении криминалистического сопровождения следствия по делам террористической направленности.

В большей степени, это используется в регионах, где чаще совершаются преступления террористического характера, преимущественно, в Северо-Кавказском регионе. Например, в СУ по Республике Северная Осетия-Алания существует криминалистическая база данных, содержащая сведения из аккаунтов, удостоверения личности, учетные записи, имена пользователей[1].

Председателем Следственного комитета Российской Федерации распоряжением от 10.06.2013 №69/108р «О введении в действие интегрированной базы данных по учету преступлений экстремистской и террористической направленности на территории Северо-Кавказского и Южного федеральных округов» в этих регионах заполняется учетная карточка на все преступления террористической направленности и несовершеннолетних, заполняются сведения об абонентских номерах и IMEI мобильных устройств обвиняемых. Представленные сведения вносятся в базу данных ПК «Легенда» (СК) и обрабатывается ГСУ по Северо-Кавказскому федеральному округу[2].

Таким образом, эффективность расследования криминальных взрывов в современных условия напрямую зависит от возможностей правоохранительных органов по возможному обнаружению цифровых следов преступников. Расследование преступлений террористического характера имеет особую сложность. Необходимым является созданием в системе Главного управления криминалистики (криминалистического центра) Следственного комитета структурного подразделения, в котором будут работать специалисты, проводящие анализ и сбор данных из открытых источников, будут грамотно разрабатывать и создавать базы с использованием компьютерных средств и информационно-телекоммуникационных систем баз данных криминалистически значимой информации.

Литература

1. Вестник Главного управления криминалистики. 2021. № 1. 54 с.
2. А.В. Гончаров. Использование возможностей современных инновационных технологий при исследовании цифровых устройств мобильной связи и компьютерных носителей информации при расследовании преступлений//Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: материалы Международной научно-практической конференции (Москва, 17 октября 2019 года) / под общ. ред.

[1] Вестник Главного управления криминалистики. 2021. № 1. С. 30.
[2] Вестник Главного управления криминалистики. 2021. № 1. С. 30.

А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 188.
3. Официальный сайт Следственного комитета Российской Федерации// URL: https://sledcom.ru/news/item/1633876/.
4. Официальный сайт компании Tazeros Global System// URL: https://tazeros.com/info.
5. Официальный сайт международной компании «Лаборатория Касперского» // URL: https://www.kaspersky.ru/blog/remote-car-hack/8430/.

Сведения об авторах

Аверьянов Виталий Сергеевич – аспирант ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева».

Баркалова Елена Владимировна − доцент кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического Института (филиала) Университета прокуратуры РФ, кандидат юридических наук.

Белодед Диана Роландовна − аспирант КГУ им. К. Э. Циолковского.

Белых-Силаев Дмитрий Владимирович – старший научный сотрудник Всероссийского научно-исследовательского института МВД России (ВНИИ МВД России).

Боков Сергей Никанорович – доцент кафедры криминалистики юридического факультета ФГБОУ ВО «Воронежский государственный университет», кандидат медицинских наук, доцент по кафедре общей и юридической психологии.

Голоскоков Леонид Викторович – ведущий научный сотрудник научно-исследовательского отдела факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.

Гончаров Дмитрий Константинович – старший оперуполномоченный отдела экономической безопасности и противодействия коррупции Управления МВД России по г. Керчи, майор полиции.

Грицианова Кристина Петровна − курсант 305 учебной группы, факультета подготовки следователей Волгоградской академии МВД России, Федеральное государственное казенное образовательное учреждение высшего образования «Волгоградская академия Министерства внутренних дел Российской Федерации», рядовой полиции.

Даценко Кристина Олеговна – студент 5 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Деулин Дмитрий Владимирович – ведущий научный сотрудник Всероссийского научно-исследовательского института МВД России (ВНИИ МВД России), кандидат психологических наук, доцент.

Жданов Максим Игоревич − психолог группы морально-психологического обеспечения отдела кадров Управления вневедомственной охраны по г. Воронежу – филиал ФГКУ «УВО ВНГ России по Воронежской области», лейтенант полиции.

Житков Алексей Анатольевич – старший преподаватель кафедры уголовного права и криминологии юридического факультета ВИПЭ ФСИН России.

Жукова Полина Николаевна − доктор физико-математических наук, доцент.

Зобнин Павел Андреевич – старший следователь следственного отдела по Ленинскому административному округу г. Тюмень следственного управления Следственного комитета Российской Федерации по Тюменской области, старший лейтенант юстиции, аспирант кафедры уголовно-

правовых дисциплин Института государства и права Тюменского государственного университета.

Золотухина Наталья Валерьевна − доцент кафедры уголовного процесса Военного университета Министерства обороны Российской Федерации, кандидат юридических наук.

Зыков Илья Александрович − аспирант кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации.

Илларионова Евгения Алексеевна − магистрант 1 курса программы «Юрист в сфере уголовного судопроизводства» Санкт-Петербургского государственного университета юридического факультета.

Казаков Александр Алексеевич – магистрант 2 курса факультета подготовки криминалистов ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Кардашевская Марина Владимировна − профессор кафедры предварительного расследования Московской академии СК России, доктор юридических наук, профессор.

Климято Павел Викторович – старший преподаватель кафедры организации предварительного расследования учреждения образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь», подполковник юстиции.

Кобец Петр Николаевич − главный научный сотрудник Центра организационного обеспечения научной деятельности Всероссийского научно-исследовательского института Министерства внутренних дел Российской Федерации г. Москва, доктор юридических наук, профессор, Почетный сотрудник МВД России, полковник полиции.

Костенко Константин Анатольевич − заведующий кафедрой уголовного права, криминологии и уголовного процесса Хабаровского филиала Московской академии Следственного комитета Российской Федерации, полковник юстиции.

Королева Любовь Евгеньевна − обучающаяся 2 курса факультета подготовки криминалистов Московской академии Следственного комитета Российской Федерации.

Купцова Юлия Ильинична – ассистент кафедры информационных технологий и организации расследования киберпреступлений ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Кузина Валерия Гдалиевна – студент 5 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Ламыкина Софья Олеговна - студент 5 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Левашова Полина Денисовна – слушатель 171 учебного взвода Московского областного филиала Московского университета МВД России имени В. Я. Кикотя, младший лейтенант полиции.

Магомедов Ахмед Арипович – обучающийся 2 курса факультета подготовки криминалистов ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Малик Владислав Игоревич – адъюнкт кафедры оперативно-разыскной деятельности ОВД Орловского юридического института МВД России имени В.В. Лукьянова, старший лейтенант полиции.

Мироненкова Полина Олеговна – студентка 3 курса факультета подготовки следователей Санкт-Петербургской академии Следственного комитета Российской Федерации.

Морар Виталий Олегович – ведущий научный сотрудник ФГКУ «ВНИИ МВД России», кандидат юридических наук, подполковник полиции.

Мухтарова Елена Анатольевна – заместитель начальника кафедры гражданско-правовых дисциплин Вологодского института права и экономики ФСИН России.

Нестерович Сергей Александрович – доцент кафедры информационных технологий и организации расследования киберпреступлений ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации, полковник юстиции.

Озеров Игорь Николаевич − заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного Комитета Российской Федерации, кандидат юридических наук, доцент, полковник юстиции.

Орлова Мария Сергеевна – адъюнкт 1 курса факультета подготовки научно-педагогических и научных кадров Московского университета МВД России имени В.Я. Кикотя, лейтенант полиции.

Пантелеева Анастасия Олеговна - студент 5 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Рахимов Артем Ибрагимович – аспирант Московской академии Следственного комитета Российской Федерации, старший специалист отдела криминалистики следственного управления Следственного комитета Российской Федерации по Самарской области, подполковник юстиции.

Рудаков Артур Михайлович – научный сотрудник организационно-научного отдела майор внутренней службы.

Савченко Майя Михайловна − доцент кафедры «Экономическая безопасность» ФБГОУ ВПО Калининградского государственного технического университета, кандидат экономических наук, доцент.

Сайфуллина Мария Ивановна − студентка 1 курса магистратуры Юридического института РУДН.

Санташов Андрей Леонидович – главный научный сотрудник (по социологическим исследованиям) научно-исследовательского отдела факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы, доктор юридических наук, доцент.

Сарыгина Элина Сергеевна − доцент кафедры судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного

Комитета Российской Федерации, кандидат юридических наук, лейтенант юстиции.

Серова Елена Борисовна − заведующий кафедрой уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

Смирнов Александр Михайлович − главный научный сотрудник АУС ФКУ НИИ ФСИН России, профессор кафедры уголовно-правовых дисциплин Международного юридического института, доктор юридических наук, доцент.

Смолин Михаил Сергеевич − следователь-криминалист следственного управления Следственного комитета Российской Федерации по Челябинской области, полковник юстиции.

Собина Юрий Юрьевич – аспирант кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации.

Танцюра Виктор Сергеевич – аспирант кафедры уголовного права и криминологии ФГБОУ ВО «Ярославский государственный университет им П.Г. Демидова».

Терехов Максим Геннадьевич – соискатель кафедры гражданского и трудового права, гражданского процесса Московского университета МВД России имени В.Я. Кикотя.

Холмогорова Анастасия Александровна, – студент 5 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Хомяков Эдуард Геннадьевич – доцент кафедры криминалистики и судебных экспертиз Удмуртского государственного университета, Заслуженный юрист Удмуртской Республики, кандидат юридических наук, доцент, полковник полиции в отставке.

Содержание

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ И ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Материалы международной научно-практической конференции

(Санкт-Петербург-Москва, 2-3 декабря 2021 года)

Подписано в печать 01.02.2022

Формат 60х90 1/16
Усл. печ. л. 12,56
Тираж 100 экз.
Печать офсетная
Заказ № 334

_____

Отпечатано в типографии Московской академии
Следственного комитета Российской Федерации,
ул. Врубеля, д. 12