Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ТЕОРИЯ И ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Материалы заочной Международной научно-практической конференции
(Минск, 12 декабря 2022 г.)

Минск
Академия МВД
2023

УДК 343.985.7 + 004:34 + 343.534
ББК 67.52 + 67.408
Т11

ISBN 978-985-576-400-8

УДК 343.98

А.В. Балиткин

АКТУАЛЬНЫЕ АСПЕКТЫ ВЗАИМОДЕЙСТВИЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ С БАНКАМИ И НЕБАНКОВСКИМИ КРЕДИТНО-ФИНАНСОВЫМИ ОРГАНИЗАЦИЯМИ ПРИ ПРОТИВОДЕЙСТВИИ СБЫТУ НАРКОТИКОВ В СЕТИ ИНТЕРНЕТ

Распространение наркопотребления представляет собой угрозу нормальному функционированию любого государства. В Республике Беларусь, как и во всем мире, сбыт наркотических средств, психотропных веществ и их аналогов (далее – наркотики) часто осуществляется организованными группами, в том числе транснационального характера. Учитывая тот факт, что сбыт наркотиков в первую очередь направлен на обогащение, а деятельность преступных организаций обусловливается конъюнктурой рынка наркосбыта, то и противодействие целесообразно осуществлять в совокупности как оперативно-розыскными, так и финансовыми инструментами заинтересованных субъектов, в том числе в информационном пространстве.

Статья 13 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» определяется содержание взаимодействия между органами, осуществляющими оперативно-розыскную деятельность, иными организациями и специальными службами иностранных государств, что предопределяет значимость совместных действий для противодействия преступности. В части противодействия наркопреступности представляется наиболее актуальным направлением взаимодействие, связанное с пресечением фактов легализации доходов, полученных от сбыта наркотиков, а также с нейтрализацией таких возможностей вовсе, что возможно в ходе взаимодействия оперативных подразделений органов внутренних дел с банками и небанковскими кредитно-финансовыми организациями (НКФО).

Анализ правового регулирования позволяет сделать вывод о наличии системы контроля над совершением операций, сопряженных с возможной легализацией доходов, полученных преступным путем, на национальном и наднациональном уровнях. В частности, Законом Республики Беларусь от 30 июня 2014 г. № 165-З «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения» определены правовые и организационные основы государственной политики в сфере предотвращения легализации доходов, полученных преступным путем. В соответствии с постановлением Совета Министров Республики Беларусь от 24 декабря 2014 г. № 1249 «Об установлении общих требований к правилам внутреннего контроля» такие правила определяются лицами, осуществляющими финансовые операции, с учетом общих требований к правилам внутреннего контроля, в том числе определяемых государственными органами, контролирующими деятельность по осуществлению финансовых операций. Таким образом, законодательно выстроена система внутреннего контроля в банках и НКФО, однако на практике возникают проблемные аспекты, обусловленные нормативным закреплением лишь общих требований к организации внутреннего банковского контроля. В свою очередь, за банками сохраняется право самостоятельно определять критерии риска банковской услуги (продукта) и риска работы с клиентом. Эти критерии разнятся в зависимости от банка и дают возможность толковать риск произвольно, что не позволяет эффективно противодействовать легализации доходов, полученных от незаконного сбыта наркотиков. Решением проблемы станет разработка единообразных критериев отнесения операций к потенциально связанным с легализацией такого дохода на основании общих закономерностей, присущих бесконтактному сбыту наркотиков (однотипные финансовые операции, связанные с фиксированным размером переводов денежных средств от разных лиц, а также эквивалентные стоимости разового объема наркотика в незаконном обороте на день совершения операции и т. п.), так как основным способом противодействия легализации средств, полученных преступным путем, представляется выделение в общей массе финансовых операций подозрительных сделок и раскрытие их экономической сущности.

При этом представляется, что эффективному противодействию легализации доходов, полученных от незаконного сбыта наркотиков, будет способствовать оперативный обмен финансовой информацией, который должен осуществляться свободно с использованием современных информационно-коммуникативных технологий между правоохранительными, регулирующими, надзорными и другими компетентными органами.

УДК 343.9.01

Р.А. Белевский

НЕКОТОРЫЕ АСПЕКТЫ И ТЕНДЕНЦИИ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ

Слово «киберпреступление» может быть интерпретировано на основе слова «кибернетика», которое в 1960-е гг. считалось обозначением чего-то передового, связанного с компьютерами, а «кибер» употребляли как приставку к различным словам; с начала 1990-х гг. понятие «кибернетика» метафорично применялось к преступлениям, связанным с компьютерами и интернетом.

Однако в российском правовом (законодательном) поле иностранные метафоры на основе приставки «кибер» не используются.

Хотя Н. Винер считал, что он первым стал употреблять слово «кибернетика», однако этот термин в 1834 г. использовал физик Ампер для обозначения науки об управлении общественными системами, а в 1843 г. польский ученый Ф. Трентовский издал в Познани книгу, которая называлась «Отношение философии к кибернетике как искусству управления народом».

Подчеркнем, что обозначать виртуальный мир как киберпространство нельзя, так как понятие пространства обозначает свойство мира, поля, среды, а не само поле, в том числе и виртуальное. Не надо представлять себе поле как площадку – виртуальное поле может быть многомерным. Если и использовать понятие «пространство», то в значении интернет-пространства (интернет-территории), т. е. как юридический термин, обозначающий наличие национальной юрисдикции на некоторой территории. Однако лучше пользоваться выражением «сфера пространства виртуального мира».

С инфраструктурной точки зрения понятие «интернет-пространство» необходимо рассматривать как глобальное адресное пространство, которое состоит из региональных и (или) национальных сегментов интернета.

Считается, что первое преступление с помощью компьютера в мире было совершено в США в 1960-х гг. Криминологическое определение компьютерного инцидента появилось в 1983 г. Под ним понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных. В СССР первое преступление с помощью ЭВМ «Онега» было совершено программистом в 1979 г. в городе Вильнюсе.

В настоящее время появляются преступники, которые не обладают специальными знаниями, а используют готовые, понятные программ-

ные инструменты. Они, как правило, очень молоды, большинству нет 30 лет. Программы, которыми они пользуются, предельно просты и могут иметь лицензионную политику, а создающие их злоумышленники тратят время на борьбу с пиратством и на защиту своей собственности. Эти сайты предлагают круглосуточную техподдержку на нескольких языках, которой могут позавидовать некоторые производители программного обеспечения.

Словом «хакер» (взломщик) обозначают человека, который способен, используя электронные устройства как инструменты, получить доступ к защищаемым от несанкционированного доступа данным, содержимое которых в виде информации может быть его целью. Поэтому хакеров разделяют:

на «черных» хакеров (хакеров-злоумышленников);

«белых» хакеров, которые проникают в искомую систему без злого умысла;

условных хакеров-программистов, которые должны тестировать систему на предмет выявления в ней уязвимостей.

В определенных случаях программисты могут стать хакерами или, наоборот, хакеры могут работать как условные хакеры. Естественно, все программные инструменты продуцируются самостоятельно программистами и являются нейтральными, но их можно использовать в хакерских целях.

Таким образом, высокотехнологичные преступления в виртуальной сфере подразумевают, что злоумышленники могут пользоваться рынком криминальных программных инструментов. Хакеры объединяются в международные группы и совершают атаки на компьютеры, расположенные в других странах. Поэтому полицейские считают, что для ликвидации незаконных рынков хакерских инструментов, незаконного обналичивания денег требуется объединение усилий полиции для противодействия хакерам из разных государств. Безусловно, необходима Конвенция по борьбе с компьютерными преступлениями на базе ООН, а не только аналогичная конвенция Совета Европы.

Конвенция Совета Европы о киберпреступности выделяет четыре типа компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

незаконный доступ – противоправный умышленный доступ к компьютерной системе либо ее части (ст. 2);

незаконный перехват – противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах (ст. 3);

вмешательство в данные – противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных (ст. 4);

вмешательство в систему – серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных (ст. 5).

Однако современные преступления в виртуальной сфере стали значительно более разнообразными. Считается, что существует примерно 100 векторов возможных хакерских атак, хотя наиболее известна следующая типизация компьютерных инцидентов:

вредоносное программное обеспечение;

DDoS-атаки;

мошеннические SMS и звонки;

несанкционированный доступ к конфиденциальной информации.

Тремя основными причинами взлома данных являются:

внешняя хакерская атака – 24,6 %;

сбой системы безопасности и внутренние уязвимости – 19,5 %;

человеческий фактор – 18,7 %.

Если вести речь о современных трендах развития преступлений в виртуальной сфере, необходимо отметить, что, согласно докладу о глобальных рисках Всемирного экономического форума, подавляющее большинство экспертов ожидают повышения частоты кибератак, ведущих к краже денег и данных (82 %) и срыву операций (80 %). К 2022 г. к интернету будет подключен один триллион устройств. К 2023 г. у 80 % людей появится аватар в цифровом мире. При этом более 50 % интернет-трафика в 2024 г. будут потреблять «умные» устройства. Ожидается развитие Deepfakes систем для продуцирования правдоподобных сообщений и заявлений, которые смогут воздействовать не только на сознание, но и подсознание людей.

Таким образом, одной из причин ускоренного роста киберпреступности являются технологические тренды. Ожидается использование искусственного интеллекта (ИИ) для борьбы с киберпреступностью. По мере того как организации переходят от центра обработки данных к облачным платформам, использование технологий на основе ИИ будет продолжать расти и получать более широкое распространение. Развитие фейковых видео- и аудироликов, изображений также создает высокий риск быть обманутым. Телефонные боты научатся имитировать знакомый голос человека, который может отдать приказ.

УДК 343.915

В.А. Беспалов

КРИМИНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ЛИЧНОСТИ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЮЩИХ КИБЕРПРЕСТУПЛЕНИЯ

Технологии являются неотъемлемой частью современной жизни человека. Достижения науки и техники открыли множество возможностей для взрослых и детей, улучшая и облегчая жизнь во многих сферах жизнедеятельности. В то же время развитие технологий является не только благом, но и влечет явные угрозы безопасности. Одним из приоритетных направлений государственной политики является обеспечение информационной безопасности, что напрямую связано с использованием информационных технологий. Часто преступления, связанные с использованием компьютерных технологий, совершаются несовершеннолетними.

Таким образом, развитие сферы компьютерных технологий имеет не только положительные, но и негативные последствия, о чем свидетельствует динамика количества преступлений, совершенных несовершеннолетними в сфере киберпреступности. Самым распространенным преступлением, совершаемым несовершеннолетними в данной сфере, является хищение имущества путем модификации компьютерной информации, предусмотренное ст. 212 Уголовного кодекса Республики Беларусь (УК). За период с 2017 по 2021 г. несовершеннолетними совершено 539 таких преступлений. Из них в 2017 г. зарегистрировано 53 преступления, в 2018 г. – 60, в 2019 г. – 144, в 2020 г. – 210, в 2021 г. – 72.

За последние пять лет несовершеннолетними совершено 98 преступлений против компьютерной безопасности, предусмотренных гл. 31 УК. В 2017 г. было зарегистрировано 67 таких преступлений, в 2018 г. – 5, в 2019 г. – 11, в 2020 г. – 12, в 2021 г. – 3.

Несмотря на отсутствие поступательности в динамике киберпреступлений, совершаемых несовершеннолетними, а также на незначительное их количество по отдельным составам в абсолютном выражении, удельный вес таких преступлений в структуре преступности несовершеннолетних остается достаточно высоким.

Субъектом преступлений, предусмотренных гл. 31 УК, может быть вменяемое физическое лицо, достигшее шестнадцатилетнего возраста. За преступление, предусмотренное ст. 212 УК, уголовная ответственность наступает с четырнадцати лет. Такой критерий субъекта, как

возраст, говорит о том, что лицо на момент совершения преступления достигло такого уровня развития, который достаточен для адекватного восприятия характера своих действий и их запрещенности. Как показывает опыт изучения личности несовершеннолетних киберпреступников, субъектом указанных выше преступлений чаще всего являются лица, не имеющие соответствующего образования либо опыта работы в информационной сфере, однако они имеют специальные знания относительно программного обеспечения и владеют некоторыми навыками программирования.

Примечательно, что уровень знаний компьютерных технологий, а также владения компьютерной сетью Интернет отдельными несовершеннолетними уже давно превосходит знания, предусмотренные школьной программой либо программами начальных курсов высших учебных заведений, что позволяет им не только самостоятельно использовать технологии, но и совершать киберпреступления. Таким образом, фундаментом будущей криминальной деятельности является самостоятельное освоение несовершеннолетними информационных технологий.

К наиболее распространенным противоправным действиям несовершеннолетних в сфере киберпреступности относятся следующие: «взлом» страниц в различных социальных сетях; получение незаконного доступа к охраняемой законом информации; совершение кибератак; создание, использование и распространение вредоносных программ; получение несанкционированного доступа к различным игровым ресурсам; осуществление кибертравли; незаконное использование банковских платежных карточек членов семьи или других лиц.

По нашему мнению, можно выделить четыре основные категории несовершеннолетних киберпреступников.

Во-первых, лица, которые, только освоив информационные технологии, хотят проверить свои знания и мастерство или продемонстрировать свои умения. Совершая противоправные поступки, подростки завоевывают внимание сверстников и полагают, что их будут уважать за то, что они умеют это делать. Такие молодые люди обычно совершают преступления, используя несложные методы и примитивные вредоносные программы.

Во-вторых, талантливые молодые люди, которые приобрели достаточно глубокие знания и определенный опыт в области информационных технологий. Они могут создавать довольно опасные компьютерные вирусы, придумывать новые способы заражения компьютеров, а также противодействовать антивирусным программам. Как правило, целью таких преступников является обнаружение инновационных способов проникновения в информационные системы или иных уязвимостей. Они могут не распространять свои программы, но активно продвигают свои

идеи через интернет-ресурсы, посвященные созданию вредоносных программ. Затем такие идеи могут быть использованы другими.

В-третьих, несовершеннолетние, вовлеченные в преступление взрослыми. В таких преступлениях несовершеннолетний может быть как непосредственным исполнителем, так и другим соучастником совершения преступления, например, путем сбора какой-либо информации, разработки вредоносного программного обеспечения или предоставления других средств преступнику.

В-четвертых, лица, чья основная задача – получение незаконной финансовой прибыли. Несовершеннолетние с использованием найденной или украденной банковской платежной карточки, либо с использованием незаконно полученных реквизитов банковской платежной карточки осуществляют снятие денег в банкомате, оплачивают покупки в торговых точках в интернет-магазинах, расплачиваются в онлайн-играх за дополнительные бонусы, уникальные предметы и другие преимущества. Они активируют финансовые услуги, предоставляемые мобильными операторами, на мобильном телефоне другого человека и переводят деньги, предоставленные компанией в качестве займа, на свой абонентский номер телефона.

Несовершеннолетние, являющиеся субъектом того или иного киберпреступления, как правило, не имеют криминального прошлого и часто совершают преступления из-за незнания закона, например, когда подросток не осознает, что «взлом» страницы в социальных сетях или несанкционированный доступ к игровым ресурсам является противоправным деянием и влечет за собой уголовную ответственность.

Таким образом, в связи с тем, что киберпреступления стали совершаться не только людьми, обладающими специальными знаниями в этой области, но и несовершеннолетними, возрастает актуальность борьбы с преступлениями данного вида. Одним из направлений борьбы с преступлениями, совершаемыми несовершеннолетними в сфере киберпреступности, является совершенствование норм УК.

Представляется, что эффективным способом воздействия на несовершеннолетних, совершающих преступления с использованием компьютерных технологий, будет являться закрепление в УК положений, которые позволят ограничивать доступ таких несовершеннолетних к компьютерной технике, определенным информационным порталам и интернет-ресурсам, устанавливать программы дистанционного контроля за телефонными соединениями и интернет-трафиком. Такие положения, по нашему мнению, должны быть включены в п. 4 ч. 1 ст. 117 УК и дополнить перечень форм ограничения свободы досуга несовершеннолетнего.

УДК 519.876

Н.М. Бобович

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Основными задачами исследования путей повышения устойчивости функционирования критически важных объектов информатизации (КВОИ) является: выявление всех возможных способов и средств снижения потерь и сохранения работоспособности (производительности) КВОИ, оценка их эффективности и разработка рекомендаций по практическому использованию с учетом конкретных условий размещения и деятельности КВОИ и его структурных подразделений.

Совокупность всех возможных путей (способов, мероприятий), принципиально способных изменять устойчивость функционирования, будем называть областью управления устойчивостью функционирования. Систему мероприятий, проводимых для повышения устойчивости функционирования, в дальнейшем будем называть системой защиты.

Для оценки эффективности защиты целесообразно использовать два обобщенных критерия, соответствующие двум показателям устойчивости:

1. Приращение сохраняемой производительности за счет осуществления защиты:

$$Э_I = \Delta I = I^з_{\max}(B^з) - I_{\max}(B).$$

2. Приращение деструктивного воздействия, необходимого для обеспечения заданного снижения производительности:

$$Э_B = \Delta B = B^з(I_з) - B(I_з).$$

Верхним индексом (з) обозначены параметры, соответствующие их значениям при осуществлении защиты.

Помимо обобщенных критериев могут использоваться частные критерии, соответствующие конкретным направлениям повышения устойчивости, например, снижение вероятности деструктивного воздействия, уменьшение потерь КВОИ и т. д. Частные и обобщенные критерии связаны между собой функциональными зависимостями.

Для оценки экономической эффективности защиты целесообразно использовать три категории оценок:

реальная деятельность КВОИ за счет сохраняемых защитой возможностей КВОИ;

реальный экономический эффект, выражающийся в снижении бюджета на повышение эффективности использования КВОИ;

условный экономический эффект, определяемый по прогнозу на рассматриваемый период времени, как экономия информационного ресурса КВОИ и перерасход деструктивных средств злоумышленником для исключения эффекта защиты.

Третья категория оценки является основной на этапе исследования, вторая может возникнуть при совершенствовании первоначальных решений и корректировки планов, первая возможна после выполнения хозяйственных восстановительных работ.

Экономия информационного ресурса определяется через сохраняемую защитой производительность ΔI и себестоимость работ *(c)*:

$$\Delta C_I = \int_0^\infty c\Delta I(t)dt.$$

Перерасход средств для исключения эффекта защиты может быть принят в первом приближении равным стоимости дополнительного числа активных деструктивных средств и мощностей, необходимых для поражения структурных элементов КВОИ:

$$\Delta C_B = C\left(B^3\right) - C\left(B\right).$$

Условный экономический эффект с учетом расходов на защиту Сз необходимо принимать равным его минимальному значению при всех возможных вариациях деструктивных воздействий:

$$Эс = \min(B)\{\Delta C_I + \Delta C_B - C_з\}.$$

Предлагаемый подход оценки экономической эффективности защиты может быть использован в процессе проектирования и модернизации сложных систем, к которым относится система защиты КВОИ, когда не удается заранее исследовать, промоделировать и рассчитать основные характеристики и логику функционирования КВОИ адекватно реально протекающим процессам.

УДК 519.876

Н.М. Бобович, Д.А. Петрович

О ПРОГНОЗИРОВАНИИ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

При разработке системы мероприятий защиты объектов информатизации (ОИ) от деструктивных воздействий возникает задача прогнозирования результатов воздействий противоборствующей стороны

по ОИ, который подлежит защите. В настоящее время эта задача для объектов со сравнительно простыми функциональными связями между технологическими звеньями (элементами в звеньях) решается с использованием методов, разработанных применительно к выбору совокупности средств для воздействия по объектам противоборствующей стороны.

Основной исходной предпосылкой этих методов является предположение о полной определенности сведений относительно средств воздействия и недостаточной достоверности сведений о цели воздействия. При решении обратной задачи исходные предпосылки и в равной степени и задачи расчета коренным образом меняются. Прежде всего метод решения этой задачи должен быть чувствителен к размещению объектов на местности, их устойчивости к поражающему деструктивному воздействию, функциональным связям между элементами объекта и т. д. Отсюда следует, что основные сведения о цели должны быть известны и введены в алгоритм расчета. В то же время данные о внешнем воздействии на цель, а также ряд данных о цели (случайные отклонения от прочностных характеристик элементов цели, их ориентация относительно деструктивного воздействия и т. д.) не могут быть предсказаны точно.

Производительность объекта информатизации, определяемая оператором сопряжения последовательно-параллельной модели, будет представлять собой функцию, содержащую операции «сумма» и «выбор минимума».

При случайной вариации производительности элементов и подсистем статистические характеристики производительности объекта информатизации I = Ф(Ii) определяются методами расчета статистических характеристик функций случайных аргументов в рамках классической теории вероятностей.

Задача сводится к определению статистических характеристик вида

$$I_i = \sum_{j=1}^{m_i} I_{ij} \left(j = \overline{1, m_i} \right) \qquad (1)$$

$$I = \min_{(i)} \{ I_i \} \left(i = \overline{1, n} \right), \qquad (2)$$

где n – число технологических звеньев в системе;

m_i – число элементов, выполняющих (обеспечивающих выполнение) i -той технологической операции.

Математическое ожидание и дисперсия функций распределения «сложение» (1) и «минимум» (2) (для системы, состоящей их двух групп элементов) для случая нормального распределения определяются соотношениями, приведенным в (1).

Задача сводится к определению числовых характеристик производительностей, входящих в систему групп элементов и соответствующих корреляционных моментов.

УДК 343.8

П.Л. Боровик, В.А. Самойло

АКТУАЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ДЕАНОНИМИЗАЦИИ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Анализ оперативно-следственной и судебной практики по делам о преступлениях, связанных с использованием криптовалют, свидетельствует, что одной из насущных проблем выявления и расследования соответствующих криминальных деяний является установление личности (идентификация) владельца публичного биткоин-адреса, с которого либо на который осуществлялась транзакция. Поскольку процесс создания криптокошелька в основном анонимен, а переводы с одного биткоин-адреса на другой не верифицируются, установить персональные сведения о лицах (IP-адрес, географическое местоположение, Ф.И.О. и пр.), участвующих в транзакции, традиционными средствами не представляется возможным.

В ходе изучения и обобщения специальной литературы, посвященной рассматриваемой проблематике [1–4], было установлено, что в основу практической деятельности по деанонимизации лиц, совершающих преступления с использованием криптовалют, может быть положен процесс привязки публичного биткоин-адреса к цифровому идентификатору пользователя или его IP-адресу. Исследование показало, что этот процесс может осуществляться с применением так называемых интерактивных, активных и пассивных методов (данное деление в некоторой степени условно, оно лишь демонстрирует степень активности субъекта оперативно-розыскной деятельности по отношению к объекту исследования).

Так, интерактивные методы деанонимизации владельца публичного биткоин-адреса могут быть реализованы с использованием социальной инженерии, позволяющей установить непосредственный контакт с владельцем с целью совершения им определенных действий или разглашения соответствующей информации. Такие методы подходят в основном для деанонимизации частично неизвестных владельцев биткоин-адресов в условной цепочке биткоин-транзакций.

В основу активных методов могут быть положены подходы, основанные на внедрении специально разработанных обфусцированных биткоин-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик либо устанавливать прямую связь с другими узлами в сети. Использование обфусцированных биткоин-узлов позволяет перехватить IP-адреса владельцев и связать с ними определенные транзакции.

Пассивные методы могут основываться на использовании данных, полученных из блокчейна (https://www.blockchain.com/) либо иного общедоступного источника информации. Применяемые при этом подходы, с одной стороны, подразумевают отсутствие прямого взаимодействия с одноранговой сетью биткоин; с другой – полагаются на комплексные и широко представленные в открытых источниках методы анализа графов и иные эвристические технологии, связанные с биткоин-протоколом.

По нашему мнению, наиболее востребованными на первоначальном этапе решения обозначенной проблемы, а следовательно, и практической значимостью, могут обладать пассивные способы, основанные на использовании эвристики – совокупности логических и аналитических приемов, методов и правил, облегчающих и упрощающих решение конкретных познавательных и практических задач.

При пассивном сборе исследователь осуществляет поиск цифровых имен пользователей публичных биткоин-адресов из открытых источников глобальной сети: веб-сайты, форумы, социальные сети, майнинговые пулы, кошельки, банковские и небанковские биржи, порталы азартных игр и др.

Пассивные методы деанонимизации владельца публичного биткоин-адреса подразделяются на следующие разновидности:

метод прямого совпадения. В его основе лежит традиционный поиск цифрового идентификатора владельца биткоин-адреса в общедоступных источниках с использованием поисковых систем;

эвристический метод нескольких входов. Основан на сопоставлении входных биткоин-адресов. Например, если сумма транзакции превышает стоимость каждого из доступных биткоинов в кошельке пользователя, то существующие биткоин-клиенты выбирают набор биткоинов из разных имеющихся адресов в кошельке владельца и выполняют платеж с помощью транзакций с несколькими входными адресами, принадлежащими одному пользователю;

анализ смены биткоин-адреса. Суть данного метода основывается на генерации в ходе транзакции сетью биткоин так называемых теневых адресов [5], на который владельцу кошелька поступает «сдача». Используя методы сопоставления и анализа, можно легко установить начальный адрес владельца кошелька, который осуществлял оплату;

метод кластеризации. Основан на двух предыдущих подходах. Используя эвристический метод нескольких входов, исследователи смогли разделить сеть на 5.579.176 кластеров пользователей, начав с 12.056.684 открытых ключей. В последующем, анализируя смену биткоин-адресов, авторы предложили новую эвристику кластеризации, основанную на изменении адреса, позволяющую выделить и объединить адреса, принадлежащие одному и тому же владельцу кошелька [6]. С помощью данного метода можно идентифицировать основные финансовые субъекты (биржи, обменники, игровые сайты и т. п.) и способы взаимодействия между ними, используя лишь незначительное количество идентифицированных транзакций;

метод анализа виртуальных следов (цифровых отпечатков). В его основе лежит механизм формирования виртуальных следов сторонними веб-трекерами в открытом сегменте сети Интернет. В литературе, посвященной рассматриваемому вопросу, отмечается, что сторонний веб-трекер в состоянии деанонимизировать пользователей криптокошельков [7]. Так, при совершении покупок в интернет-магазине и проведении соответствующих транзакций в криптовалюте в интернет-пространстве будет оставлено множество релевантных виртуальных следов. Данные следы могут быть проанализированы двумя способами:

путем сопоставления транзакции (например, если у стороннего веб-трекера имеется доступ к адресу пользователя, то привязка последнего к адресу осуществляется тривиально; в другом случае, если веб-трекер владеет информацией о стоимости (даже приблизительной) покупки и времени совершения транзакции, то исследователю достаточно получить доступ к журналу транзакций);

путем формирования кластерного перекрестка (идентификация кластера адресов, позволяющая связать две либо более покупок одних и тех же пользователей с блокчейном);

метод деанонимизации с графовым анализом, основанный на реализации алгоритмов обнаружения сообществ и метрик центральности. Для этого могут использоваться социальные сети и (или) методы социальной инженерии. Так, исследователь может выявить сообщество друзей или соседей искомого лица, найти людей в середине цепочки, замешанных в незаконной деятельности, и т. д.;

метод построения и анализа график транзакций. Его суть состоит в следующем. Всю цепочку блоков в блокчейне можно рассматривать как ациклический граф транзакций $G = \{T, E\}$, где T – множество транзакций, хранящихся в цепочке блоков, E – множество однонаправленных ребер между этими транзакциями. Указанный граф представляет собой поток биткоинов между транзакциями в блокчейне с течением времени. При этом набор входных и выходных биткоинов в транзакции

следует рассматривать как веса на ребрах графа. Соответственно, каждое входящее ребро в транзакции несет метку времени и количество биткоинов, формирующих вход для указанных транзакций;

метод построения и анализа графа адресов. Его сущность сходна с приведенным выше. Анализируя граф транзакций G, исследователь может выявить корреляцию между различными входными и выходными адресами. Открытые ключи и соответствующие взаимосвязи можно использовать для построения графа адресов G = {P, E}, где P – это набор биткоин-адресов, а E – ребра, соединяющие эти адреса.

метод построения и анализа графа пользователя. Предполагает создание на основе вышеприведенных эвристических подходов графа пользователя путем группировки адресов, которые предположительно принадлежат одному и тому же владельцу.

Каждый из вышеприведенных методов деанонимизации состоит из двух этапов: этапа сбора данных и этапа анализа данных. Сбор данных может осуществляться как в режиме онлайн (например, с применением специально разработанных обфусцированных биткоин-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик, исследовать механизм распространения адресов, устанавливать прямую связь с другими узлами в сети), так и в автономном режиме с использованием обычного биткоин-кошелька.

Изложенное является лишь частным фрагментом важной проблемы выявления и пресечения преступлений, совершаемых с использованием криптовалют. В сочетании с соответствующими оперативно-розыскными подходами представленные в работе методы деанонимизации публичных биткоин-адресов могут помочь сотруднику органов внутренних дел установить лицо, совершившее преступление рассматриваемого вида.

Список использованных источников

1. Перов, В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты : учеб.-метод. пособие / В.А. Перов. – М. : Юрлитинформ. – 2017. – 200 с.

2. Сидоренко, Э.Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации / Э.Л. Сидоренко // Б-ка криминалиста. Науч. журн. – 2016. – № 3 (32). – С. 148–154.

3. Батоев, В.Б. Использование криптовалюты в преступной деятельности: проблемы противодействия / В.Б. Батоев, В.В. Семенчук // Тр. Акад. упр. МВД России. – 2017. – № 2. – С. 9–15.

4. Авдошин, С.М. Методы деанонимизации пользователей Bitcoon / С.М. Авдошин, А.В. Лазаренко // Тр. ИСП РАН. – Вып. 30. – 2018. – С. 89–102.

5. Накамото, С. Биткоин: одноранговая электронная кассовая система [Электронный ресурс] / С. Накамото // Биткоин [Офиц. сайт]. – Режим доступа: https://bitcoin.org/bitcoin.pdf. – Дата доступа: 22.10.2022.

6. Андрукли, Э. Оценка конфиденциальности пользователей в биткоинах [Электронный ресурс] / Э. Андрукли, Г.О. Караме // Cryptology ePrint Archive [Офиц. сайт]. – Режим доступа: https://eprint.iacr.org/2012/596.pdf. – Дата доступа: 22.10.2022.

7. Голдфедер, С. Когда cookie встречается с блокчейном: риски конфиденциальности веб-платежей через криптовалюты [Электронный ресурс] / С. Голдфедер // Б-ка Корнел. ун-та [Офиц. сайт]. – Режим доступа: https://arxiv. org/pdf/708.04748.pdf. – Дата доступа: 22.10.2022.

УДК 34:004.77

П.Л. Боровик

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Актуальность проблемы информационной безопасности обусловлена фундаментальной зависимостью всех сфер современного социума (экономика, культура, наука, медицина, правоохранительная деятельность и др.) от нормального развития и обмена информацией, что связано с повсеместным внедрением новейших информационно-коммуникационных технологий (ИКТ). Данное утверждение аргументируется рядом обстоятельств:

в условиях глобализации информационного пространства реализация жизненно важных интересов личности, общества и государства осуществляется посредством процессов информатизации, т. е. указанные субъекты видят реализацию своих интересов через призму получения благ, предлагаемых развитием информационных отношений, и желают развиваться в данном направлении;

в контексте всеобщей цифровизации информационная сфера приобрела статус системообразующей, и от нее в значительной степени зависит уровень экономического, социального, политического развития общества и государства;

специфика информационной среды такова, что негативные последствия реализации угроз информационной безопасности проявляются в других сферах жизнедеятельности личности, общества и государства и влияют на национальную безопасность в политической, экономической и иных областях;

анализ существующих в мире вызовов и угроз показывает, что в современных условиях возрастает опасность совершения трансграничных преступлений, возникновения кризисных ситуаций и иных противоправных действий с применением современных ИКТ.

В таких условиях особую актуальность приобретают вопросы формирования активной согласованной информационной политики международного сообщества и развития единого информационного пространства, создания совместного потенциала по противодействию информационным угрозам и обеспечению информационной безопасности, защиты информационных ресурсов и коммуникаций национальных органов власти и управления.

Отдельные аспекты данной проблемы в различные периоды исследовались в научных работах Э.Л. Бернейса, Н.А. Брусницына, Г.В. Вирена, В.Б. Вепринцева, Л. Войтасика, Д.А. Волкогонова, А.Б. Губарева, Л.В. Воронцовой, В.К. Новикова, И.Н. Панарина, Г.Г. Почепцова, С.П. Расторгуева, Д.Б. Фролова и др. Несмотря на пристальное внимание ученых и специалистов к этому вопросу, как в нашей стране, так и за рубежом, в настоящее время не существует единого терминологического аппарата и согласованного подхода к реализации политики международной информационной безопасности, а нормативная база, регулирующая методы и технологии ведения и противодействия кибервойнам, требует глубокого изучения и политологической концептуализации. В связи с этим обеспечение информационной безопасности становится одной из важнейших задач современного политического управления на государственном уровне с целью сохранения суверенитета национального пространства политических коммуникаций, включая национальные сегменты сети Интернет.

Следует отметить, что концептуальные методологические подходы к обеспечению информационной безопасности непосредственным образом опираются на государственные и международные нормативные правовые акты, регулирующие внутренние и внешние политические отношения. Ключевую роль при этом играют национальные стратегии информационной безопасности (кибербезопасности) – концептуальные документы, принятые в том или ином государстве, в соответствии с которыми осуществляется политика обеспечения информационной безопасности страны.

Изучение действующих стратегий информационной безопасности иностранных государств (США, Швеция, Эстония, Словакия, Финляндия, Голландия, Чехия, Литва, Германия, Франция и др.) показало, что их концептуальные подходы основываются на принципах, закрепленных в ключевых документах, к важнейшим из которых относятся стратегии информационной безопасности или равнозначные им по своим

функциям документы. Информационная безопасность рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества. Участие ряда стран, в частности, членов ЕС в общей оборонной организации НАТО, во многом определяющей конкретные методы обеспечения информационной безопасности, также способствует сходству политических курсов отдельных европейских стран в сфере информационной безопасности.

Вместе с тем результаты анализа содержания вышеприведенных стратегий свидетельствуют о том, что как на европейском, так и на международном уровне отсутствуют единые подходы к пониманию категории «информационная безопасность» («кибербезопасность») и других ключевых терминов. Как следствие, различаются и подходы к составлению стратегий, что приводит к невозможности сформулировать общие цели для международного сообщества по обеспечению информационной безопасности на глобальном уровне. Отсутствие общего «языка» и согласованного подхода усложняет процесс международного сотрудничества в данной сфере, ведь важность сотрудничества признается всеми странами. Кроме того, отсутствие конкретных планов действий в принятых стратегиях, отчетливого указания их целей, а также спектра решаемых проблем приводит к невозможности сформулировать конкретные практические рекомендации по реализации поставленных целей и задач для правительственных ведомств, национальных органов власти и других государственных органов.

Таким образом, проблема информационной безопасности в условиях глобализации носит комплексный, международный характер. Для ее решения каждое государство принимает концептуальные политические документы, к важнейшим из которых относится стратегия информационной безопасности или равнозначный ей по своим функциям документ (концепция, доктрина). Подобного рода документы не только определяют стратегические цели, конкретную политику и регулирующие меры для достижения и поддержания высокого уровня сетевой и информационной безопасности, но и играют ключевую методологическую роль в системе обеспечения национальной безопасности.

Особую актуальность приобретают вопросы формирования активной согласованной информационной политики международного сообщества и развития единого информационного пространства, создания совместного потенциала по противодействию информационным угрозам и обеспечению информационной безопасности, защиты информационных ресурсов и коммуникаций национальных органов власти и управления.

Для эффективной подготовки и своевременного реагирования на угрозы информационной безопасности необходимо согласованное ме-

ждународное сотрудничество. Первым шагом на пути к реализации этой задачи может стать принятие комплексной международной стратегии кибербезопасности. Для ее реализации необходимы:

унификация терминологического аппарата;

гармонизация законодательной базы;

разработка конкретных планов действий, отчетливое указание их целей, а также спектра решаемых проблем;

тесное сотрудничество частного и государственного сектора, осуществляемого посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами, обучения специалистов и обычных пользователей ИКТ), а также путем проведения специальных учебных мероприятий (учений, тренингов) на государственном и международном уровнях.

УДК 343.985

В.Л. Венгловский

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ НАРКОПРЕСТУПЛЕНИЙ

Используя интернет-технологии наркосбытчики получили возможность продавать наркотики бесконтактным способом и в определенной степени анонимно. Посредством сети Интернет создаются интернет-магазины, осуществляется реклама, привлечение и координация действий членов преступных групп в разных регионах страны, так и за ее пределами, что потребовало от правоохранителей в целях противодействия наркопреступлениям развивать и совершенствовать информационно-аналитическую деятельность.

Проделанный анализ научной и специальной литературы показал, что среди ученых и практиков отсутствует единое понимание сущности, задач и методов информационно-аналитической деятельности, что влечет существенные проблемы не только в области теоретической проработки рассматриваемого вопроса, но и в построении эффективной правоприменительной практики, организация которой осложнена наличием большого количества субъектов, в той или иной степени решающих задачи противодействия наркопреступности.

Одной из основных проблем при создании теоретической основы данной деятельности видится необходимость определения сущности и содержания информационно-аналитической деятельности при выявлении преступлений и как ее составной части – наркопреступлений, совершаемых в сети Интернет.

Ряд авторов в своих работах используют для обозначения рассматриваемой деятельности достаточно близкие по содержанию термины: «аналитическая разведка», «аналитическая работа», «аналитическая деятельность», «аналитический поиск».

Отдельные ученые относят информационно-аналитическую деятельность к числу методов познания и понимают под ним метод, заключающийся в комплексном применении сил, средств и методов оперативно-розыскной деятельности (ОРД) по сбору, обобщению и анализу конфиденциальной и легитимной информации, обеспечивающей приращение или получение новых знаний об объектах и субъектах криминальных проявлений, для упреждающего воздействия на преступность или определяют аналитический поиск как метод ОРД, предполагающий «проникновение» в документальные источники сведений и соответствующие массивы данных, содержащих знания об объектах, представляющих оперативный интерес, и их детальное изучение в целях получения оперативно значимой информации.

Вклад в развитие информационно-аналитической деятельности внес С.С. Овчинский, который в своей монографии «Оперативно-розыскная информация» предложил концептуальные основы информационного обеспечения оперативно-розыскной и профилактической деятельности органов внутренних дел.

В работе Е.Г. Белоглазова «Методология обеспечения аналитической разведки криминальных процессов и явлений» рассмотрены виды информационно-аналитической деятельности и источники информации, основанные на информационных технологиях, также определены основные направления этой деятельности применительно к различным оперативным подразделениям органов внутренних дел.

С.В. Пилюшин в своей работе «Аналитическая деятельность в принятии управленческих решений: сущность и значение» анализирует сущность информационно-аналитической деятельности на примере деятельности по выявлению экономических преступлений. При этом автор отмечает, что аналитическая деятельность вышеуказанных сотрудников осуществляется посредством применения конкретных методов познания, где для каждого характерна совокупность определенных принципов, правил, приемов и алгоритмов, сложившихся в четкую систему в процессе их применения.

В исследовании А.С. Щуровой «Незаконный оборот наркотиков в Интернете» делается акцент на том, что особенность незаконного оборота наркотиков, совершаемого посредством сети Интернет, заключается в использовании сетей телекоммуникаций и связи. При выявлении

данного вида преступлений объектом поиска выступает информация, отражающая направленность умысла на приобретение или сбыт наркотиков, как, например, непосредственно переписка приобретателя со сбытчиком, номера телефонов, паспортные и иные данные для совершения денежных переводов, иная информация, распространяемая через интернет, характеризующая преступную направленность. В свою очередь, объект и особенности информационно-аналитической деятельности автором раскрыты фрагментарно и не являются исчерпывающими, но при этом имеют прикладное значение при выявлении наркопреступлений.

Таким образом, в настоящее время отсутствует единый подход к пониманию понятия информационно-аналитической деятельности при выявлении преступлений, в том числе наркопреступлений, совершаемых в сети Интернет.

Ряд вопросов информационно-аналитической деятельности при выявлении наркопреступлений требуют научной проработки, наиболее актуальными для комплексного исследования являются аспекты, связанные с определением сущности, содержания, особенностей информационно-аналитической деятельности; получения информации и анализа ее источников, используемых при ее осуществлении; связанные с информационно-аналитическим и тактическим обеспечением данной деятельности.

УДК 343.98

О.П. Виноградова

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОВЕДЕНИЯ НЕВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Преступления в сфере информационно-телекоммуникационных технологий с каждым годом приобретают все большее распространение. Это связано с ростом уровня информатизации общества и внедрения интернет-технологий, что напрямую способствует увеличению таких преступлений, как кражи, совершенные с помощью интернет-технологий. В России на начало этого года насчитывалось 129,8 млн интернет-пользователей [1]. На рост пользователей сети Интернет, несомненно, повлияла пандемия коронавирусной инфекции COVID-19. Распространение коронавирусной инфекции повлияло на работу многих офлайн-площадок по продаже различных товаров и услуг и, следовательно, увеличилось количество интернет-магазинов. Все это, наряду с «цифровым невежеством» [2], обусловило значительное увеличение количества киберпреступлений.

В то же время, несмотря на понижение темпа роста рассматриваемых преступлений, нельзя не отметить, что кражи, совершенные с помощью интернет-технологий, и в целом все киберпреступления постоянно со временем видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов в настоящее время направлена на выявление, раскрытие и расследование краж, совершенных с использованием интернет-технологий.

Лицам, проводящим осмотр, необходимо знать, что компьютерно-техническое устройство находится в выключенном состоянии, его необходимо оставить в этом состоянии, чтобы предотвратить потерю доказательственной информации, а если устройство было включено, то стоит обратить внимание на информацию, содержащуюся на экране, об уровне заряда устройства, об операционной системе, службе доступа к файлам и сети. В данной ситуации могут быть выявлены цифровые следы преступления. Как отмечают В.О. Давыдов и И.В. Тишутина, такие цифровые следы «имеют высокую скорость трансформации, легко уничтожаются и модифицируются, могут быть представлены бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет, цифровой или электронный след может состоять из большого количества отдельных информационных элементов, которые могут быть записаны как на одном, так и на нескольких электронных носителях информации, подключенных как к одному, так и к нескольким компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть» [3]. Стоит отметить также, что на устройстве, которое является объектом осмотра, может быть установлена защита, требующая ввода определенного защитного кода или другой специальной команды, и если не произвести вышеперечисленные действия, то информация на устройстве может быть уничтожена, и поэтому для получения доступа к осматриваемому устройству необходим пароль. В таком случае считается целесообразным получить указанные пароли добровольно. Если будут проведены все эти действия, то обнаружение и копирование значимой информации для расследования уголовного дела будет осуществлено в более короткий

срок. В противном случае, несоблюдение порядка этих действий может привести к утере информации, содержащейся на компьютерно-техническом устройстве. Копирование информации с объекта осмотра осуществляется с возможностью сохранения неизменности копируемой информации с применением накопителей большой вместимости, для того чтобы в процессе копирования необходимые данные не были утрачены. Сохранность и неизменность изъятых следов на месте происшествия достигаются использованием надлежащих упаковочных материалов, исключающих возможность их физического повреждения.

Обыск по данной категории уголовных дел обладает определенной спецификой и требует незамедлительного проведения после возбуждения уголовного дела, поскольку следы преступления могут быть утрачены.

При подготовке к обыску должностное лицо должно определить следующие аспекты.

Выбрать оптимальный день и время для производства обыска. Если обыск проводится в жилом помещении, стоит выбрать то время, когда владельцы находятся дома, в служебных помещениях обыск проводится в рабочее время.

Провести анализ имеющейся информации о месте производства обыска (вид жилого помещения, количество этажей, расположение комнат, наличие в комнатах компьютерной техники и др.), также об обыскиваемых лицах и лицах, которые могут находиться в месте, где производится обыск, о наличии домашних животных, о путях подхода и отхода.

Исходя из анализа вышеуказанной информации, определяется состав участников следственного действия, решается вопрос о привлечении специалиста в области информационных технологий.

Определение необходимых технических средств, необходимых для производства следственного действия, а также предметов, которые нужны для изъятия и упаковки следов преступления.

Изъятие мобильного устройства и планшета обладает специфическими особенностями, потому что помимо электронной информации эти устройства несут в себе материальные следы, свидетельствующие о том, что именно подозреваемый пользовался данным устройством, например, следы пальцев рук, микрочастицы и т. д. Для упаковки и изъятия следов преступления обязательно привлекается специалист. При изъятии мобильный телефон переводится в режим полета. Изымать следует с зарядным устройством, это относится не только к мобильному устройству, а также и к ноутбуку.

На заключительном этапе составляется протокол следственного действия, в котором фиксируются абсолютно все проводимые действия, например, нажатие на клавиши, место обнаружения устройства и др., к протоколу прилагаются чертежи и схемы.

Список использованных источников

1. Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях – главные цифры [Электронный ресурс]. – URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472 (дата обращения: 20.10.2022).

2. Пандемия и цифровое невежество: эксперты назвали причины роста киберпреступности в России [Электронный ресурс]. – URL: https://online47-ru.turbopages.org/ (дата обращения: 23.10.2022).

3. Давыдов, В.О. Цифровые следы в расследовании дистанционного мошенничества / В.О. Давыдов // Изв. Тул. гос. ун-та. экон. и юрид. науки. – 2020. – № 3. – С. 22.

УДК 343.3

В.Р. Гайнельзянова

О ПОДГОТОВИТЕЛЬНОМ ЭТАПЕ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ В ХОДЕ РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Борьба с преступлениями, связанными с неправомерным доступом к компьютерной информации, в современных реалиях становится одной из приоритетных задач правоохранительных органов. Часто у лиц, производящих действия в пределах своей компетенции, в рамках расследования возникают определенные сложности в получении сведений о месте, времени и других данных, которые характеризуют совершенное деяние. Извлечение же криминалистически значимой информации об обстоятельствах преступления относится к числу важнейших составляющих работы следователя. Процесс получения таких данных осуществляется путем реализации осмотра места происшествия.

Расширение использования информационно-телекоммуникационных технологий во всем мире привело к правовым проблемам. Неблагоприятным условием процесса цифровизации общества являются компьютерные преступления, представляющие реальную угрозу не только для отдельных пользователей электронно-вычислительных машин, но и в целом для национальной безопасности страны.

Сохраняется высокая латентность данного вида преступления, которая обусловлена недостаточной цифровой грамотностью граждан, распространением программных средств анонимизации личности, обеспечивающих сокрытие информации о совершившем преступление лице, размножением программ для мобильных устройств, позволяющих перехватывать сетевой трафик, расшифровывать имена и пароли пользователей и пр. При этом следует констатировать низкую эффективность про-

изводства предварительного следствия по преступлениям в сфере компьютерной информации и судебного рассмотрения таких дел.

Указанный вид преступлений относится к группе сложных в расследовании и идентификации лиц, их совершивших. Использование преступниками возможностей информационно-телекоммуникационных технологий затрудняет определение механизма преступления, вследствие чего усложняется реализация следственных действий.

Приведем пример из правоприменительной практики. Так, Р.С.И. совершил неправомерный доступ к компьютерной информации, в результате которого осуществил списание со счета личных кабинетов интернет-магазина Sitilink бонусных баллов в виде денежных средств на сумму 31 776 р., принадлежащих С.Р.Т. По результатам проверки несанкционированных действий Р.С.И. произошла модификация компьютерной информации, выразившаяся в изменении количества бонусных денежных средств, которые принадлежали правообладателям личных кабинетов вышеуказанного интернет-магазина, а также преобразование их контактной информации и блокирование доступа к личным данным кабинета интернет-магазина.

В практике расследования неправомерного доступа к компьютерной информации осмотр места происшествия является первоначальным неотложным следственным действием, результаты которого представляются главными составляющими в сборе доказательственной базы.

Неправомерный доступ к компьютерной информации реализуется с использованием цифровых технологий и ресурсов сети Интернет. В связи с этим место совершения несанкционированных действий становится не конкретно-определенным. Криминалистически значимая информация, интересующая предварительное следствие, может находиться и в иных местах, а именно: в местах размещения цифровых носителей с данными, полученными в результате преступного деяния; в местах нахождения цифровых носителей со сведениями, которые могут представлять интерес для следствия; в местах, где установлены общественно опасные последствия от несанкционированных действий.

Перед проведением данного следственного действия с особой бдительностью и достаточной ответственностью рекомендуется подходить к избранию специалиста.

Основной целью осмотра места происшествия по уголовным делам указанного вида является установление определенного ЭВМ и компьютерных сведений, которые могут выражаться в качестве предмета либо орудия, используемых в реализации преступных действий, и содержать объекты преступной деятельности.

В ходе подготовительного этапа к осмотру места происшествия по делам о неправомерном доступе к компьютерной информации у руководителя учреждения, а также лица, отвечающего за обслуживание и

использование компьютерного оборудования, либо иного сотрудника предприятия, фирмы, следует взять объяснение, а при возбуждении уголовного дела – допросить и выяснить обстоятельства, связанные с блокированием помещения, где находится вычислительная техника, электронная система либо оборудование охранной сигнализации, разрешения, также логины, пароли, коды, дополнительные устройства и документация для беспрепятственного доступа к ним. Следует помнить, что дистанционное блокирование помещения связано с механизмом самоуничтожения значимой информации в компьютерном оборудовании, действие которой определяется вмонтированным в ЭВМ источником питания. При несоблюдении правил входа в помещение включается устройство защиты и ЭВМ устраняет значимую информацию на винчестере. Организации, эксплуатирующие данные механизмы уничтожения важных сведений на жестком диске вычислительной техники, часто имеют скрытую систему резервирования данных.

Алгоритм действий следственно-оперативной группы по прибытию на место происшествия, в первую очередь, путем криминалистических приемов фотографирования, рекомендуется зафиксировать сложившуюся обстановку на месте происшествия. Специалисту в данной отрасли знаний предлагается выполнить мероприятия, направленные на недопущение воздействия на имеющуюся информацию. Для этого путем отстранения их от компьютерных средств необходимо лишить сотрудников организации возможности выполнять действия по осуществлению порчи сведений, размещая их в ином помещении, по возможности изъять у них средства вычислительной техники. От услуг специалистов организации в сфере компьютерной информации целесообразно отказаться во избежание повреждения (уничтожения) информации.

Исходя из вышеизложенного, подытожим, что эффективность производства осмотра места происшествия при расследовании указанного вида преступлений обусловлена организацией тщательной подготовки к осмотру места происшествия, непременным использованием специальных познаний в области информационно-телекоммуникационных технологий и, соответственно, привлечением лиц, обладающих знаниями, опытом работы в данной сфере. В целях установления обстоятельств совершения неправомерного доступа к компьютерной информации совместная работа следователя и специалиста может осуществляться как на этапе получения консультативной информации, так и в ходе реализации рабочего этапа осмотра места происшествия. Решающее значение в ходе производства данного следственного действия имеет правильная фиксация и изъятие, упаковка объектов преступления, которые требуют обоснованного информационного взаимодействия следователя и специалиста.

УДК 34.07

Е.В. Герасимова, А.П. Жукова

ОТДЕЛЬНЫЕ ВОПРОСЫ ЭКСПЛУАТАЦИИ МОДУЛЯ СООП ИСОД МВД РОССИИ «УЧАСТКОВЫЙ»

На протяжении длительного времени в Российской Федерации наблюдается тенденция к развитию технических информационных систем, направленных на повышение эффективности и оптимизации деятельности различных государственных структур и негосударственных органов и организаций. Данный процесс характерен и для МВД России, где современные технологии направлены на обеспечение постоянного и качественного доступа к информации и повышение эффективности ведения электронного документооборота.

Приказом МВД России от 11 января 2016 г. № 1 «Вопросы эксплуатации программного обеспечения для реализации Сервиса обеспечения охраны общественного порядка» был утвержден сервис ведомственной информационной системы, обеспечивающий автоматизацию деятельности сотрудников и служащих органов внутренних дел Российской Федерации по различным направлениям работы.

Для оптимизации деятельности участковых уполномоченных полиции (УУП) в Сервисе обеспечения общественного порядка единой системы информационно-аналитического обеспечения деятельности МВД России (далее – СООП ИСОД МВД России) был разработан модуль «Участковый», который предназначен для автоматизации повседневной деятельности сотрудников подразделения УПП, обеспечения возможности выборки данных в разрезе обслуживаемых административных участков.

Практическое применение модуля «Участковый» имеет как положительные, так и отрицательные моменты. К удобствам эксплуатации данной системы следует отнести: доступность в любом месте; удобное размещение большого количества необходимой для работы УУП информации; использование данной системы через имеющиеся средства связи; возможность отправки электронного документа другим сотрудникам подразделения УУП. Все это позволяет своевременно решать множество задач и упрощает работу УУП при обслуживании административного участка.

К отрицательным моментам, а вернее будет сказано – к недостаткам эксплуатации модуля, следует отнести: невозможность произвести изменение информации в СООП лично участковым уполномоченным полиции, так как все изменения осуществляются с помощью администратора

СООП, что не позволяет сотрудникам корректировать неверные или утратившие силу данные; отсутствие контроля над применением и использованием этой системы лицами, замещающими руководящие должности в ТО МВД России, что может повлечь неэффективность ее применения, так как некоторые руководители привыкли использовать бумажные носители информации, считая их более надежными; отсутствие технической возможности передачи сведений по обращениям граждан в дежурную часть территориального органа непосредственно после их получения; исключение возможности программного обобщения результатов деятельности УУП за конкретный период времени и т. д.

Модуль «Участковый» позволяет участковым уполномоченным полиции, при осуществлении своей деятельности на административном участке, оперативно выполнить необходимые действия в различных ситуациях, так как воспользоваться данной системой с помощью гаджетов и иных устройств в любом месте, тем самым можно отметить удобность в применении и простоту в работе. Однако, используя такой модуль, приходится сталкиваться и с определенными проблемами, которые снижают эффективность работы. Так, в соответствии с п. 10.2 приказа МВД России от 29 марта 2019 г. № 205 «О несении службы участковым уполномоченным полиции на обслуживаемом административном участке и организации этой деятельности» на участковых уполномоченных полиции возлагается обязанность по розыску не только лиц, которые не прибыли к месту осуществления административного надзора либо самовольно оставивших его, но и иных лиц, в случае и порядке, предусмотренных актами МВД России об организации и осуществлении розыска.

Сегодня участковый уполномоченный полиции может выявить лицо, находящееся в розыске, только через проверку установочных данных граждан через интегрированные банки данных, доступ к которым имеется в дежурных частях территориальных органов МВД России на районном уровне.

При этом в модуле «Участковый» СООП ИСОД МВД России не имеется возможности у участкового уполномоченного полиции проверить лицо на предмет нахождения в федеральном розыске.

В связи с этим целесообразно на ведомственном уровне доработать этот модуль в части, касающейся создания в нем вкладки «Поиск по стране разыскиваемых преступников», в которой концентрировать информацию о лицах, находящихся в розыске на территории Российской Федерации.

Интеграцию и актуализацию информации о преступниках, находящихся в федеральном розыске, в модуль «Участковый» осуществлять из имеющихся учетов ФКУ «ГИАЦ МВД России» (вкладка Федераль-

ный розыск «Оповещение» в подсистеме ИБД-Ф). Создание такой вкладки позволит УУП оперативно проверять на законных основаниях граждан на предмет их нахождения в розыске, в том числе по преступлениям прошлых лет.

УДК 378

М.Г. Гизатуллин

НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Рассматривая направление обеспечения национальной безопасности того или иного государства, нельзя не отметить, что вопросы, относящиеся к организации и реализации образовательной деятельности, с позиции различных уровней образования, так же, как и другие вопросы данного направления, являются одним из ключевых направлений развития и функционирования государства в целом, определяют вектор его стратегического развития. Иными словами, образование выступает своего рода приоритетным направлением развития любого современного государства. Изучая же вопросы организации и реализации образовательного процесса в той или иной образовательной организации, например, высшего образования того или иного государства, необходимо отметить, что образовательный процесс в данном случае представляет собой непрерывный процесс становления обучающегося (студент, курсант, иностранный обучающийся), как личности, индивида, «профессионала» в той или иной области (сфере) деятельности. Этот процесс направлен на формирование у обучающегося знаний, умений, навыков и (или) опыта деятельности по определенному направлению подготовки (специальности), которые реализуются в той или иной образовательной организации.

Образовательные организации высшего образования России и государств – участников Международной парламентской ассамблеи (МПА) СНГ различных министерств и ведомств имеют как сходные, так и разные признаки, которые присущи различным видам деятельности, реализующимся в образовательных организациях.

В 2021 г. Министр внутренних дел Российской Федерации В.А. Колокольцев официально заявил: «Основное влияние на рост тяжких преступлений по итогам 2020 года оказало увеличение количества крими-

нальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий». Были и другие официальные заявления. Возможно, озвучивание данных проблем на государственном уровне и повлияло на то, что в 2021 г. почти все образовательные организации высшего образования системы МВД России перешли на так называемый новый формат с позиции, например, основных профессиональных образовательных программ высшего образования по специальностям и направлениям подготовки. Этот «новый формат» является актуальным направлением не только с позиции «теоретиков», но и с позиции «практиков». Иными словами, данное направление затрагивает как обучающихся образовательных организаций высшего образования системы МВД России, так и сотрудников территориальных органов МВД России. Это направление прежде всего касается формирования у обучающихся образовательных организаций высшего образования системы МВД России ключевых знаний, умений, навыков и (или) опыта деятельности в рамках такого достаточно актуального и востребованного в наши дни направления (в том числе в условиях нестабильной геополитической ситуации в мире), как организация кибербезопасности и обеспечение противодействия киберпреступности.

Сегодня многие организации, предприятия, учреждения той или иной области (сферы) деятельности испытывают на себе достаточно агрессивное, негативное, деструктивное и т. д. проявление со стороны определенного типа лиц – злоумышленников. Они подвержены, например, различного рода и типа кибератакам как извне, так и, к сожалению, в ряде случаев – изнутри, с целью осуществления своего рода дестабилизации как самой организации, учреждения, предприятия, так и государства в целом.

Таким образом, в 2021 г. в образовательных организациях системы МВД России почти по всем специальностям и направлениям подготовки появилась новая учебная дисциплина «Основы кибербезопасности». Ранее же вопросы обеспечения безопасности информации и противодействия различного рода и типа угрозам изучались обучающимися на таких учебных дисциплинах, как «Информатика и информационные технологии в профессиональной деятельности», «Основы информационной безопасности в органах внутренних дел» и др.

Учебная дисциплина «Основы кибербезопасности», реализуемая с 2021 г. в Уральском юридическом институте МВД России (далее – УрЮИ МВД России), прежде всего ориентирована на изучение обучающимися:

нормативно-правового регулирования в области информационных технологий, в том числе в области обеспечения кибербезопасности как на уровне государства, так и на уровне деятельности органов внутренних дел;

способов, методов, приемов и средств в области организации и реализации обеспечения безопасности различных вычислительных устройств;

природы возникновения и реализации различных каналов утечки информации;

вопросов в области организации и реализации обеспечения технической защиты информации, а также криптографической и стеганографической защиты информации;

вопросов в области различных инцидентов, возникающих на базе имеющегося у «пользователя» аппаратного обеспечения, программного обеспечения, информационных ресурсов, среды передачи, а также правил и алгоритмов реагирования на них и их детальную обработку и др.

УрЮИ МВД России на базе имеющихся компьютерных классов, полигонов, центров и других объектов также осуществляет проведение киберучений для закрепления у обучающихся компетенций, приобретаемых ими на учебных занятиях и в ходе самостоятельного изучения разделов учебной дисциплины «Основы кибербезопасности» в рамках внеаудиторной самостоятельной работы.

После завершения 2021/2022 учебного года и начала 2022/2023 учебного года в УрЮИ МВД России, помимо достаточно большого количества положительных моментов от появления в учебных планах учебной дисциплины «Основы кибербезопасности», можно выделить ряд потребностей субъектов образовательного процесса в рамках совершенствования методики проведения учебных занятий.

При этом достаточно важным направлением в области организации и реализации образовательного процесса является рассмотрение вопроса о необходимости оснащения автоматизированных рабочих учебных мест обучающихся (с позиции практической реализации):

системами, основанными на реализации сбора и анализа информации о тех или иных событиях, появляющихся на базе имеющихся у «специалиста» аппаратного обеспечения, программного обеспечения, информационных ресурсов и среды передачи (SIEM);

системами, основанными на реализации фильтрации трафика организации, учреждения, предприятия, а также его анализа (DLP).

Полагается, что учебная дисциплина «Основы кибербезопасности» может также найти свое отражение и в образовательных организациях системы МВД государств – участников МПА СНГ для формирования у обучающихся данных организаций компетенций в области организации кибербезопасности и обеспечения противодействия киберпреступности.

УДК 343.79

М.Г. Головенчик

КИБЕРПРЕСТУПНОСТЬ И ЭКОНОМИЧЕСКАЯ ПРЕСТУПНОСТЬ: ПРОБЛЕМЫ СООТНОШЕНИЯ

В соответствии с Концепцией информационной безопасности Республики Беларусь под киберпреступлениями понимаются предусмотренные Уголовным кодексом Республики Беларусь (далее – УК Беларуси) преступления против информационной безопасности. В УК Беларуси данным преступлениям посвящен разд. XII, гл. 31, где рассматриваемые преступления называются преступлениями против компьютерной безопасности. К таким преступлениям, в частности, относится несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации) (ст. 349 УК Беларуси), умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этим системе или сети, повлекшее по неосторожности причинение существенного вреда (ст. 355 УК Беларуси) и др.

Вместе с тем противодействие киберпреступности, в том числе подготовка специалистов в данной сфере, должно учитывать и то, как киберпреступления соотносятся с иными преступлениями, связанными с цифровой информационной средой.

Рассмотрим эту проблематику на примере экономических преступлений, к которым относят преступления, указанные в гл. 25 «Преступления против порядка осуществления экономической деятельности» УК Беларуси. В условиях цифровизации такие преступления также могут совершаться с помощью информационно-коммуникационных технологий, способами, сходными со способами совершения киберпреступлений. В этой связи может быть затруднительно отграничивать их друг от друга в практической деятельности. Так, в частности, ст. 222 УК Беларуси запрещает изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам. Последующее получение доступа к счетам или электронным кошелькам ставит вопрос о том, что в данном случае совершено: экономическое преступление или киберпреступление?

Актуальным в этой связи является и вопрос о том, как экономические преступления и киберпреступления могут и должны соотноситься между собой. Следует отметить, что уже сегодня отдельные исследователи говорят об экономической преступности в киберпространстве (Л.Н. Киданова, М.А. Простосердов), а также о формировании экономической киберпреступности (Ю.А. Грачев, И.А. Вишневенский, Д.В. Борцов). С учетом изложенного необходимо понимать, как следует осуществлять квалификацию преступлений, которые находятся «на стыке» экономических отношений и информационных технологий. Знание того, какие процессы происходят в экономической сфере в современных условиях, также является залогом более системной реализации действий, связанных с осуществлением противодействия киберпреступности.

При этом проблематика, связанная с совершением экономических преступлений в новых условиях, не может быть сведена исключительно к добавлению «цифровых технологий» к «традиционным» преступлениям, поскольку важно правильно квалифицировать совершенные деяния: будет ли совершаться в данном случае несколько преступлений (т. е. усматривается множественность преступлений), или же совершается единичное преступление. В связи с изложенным важно разграничивать экономические преступления, при совершении которых тем или иным образом используются новые технологии, и киберпреступления как таковые.

В целом процессы, происходящие в сфере экономической преступности, могут реализовываться разными способами и в рамках различных процессов. На основании проведенного анализа нами были определены следующие основные варианты:

совершение экономических преступлений с помощью компьютера или иных цифровых устройств;

совершение экономических преступлений посредством совершения киберпреступлений;

совершение экономических преступлений в рамках экономических процессов, имеющих цифровую форму.

В первом случае квалификация таких деяний не отличается от квалификации экономических преступлений, совершаемых без помощи компьютера, поскольку в этих преступлениях не усматривается цифровых экономических процессов или операций. Следует отметить, что сегодня почти все аспекты жизнедеятельности человека связаны с использованием той или иной цифровой техники или устройства. Например, почти всегда, в том числе при совершении экономических преступлений, совершаются звонки с телефонов, отправляются письма с использованием компьютеров, иных устройств.

Во втором случае, по нашему мнению, квалификация должна осуществляться по совокупности с киберпреступлениями. Следует отметить, что характер экономических преступлений не изменяется, поскольку, несмотря на цифровую форму отражения экономических операций, сами экономические процессы не имеют цифрового характера.

В третьем случае экономические преступления совершаются в сфере экономических отношений, имеющих цифровую форму. Здесь следует пояснить, что отдельные виды экономической деятельности сегодня осуществляются исключительно в цифровой среде. Это, например, деятельность криптообменников (операторов обмена криптовалют). Цифровые технологии в такой ситуации являются неотъемлемой частью деятельности соответствующих субъектов. В ситуации, когда кибердействия совершаются исключительно с целью влияния на программное обеспечение, такие деяния следует считать преступлениями против компьютерной безопасности. В случае же, когда программные средства используются исключительно с целью влияния на экономические процессы, то имеет место экономическое преступление в цифровой информационной среде. Если же подвергаются посягательству оба объекта, то деяние должно квалифицироваться по совокупности как преступление против компьютерной безопасности и как экономическое преступление.

Таким образом, понимание и разграничение различных видов преступлений является значимым фактором, как при проведении научных исследований, так и в деятельности специалистов в сфере противодействия киберпреступности.

УДК 342.9

М.В. Губич

ТЕОРЕТИКО-ПРИКЛАДНЫЕ ПРОБЛЕМЫ ПОНЯТИЙНО-КАТЕГОРИАЛЬНОГО РЯДА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нормативное правовое установление понятийно-категориального ряда в сфере информационной безопасности обусловлено преемственностью теоретико-методологической основы Концепции национальной безопасности Республики Беларусь (далее – Концепция нацбезопасности), а также спецификой рассматриваемой сферы. При этом нерешенность ряда доктринальных вопросов, особенно в части построения четкого понятийного аппарата, присуща как сфере национальной безопас-

ности, так и ее составляющей – информационной безопасности, что имеет принципиальное значение для построения эффективной системы ее обеспечения.

Анализ положений Концепции нацбезопасности и принятой в ее развитие Концепции информационной безопасности Республики Беларусь (далее – Концепция инфбезопасности) в части определения понятий «риски», «вызовы» и «угрозы» национальной безопасности позволяет сделать вывод, что «риски», «вызовы» и «угрозы» информационной и национальной безопасности понимаются как определенные состояния опасности.

Так, в соответствии с действующей редакцией Концепции нацбезопасности:

угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь;

формами угроз в стадии их зарождения и насыщения являются риски и вызовы национальной безопасности.

Однако, как на теоретическом уровне, так и на уровне нормативно-правового регулирования, не выработаны четкие и понятные для правоприменителя критерии и признаки, описывающие моменты перехода одного состояния опасности в другое. Изложенное не позволяет провести четкие границы между рассматриваемыми состояниями, что влечет существенные проблемы при практической реализации положений указанных концепций, а также, в определенной степени, вносит путаницу в нормативные предписания.

В качестве иллюстрации представляется возможным привести следующие примеры:

в соответствии с п. 33 Концепции инфбезопасности «государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия», что противоречит Концепции нацбезопасности, в соответствии с которой риски и вызовы – это формы угрозы;

в соответствии с п. 34 Концепции инфбезопасности государственное реагирование на риски, вызовы и угрозы состоит в локализации последствий и восстановлении нанесенного ущерба (при этом в соответствии с Концепцией нацбезопасности угроза рассматривается как возможность нанесения ущерба и не предполагает нанесения ущерба), в выявлении реализующихся вызовов (при этом в соответствии с Концепцией нацбезопасности вызов является формой угрозы в стадии ее насыщения, что не предполагает реализацию).

Таким образом, необходимым условием построения эффективной системы обеспечения безопасности являются разработка и внедрение

нового подхода к пониманию основных категорий механизма возникновения и реализации угроз информационной безопасности.

По нашему мнению, риск не должен рассматриваться как форма угрозы, так как по своей сущности риск является понятием, отражающим зависимость причинения ущерба от поведения субъекта в ситуации опасности. Что позволяет определить риск информационной безопасности как характеристику деятельности субъекта (объекта) информационной безопасности по предотвращению ущерба, осуществляемой в условиях возможности выбора варианта действий и неопределенности их последствий.

Помимо теоретической значимости предложенного понимания риска информационной безопасности, полагаем возможным подчеркнуть и практическую сторону его внедрения в правовую сферу, а именно – официальное закрепление возможности использования в сфере обеспечения информационной безопасности современных достижений в области риск-менеджмента – системы оценки риска, управления риском и отношениями, возникшими в процессе этого управления. Тем более разработчики Концепции инфбезопасности определили стратегической целью развитие системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня.

Относительно категории «вызов» следует отметить, что в научной литературе теоретико-методологическая проработка понятия «вызов» является одной из наименее разработанных проблем. Толковые словари предлагают несколько значений данного слова: предложение, требование явиться; сигнал, звонок, которым вызывают в аппаратах связи; призыв к борьбе, состязанию; поступок, оцениваемый как объявление борьбы, как оскорбление общепринятых норм. Иными словами, смысловое значение слова «вызов» применительно к сфере информационной безопасности заключается в описании опасности, исходящей от субъекта, имеющего умысел на причинение ущерба либо эскалацию опасности.

Следовательно, вызов должен рассматриваться как форма угрозы, исходящей от субъекта взаимоотношений в сфере защищаемого интереса, при этом данный субъект обязательно должен быть наделен волей выбора варианта поведения. Этимология рассматриваемого слова указывает, что вызов безопасности не может исходить от объекта, фактора, явления, не наделенного волей (объекты, факторы, явления природного характера, или ими обусловленные).

Таким образом, полагаем возможным определить вызов информационной безопасности как потенциальную или реально существующую возможность умышленного нанесения ущерба национальным интересам в информационной сфере.

Анализ понятия «угроза безопасности» и его употребления в нормативных правовых актах позволяет согласиться с пониманием данной категории, приведенной в Концепции нацбезопасности, в соответствии с которой угроза – потенциальная или реально существующая возможность нанесения ущерба.

Вместе с тем некоторые положения данного нормативного правового акта не в полной мере соответствуют определению рассматриваемого понятия. Так, к числу основных угроз национальной безопасности причислены: деструктивное информационное воздействие, наносящее ущерб национальным интересам; нарушение функционирования критически важных объектов информатизации. Иными словами, к угрозам отнесены воздействия уже причинившие ущерб, что, по своей сути, не соответствует представленному выше подходу к пониманию угрозы как возможности нанесения ущерба.

Следует отметить, что в гл. 19 «Противодействие киберпреступности» Концепции инфбезопасности не используются рассмотренные в настоящей статье понятия, что, в определенной степени, может объясняться относительной новизной борьбы с данными преступлениями, отсутствием устоявшихся понятий и категорий, что естественно для этой интенсивно развивающейся сферы. Однако, как и для всех сфер человеческой длительности, построение эффективной системы противодействия киберпреступности возможно только при наличии сформированной теоретической и правовой основы функционирования. Соответственно, решение обозначенных и иных теоретико-прикладных проблем понятийно-категориального ряда информационной безопасности положительно отразится на решении задач обеспечения информационной безопасности и противодействии киберпреступности.

УДК 342.9

М.В. Губич, Д.А. Шкурко

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ НАРКОПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Интернет является практически идеальной площадкой для обеспечения коммуникации поставщиков и потребителей наркотических средств, координации деятельности и отмывания денег, что порождает ряд проблем в сфере противодействия наркопреступности в сети Интернет.

Так, виртуализация наркопреступности проявляется в создании интернет-магазинов по продаже наркотиков, оплате посредством электронных платежных систем, криптовалют, общении при помощи различных интернет-мессенджеров и интернет-приложений, осуществляющих шифрование получаемых и передаваемых данных, и т. д.

В докладе Международного комитета по контролю над наркотиками за 2021 г. неоднократно отмечается, что рост наркопреступности во многом связан с использованием перечисленных нами выше возможностей интернета [1].

Стремительное развитие сети Интернет превратило его использование в преступной деятельности в основной ресурс для распространения наркотиков, позволило перейти на бесконтактные способы сбыта наркотиков, что существенным образом изменило весь преступный наркобизнес, а также деятельность правоохранительных органов по противодействию рассматриваемым преступлениям.

Наиболее проблемным полем в сфере противодействия наркопреступности является деанонимизация лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, особенно в его теневом сегменте сети – DarkNet, доступ к которому возможен только посредством использования специализированных браузеров и программного обеспечения, например Tor – одна из самых популярных технологий для доступа в DarkNet, представляющая собой систему прокси-серверов, позволяющих устанавливать анонимное сетевое соединение. Данная сеть рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Программное обеспечение Tor обеспечивает анонимность пользователя в сети Интернет, защищает его от анализа, скрывает IP-адрес используемого технического устройства, что затрудняет для представителей правоохранительных органов обнаружение следов, оставляемых преступниками в сети Интернет. Названные свойства достигаются за счет многоуровневого шифрования передаваемого трафика для нескольких произвольно выбранных узлов сети Tor и последовательной трансляции через эти узлы к получателю. Именно в сети Tor созданы и действуют онлайн-магазины, в которых предлагаются для продажи различные виды запрещенных веществ.

Активное использование в преступной деятельности интернет-мессенджеров, осуществляющих шифрование получаемых и передаваемых данных (Signal, Telegram, Vipole, Jabber и др.), также существенным образом трансформирует деятельность подразделений правоохранительных органов, осуществляющих борьбу с рассматриваемыми преступлениями. Это связано со следующими особенностями рассматриваемых мессенджеров: электронные ключи для расшифровки сооб-

щений создаются и хранятся на устройствах пользователей, а не на внешних серверах; в процессе отправки сообщения программным обеспечением отправителя и получателя по специальным алгоритмам генерируется уникальный ключ, дешифрование которого за разумное время представляется затруднительным, что делает передаваемую информацию труднодоступной для третьих лиц.

Наибольшее распространение в преступной деятельности, связанной с незаконным оборотом наркотиков, получило использование интернет-мессенджера Telegram. Преступниками все более активно используются специальные программы (боты), которые автоматизируют процесс продажи наркотиков, минимизируя участие в процессе распространения наркотиков физических лиц.

Следует отдельно отметить, что преступниками, в совокупности с рассмотренным программным обеспечением, активно используются специализированные технические средства, предназначенные для анонимизации пользователей в сети Интернет – анонимайзеры, VPN-сервисы, прокси-серверы.

Таким образом, деанонимизация лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, является одной из первоочередных задач, решаемых в ходе противодействия наркопреступности.

Необходимо отметить, что в Республике Беларусь принимаются определенные меры для решения указанной задачи. Так, в соответствии с Законом Республики Беларусь от 17 июля 2008 г. № 427-З (в ред. от 24.05.2021 г.) «О средствах массовой информации» среди оснований для ограничения доступа к интернет-ресурсу, сетевому изданию указывается распространение запрещенной информации (ст. 51^1). Постановлением Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь, Министерства информации Республики Беларусь от 3 октября 2018 г. № 8/10/6 (в ред. от 19.09.2022 г.) «Об утверждении Положения о порядке ограничения (возобновления) доступа к интернет-ресурсу, сетевому изданию» утвержден порядок ограничения доступа к интернет-ресурсам. Принимается ряд других правовых и организационных мер, направленных на недопущение «суперанонимности» пользователей сети Интернет.

Однако на практике применяемые в данном направлении меры являются недостаточно эффективными, что обусловлено многочисленными факторами, в том числе противодействием блокировкам со стороны разработчиков программных продуктов для анонимизации.

Кроме того, следует понимать, что эффективность поиска цифровых следов преступника, способствующих его деанонимизации, в значительной степени зависит от межгосударственного сотрудничества по

вопросам сбора, обработки, анализа, обмена информацией, представляющей оперативный интерес.

Необходимо отметить, что для органов внутренних дел наиболее актуальным является международное сотрудничество в целях получения значимой информации. Данное сотрудничество, как правило, осуществляется в рамках межправительственных и межведомственных договоров, либо при их отсутствии на основе принципа взаимности. При этом в силу имеющихся различий в законодательстве стран, даже при наличии нормативной базы, позволяющей осуществлять обмен информацией, ее получение не всегда возможно в силу объективных причин (короткие сроки хранения информации, усложнение процесса и т. д.).

Анализ международного и национального законодательства в сфере противодействия незаконному обороту наркотиков позволяет утверждать, что отсутствуют единые требования, обязательные для всех государств и иных субъектов, обеспечивающих функционирование сети Интернет и ее сегментов (поставщиков услуг интернета, хостинговых компаний, владельцев продуктов программного обеспечения и т. д.).

В целях разрешения указанной проблемы представляется возможным выстроить модель взаимодействия субъектов противодействия наркопреступности по аналогии с организацией межгосударственного взаимодействия в сфере борьбы с киберпреступностью, осуществляемого главным управлением противодействия киберпреступности МВД Республики Беларусь посредством национального контактного пункта (НКП), деятельность которого организована в соответствии с Положением о национальном контактном пункте МВД (утверждено приказом МВД Республики Беларусь от 12 июля 2021 г. № 201). Посредством НКП осуществляется взаимодействие с правоохранительными органами зарубежных стран и иностранными организациями, являющимися поставщиками интернет-услуг, при предупреждении, выявлении (раскрытии) и пресечении трансграничных и международных преступлений в сфере информационно-коммуникационных технологий.

Работа НКП организуется в режиме «24 часа в сутки 7 дней в неделю». При этом в нерабочее время, выходные и праздничные дни обеспечивается возможность круглосуточного получения сотрудниками, ответственными за функционирование НКП, информации либо запросов о помощи от НКП правоохранительных органов иностранных государств (в настоящее время указанная международная сеть НКП имеется в 89 странах мира).

В настоящее время НКП позволяет оперативно обмениваться информацией о готовящихся, совершаемых либо совершенных преступлениях в киберпространстве, а также запрашивать необходимую для проведения оперативно-розыскных мероприятий и следственных действий техническую и иную информацию из аналогичных подразделе-

ний правоохранительных органов государств-участников информационного обмена. Указанные возможности международного обмена информацией, несомненно, способствуют повышению эффективности противодействия киберпреступности.

Таким образом, в настоящее время наиболее актуальными проблемами в противодействии наркопреступности в сети Интернет являются осуществление деанонимизации лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, а также повышение эффективности международного сотрудничества с правоохранительными органами и иностранными организациями, являющимися поставщиками интернет-услуг.

В целях решения указанных проблем видится необходимым:

повышение компетенций сотрудников подразделений по наркоконтролю и противодействию торговле людьми в части осуществления деанонимизации лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, работы с электронными цифровыми следами, использованию методов поиска и анализа данных из открытых источников;

совершенствование механизмов межгосударственного взаимодействия в части, касающейся своевременного получения информации о сетевом трафике у поставщиков услуг интернета, хостинговых компаний, владельцев продуктов программного обеспечения (в качестве организационно-правовой основы взаимодействия рассмотреть опыт функционирования НКП).

Список использованных источников

1. Доклад Международного комитета по контролю над наркотиками за 2021 год [Электронный ресурс]. – Режим доступа: https://unis.unvienna.org/pdf/2022/INCB/INCB_2021_Report_R.pdf. – Дата доступа: 31.10.2022.

УДК 334

В.Б. Гунько

О КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ СБЫТА НАРКОТИКОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Прогресс современных информационно-телекоммуникационных технологий способствует развитию экономики государства, повышению уровня жизни граждан. Однако достижения науки и техники в данной области используются, в том числе, преступным сообществом в целях совершения различного рода противоправных деяний.

Одной из сфер преступного бизнеса, где информационно-телекоммуникационные технологии играют ключевую роль, является незаконный оборот наркотических средств, психотропных веществ или их аналогов. Так, в соответствии с официальными данными МВД России в 2019 г. выявлено 190,2 тыс. преступлений, связанных с незаконным оборотом наркотиков, в 2020 г. – 189,9 тыс. преступлений, в 2021 г. – 179,7 тыс. преступлений. При этом количество зарегистрированных преступлений в данной сфере, совершенных с использованием информационно-телекоммуникационных технологий, составило: в 2019 г. – 24 677, в 2020 г. – 47 060, в 2021 г. – 51 444. Наблюдается более чем двукратный рост за два года. За десять месяцев 2022 г. число выявленных случаев незаконного производства, сбыта или пересылки наркотических средств, психотропных веществ, а также незаконного сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, совершенных с использованием информационно-телекоммуникационных технологий, превысило показатели 2021 г. и составило 52 913. Неслучайно в Указе Президента Российской Федерации от 2 июля 2021 г. № 400 в числе стратегических национальных приоритетов Российской Федерации названо «предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе … организации незаконного распространения наркотических средств и психотропных веществ…».

В процессе расследования преступлений, в том числе и в сфере незаконного оборота наркотических средств, важное значение имеет криминалистическая характеристика преступления, которую можно определить как систему его значимых элементов и взаимообусловливающих связей между ними.

Вопрос о структуре криминалистической характеристики преступления вообще и сбыта наркотических средств с использованием информационно-коммуникационных технологий в частности является дискуссионным. Исследуя криминалистическую характеристику сбыта наркотиков с использованием информационно-телекоммуникационных технологий, ряд исследователей определяют ее состав традиционно, как содержащий сведения о предмете преступного посягательства, о месте совершения противоправных деяний и о личности типичных преступников. С учетом особенностей рассматриваемого вида преступлений представляется целесообразным при построении структуры их криминалистической характеристики акцентировать внимание на способе совершения преступления, в основе которого лежит использование возможностей, предоставляемых современными информационно-коммуникационными технологиями.

Сведения о способе совершения рассматриваемого вида преступлений должны включать информацию об использованных информационных технологиях, алгоритмах их функционирования.

Способы сбыта наркотиков с использованием информационно-телекоммуникационных технологий в значительной мере характеризуют личности типичных преступников, их умения и навыки, в том числе в создании и использовании в преступных целях соответствующего программного обеспечения. Эта информация, в свою очередь, может помочь при установлении особенностей способа незаконного сбыта наркотиков, следов анализируемого преступления, определяя его типичную обстановку.

Сведения об обстановке совершения незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий должны учитывать, что значительная часть преступных действий протекает в информационном пространстве. Другими словами, обстановка совершения преступления определяется совокупностью условий, в которых происходит функционирование информационно-телекоммуникационных технологий.

Состав и объем сведений, составляющих следовую картину анализируемых преступлений, также в значительной степени определяется способом совершения незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий. Знание особенностей функционирования аппаратного и программного обеспечения, используемого в процессе совершения преступления, позволит определить места в информационно-коммуникационной сети, где могут находиться цифровые следы, механизм их образования, направления поиска источника следообразующего воздействия, составить представление о личности типичного преступника, конкретизировать отдельные элементы обстановки расследуемого преступления.

Таким образом, криминалистическую характеристику сбыта наркотических средств с использованием информационно-телекоммуникационных технологий можно представить как модель, содержащую типичные сведения об основных элементах анализируемого вида преступлений и включающую, в том числе, элементы, определенные технологией совершения преступлений: специфический способ, обстановка, обусловливающая возможность их совершения, личность преступника, следовая картина преступлений и корреляционные связи между ними.

УДК 342.95

Д.А. Егоров

ОБ ИНФОРМАТИЗАЦИИ АДМИНИСТРАТИВНОГО ПРОЦЕССА

В соответствии с Концепцией информационной безопасности, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, национальным приоритетом и общегосударственной задачей Республики Беларусь является формирование информационного общества, основанного на доступности информации, распространении и использовании знаний для поступательного и прогрессивного развития государства.

Анализ статистических показателей, характеризующих становление цифровой экономики и уровень развития инфраструктуры информационно-коммуникационных технологий, позволяет отметить, что Республика Беларусь на протяжении последних лет реализовала значительные правовые, организационные и технические мероприятия по совершенствованию информационной сферы и цифровой трансформации государства.

В частности, с 2014 по 2020 г. удельный вес населения, использующего сеть Интернет, увеличился с 63,6 % до 85,1 %, доля населения, охваченного мобильными сетями стандарта GSM, превысила 99 %, а количество организаций, использующих стационарный широкополосный доступ в сеть Интернет, составило 94,6 %. Повышается также и эффективность функционирования Единого портала электронных услуг общегосударственной автоматизированной информационной системы, в рамках которой в 2020 г. количество оказанных электронных услуг и административных процедур превысило 70 единиц на 100 человек населения.

В таких условиях формируются объективные предпосылки для перехода к высокотехнологичным стандартам взаимодействия государства и общества не только в «восприимчивых» к информатизации направлениях функционирования государства (образование, здравоохранение, культура) и правоприменительной деятельности его органов (электронное лицензирование, расчет налогов, контрольная деятельность, персонифицированный учет), но и создаются условия для цифровых инноваций в традиционно классических сферах, связанных с обеспечением безопасности и правопорядка.

В данном контексте речь идет об информатизации административного процесса, как правового средства обеспечения частно-публичных интересов в сфере государственного управления. Его классические

задачи по защите жизни, здоровья, прав, свобод и законных интересов физических лиц, интересов общества и государства, прав и законных интересов юридических лиц обусловливают необходимость дополнительного исследования правовых средств их реализации с определением тенденций их дальнейшего развития и адаптации к условиям цифровой трансформации государства.

Конечно же, речь не идет о том, чтобы, по образному выражению отдельных исследователей, радикализировать дискурс и перевести дискуссии из реальных процессуальных проблем в квазинаучную плоскость. Административный процесс не перестанет быть классическим институтом административного права в связи с внедрением в процессуальную деятельность цифровых технологий. Речь скорее идет о том, чтобы с их помощью повысить эффективность и оперативность деятельности его участников по делу об административном правонарушении, обеспечить правоприменителей дополнительными средствами правового и технологического характера, отвечающими современным тенденциям развития информационного общества.

Следовательно, на основании анализа норм процессуально-исполнительного законодательства и практики его применения представляется возможным выделить основные направления для дальнейшей информатизации административного процесса и внедрения в правоприменительную практику современных достижений цифровых технологий.

Во-первых, речь должна идти о расширении потенциала работающих в автоматическом режиме специальных технических средств, с помощью которых осуществляется фиксация административных правонарушений. В настоящее время спектр их использования ограничен административными правонарушениями в области безопасности дорожного движения и эксплуатации транспорта и практически реализуется в отношении противоправных деяний, предусмотренных ч. 4 и 5 ст. 18.11 Кодекса Республики Беларусь об административных правонарушениях (КоАП), ст. 18.12, 18.18, 18.19 КоАП. Вместе с тем перспективными направлениями использования таких средств выступает выявление правонарушений, связанных с невыполнением требований дорожных знаков или разметки, сигналов, указаний светофора, нарушением правил маневрирования, проезда перекрестков, обгона, и правонарушений, посягающих на иные объекты правоохраны. В частности, речь идет о развитии Республиканской системы мониторинга общественной безопасности и внедрении в ее функционал механизмов лицевой биометрии, позволяющих осуществлять идентификацию лиц, совершающих административные правонарушения в общественных местах, против собственности, порядка управления и пр. Подобного рода технологии, основанные на программных продуктах компаний

NtechLab, TevianFaceSDK, Kipod, успешно функционируют в Российской Федерации.

Во-вторых, представляется важным дальнейшее внедрение электронного документооборота в производство по делам об административных правонарушениях. В настоящее время такие механизмы предусмотрены только при направлении копий постановления о наложении административного взыскания (ст. 10.3, 10.4, 12.12 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях (ПИКоАП)), постановления об освобождении от административной ответственности с вынесением предупреждения (ст.10.5 ПИКоАП), а также реализованы при вызове лиц, участвующих в административном процессе (ст. 11.6, 12.5 ПИКоАП). Вместе с тем перспективными направлениями видятся использование электронных документов при обжаловании действий и решений судьи, должностного лица органа, ведущего административный процесс, обжаловании постановления по делу об административном правонарушении, заявлении ходатайств, при заявлении (сообщении) об административном правонарушении в порядке, предусмотренном ст. 9.2, 9.3 ПИКоАП.

В-третьих, совершенствование правовой процедуры электронного документооборота в административном процессе делает в перспективе возможным «перевод» в электронную форму и самих дел об административном правонарушении. Тем более действующая редакция п. 4 ч. 1 ст. 1.4 ПИКоАП, определяющая термин «дело об административном правонарушении», не исключает возможность осуществления данного обособленного производства в электронном формате. Такой подход, безусловно, требует оптимизации законодательства об электронных документах и электронной цифровой подписи, определения порядка функционирования реестров дел об административных правонарушениях, закрепления особенностей процесса доказывания и производства процессуальных действий, совершенствования механизмов делопроизводства, документооборота и защиты персональных данных участников административного процесса. Важнейшие новации в направлении формирования электронного правосудия (e-justice) уже реализованы в деятельности судов общей юрисдикции Республики Беларусь и включают в себя сервисы «Расписание судебных заседаний», «Банк данных судебных постановлений», «Картотека обращений», «Картотека дел», «Уведомления» и «Калькулятор госпошлины». Подобные механизмы также успешно внедрены в практику судопроизводства в США (Case Management/ Electronic Case Files, Public Access to Court Electronic Records), Италии (Sistema Informativo della Cognizione Penale), Испании (Justicia Digital), Германии (Elektronischen Gerichts- und Verwaltungspostfach) и Казахстане (Единый реестр административных производств).

Таким образом, информатизация административного процесса представляет собой процесс внедрения в производство по делам об административных правонарушениях информационных технологий, совокупность которых направлена на выявление противоправных деяний, идентификацию лиц, их совершивших, повышение эффективности и оперативности деятельности суда, органов, ведущих административный процесс, иных его участников по решению задач ПИКоАП.

УДК 343.985

Б.А. Жилхайдарова

ПРАВОВЫЕ ОСНОВАНИЯ ЗАКРЕПЛЕНИЯ И ПРИОБЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ К МАТЕРИАЛАМ ЭЛЕКТРОННОГО УГОЛОВНОГО ДЕЛА

Благодаря стремительному развитию информационно-коммуникационных технологий в Республике Казахстан стало возможным ведение досудебного расследования и их судебного рассмотрения в электронном формате.

Стратегическим планом развития Республики Казахстан до 2025 г., утвержденным Президентом Республики Казахстан от 15 февраля 2018 г., правоохранительным органам поручено обеспечить поэтапный переход уголовных дел в электронный формат.

Ведение электронного уголовного дела Генеральной прокуратурой реализовано в модуле Е-УД на базе информационной системы Единого реестра досудебных расследований (ИС ЕРДР), а судебное рассмотрение происходит в ИС «Төрелік» (пер. с казах. – арбитраж). Однако сейчас в информационных системах отсутствует функционал фиксации электронных доказательств и приобщения их к электронному уголовному делу.

В настоящее время электронным доказательством являются сведения о фактах, имеющих значение для установления обстоятельств, подлежащих доказыванию по уголовному делу, зафиксированные в форме цифровой информации, восприятие содержания которой невозможно без применения технических средств.

При оценке допустимости электронных доказательств должно учитываться следующее:

надежность способа, с помощью которого обеспечивалась невозможность внесения изменений в цифровые данные;

надежность способа, при помощи которого идентифицировался его составитель;

правильность способа фиксации информации.

Указанное свидетельствует, что при формировании электронного уголовного дела необходимо учесть особенность таких доказательств.

Инструкция о ведении уголовного судопроизводства в электронном формате (далее – Инструкция) является юридическим инструментом правового регулирования нового формата досудебного расследования, которая утверждена приказом Генерального прокурора Республики Казахстан от 3 января 2018 г. № 2.

Ведение электронного судопроизводства заключается в осуществлении досудебного расследования в электронном формате путем ввода электронного документа либо вложения сканированного файла в ИС ЕРДР на основании принятых должностным лицом процессуальных решений и действий.

Порядок заполнения реквизитов электронных форм определяется Правилами приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения ИС ЕРДР, утвержденными приказом Генерального прокурора Республики Казахстан от 19 сентября 2014 г. № 89.

Конечно же, по всем процессуальным решениям и действиям составляется опись, а также к материалам электронного уголовного дела приобщаются все необходимые медиафайлы (видео-, фото- и аудиоматериалы), отображающие ход следственных действий.

При этом специальные шифровальные комплексы обеспечивают безопасность защищенных каналов связи и гарантируют тайну следствия, препятствуют искажению собранных доказательств, либо разглашению охраняемой законом тайны. Но вместе с тем участники уголовного процесса не ограничены в использовании своих прав и обязанностей в рамках действующего уголовно-процессуального законодательства.

В частности, п. 26 Инструкции предусматривает, что участники процесса получают доступ к соответствующим материалам электронного уголовного дела посредством функционала «Публичный сектор» ИС ЕРДР (Qamqor.gov.kz), через который возможна подача ходатайств (жалоб) и их своевременное рассмотрение. Для работы с «Публичным сектором» нужны подключение к сети Интернет и электронно-цифровая подпись.

По данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, за 11 месяцев текущего года число оконченных уголовных дел в электронном формате по правоохранительным органам составило 80 % (55 092 из 69 193), в том числе с рассмотрением их в суде – 74 % (32 140 из 43 654).

Электронное судопроизводство положительно повлияло также на процессуальную экономию времени и финансовых средств, сокращение сроков расследования, получения электронных санкций и других

справочных материалов, прозрачности уголовного процесса, обеспечение прав участников, системный и качественный ведомственный контроль и прокурорский надзор.

В частности, орган, ведущий уголовный процесс, уже не обременен вопросами затрат на почтово-телеграфную корреспонденцию, командировочных затрат и иных административных ресурсов. Уведомления участникам уголовного процесса поступают посредством СМС-сообщений (онлайн).

Несомненно, в ходе правоприменительной практики все еще встречаются недочеты и ошибки, связанные с техническим оснащением и бесперебойной работой каналов связи, но в целом эти вопросы характерны первоначальной стадии любого процесса и поправимы в ходе дальнейшей модернизации.

В целях дальнейшего совершенствования электронного судопроизводства в ИС ЕРДР планомерно запущена такая опция, как «интеллектуальный помощник следователя (помощь при расследовании)» и «OFFLINE-приложение», ориентирующая молодого следователя принимать правильные процессуальные действия и не допускать принятия незаконных решений.

Кроме того, в системе имеется возможность назначения экспертизы по вещественным доказательствам и получения результатов исследования. Однако сами вещественные доказательства предоставляются на исследование в материальном носителе и приобщаются к электронному уголовному делу.

Например, в рамках уголовного дела была изъята компьютерная информация о преступных махинациях, которая копируется в CD-R диск, после чего приобщается к уголовному делу на материальном носителе.

Учитывая упростившийся процесс назначения экспертизы, остались неразрешенными вопросы передачи вещественных доказательств. По нашему мнению, следует более шире применять возможности цифровых технологий в закреплении цифровых доказательств. Фиксацию и интеграцию цифровых доказательств (следы, существующие на электронно-цифровых носителях средств вычислительной техники и в виртуальном пространстве) необходимо автоматизировать без привлечения специалиста в данной области, используя информационные системы, устройства для подключения с блокираторами связи и создавая безопасный канал передачи данных (без доступа к сети Интернет). При этом доказательством по уголовному делу должен признаваться не электронный носитель, а сама цифровая информация. Следователем выносится соответствующее постановление, в котором указывается на электронный характер доказательственной информации, определяется носитель, на котором она хранится при уголовном деле, наименование

и вид программного обеспечения, информационного сервиса, с помощью которого можно осуществить доступ к сведениям, имеющим значение для уголовного дела.

УДК 343.97

Л.Л. Зубарева

ПРОСТРАНСТВЕННАЯ МОБИЛЬНОСТЬ И КИБЕРПРОСТРАНСТВО КАК НОВАЯ СРЕДА ПРЕСТУПНОСТИ

Современные люди проводят в интернет-пространстве значительную часть своего времени, в том числе выполняя служебные обязанности, обретая новые знакомства, общаясь и развлекаясь. Вполне закономерно, что преступники используют виртуальное пространство для своей противоправной деятельности. Приблизительно за пять лет число преступлений в Республике Беларусь, совершенных с использованием компьютерных систем и сети Интернет, выросло более чем в десять раз.

Современная криминология выделяет среди таких относительно новых криминальных явлений, как «преступления ненависти», «сталкерство» и прочие преступления в сфере компьютерной информации, при этом выделяя такой вид преступности, как киберпреступность. Значимость проблемы киберпреступности определяется, во-первых, ростом разработки, внедрения и использования новых информационных технологий, а во-вторых, не менее стремительным использованием вышеуказанных технологий в противоправных, нелегитимных целях и их экспансией в криминальной среде. Таким образом, в современных условиях стремительно развиваются не только технологии сами по себе, но и криминальная кибериндустрия.

Пространственная мобильность людей традиционно анализируется на основании таких критериев (индикаторов), как продолжительность и место пребывания, география и цель миграции, участники миграционных перемещений и их количество, отношения между ними, политический характер и правовой статус мигрантов. Однако это перечисление сегодня не может быть полным. В действительности, список индикаторов можно было бы составить на основе более широких обобщений. Так, на фоне глобализации и, самое главное, виртуализации жизнедеятельности $^{2}/_{3}$ населения Земли с той или иной интенсивностью живут в реальном и киберпространстве, следствием чего становится глобализация виртуализации, киберпреступность и кибердевиантность. Это та ситуация, когда территориальные границы наряду с фрагментизацией общества постмодерна, взаимопроникновением культур легко преодолеваются.

На наш взгляд, киберпространство является самостоятельным криминологическим явлением, имеющим собственные криминологические характеристики, влияющие на понятие пространственной мобильности в целом. Во-первых, в киберпространстве, как и в физическом пространстве, есть аналоги перемещения (переход по гиперссылкам), но, в отличие от физического, оно бесконечно, и его характеристики и ресурсы открываются с возрастанием опыта пользователя. Во-вторых, в киберпространстве, как и в физическом, есть общего доступа зоны (WWW или «всемирная паутина») и недоступные, в том числе и для контроля со стороны государства (здесь и организовывается киберпреступность). В-третьих, в киберпространстве имеется привязка к определенному месту (например, винчестер определенного компьютера). Таким образом, можно провести аналогию «своя» – «чужая» информация и проникновение, как в физическом пространстве, на чужую территорию. В-четвертых, на киберпространство, как и на физическое, распространяется государственный суверенитет, и оно разделено на межгосударственном уровне, что делает возможным возникновение враждебной деятельности отдельных лиц по поводу этих ресурсов. В-пятых, как и в физическом пространстве, деятельность преступников в киберпространстве при всех возможностях, затрудняющих обнаружение следов противоправной деятельности, оставляет следы, по которым их можно обнаружить. Еще одно свойство киберпространства, уже несколько отличающее его от физического пространства, – это более высокая степень анонимности пользователей. Это, несомненно, является одним из важных факторов, провоцирующих людей на противоправное поведение, и то, что в реальном мире они опасались бы совершать из-за контроля со стороны социума и государства, в киберпространстве при возможности остаться незамеченными становится для них возможным. Такие участники виртуального пространства с легкостью становятся жертвами преступлений при посещении различных сайтов, на которых реализуется запрещенный контент. Последствиями высокой степени анонимности является возможность нахождения партнеров для реализации преступных целей и любого вида девианта (возможность формирования преступных групп анонимно или из малознакомых лиц). Соответственно, сообщества в киберпространстве могут с легкостью формировать специфическое мировоззрение, систему ценностей, вырабатывать собственные правила поведения. Таким образом, одной из отличительных особенностей киберпространства является то, что в нем участники могут какое-то время противостоять государству.

Специфическими особенностями, непосредственно связанными с киберпространством, является его трансграничность, геймификация совершения преступлений (использование игровой среды (сетевых

компьютерных игр) для преступной коммуникации) и дистанционность их совершения (например, дистанционная торговля людьми).

Еще одна особенность киберпространства связана с временными границами совершаемых в нем деяний: если в физическом пространстве высказывание по реабилитации нацизма существует только в момент его произнесения, то такое же высказывание, размещенное в сети, может остаться там навсегда. Программы, попав в сеть, копируются и продолжают свою вредоносную деятельность неопределенное количество времени. С уголовно-правовой точки зрения это может быть аналогом длящихся преступлений, но продолжительность их осуществления в киберпространстве не всегда зависит от волеизъявления злоумышленника.

Несомненно, криминологический интерес вызывает и характеристика киберпространства, связанная со значением, которое имеет заявленная в нем информация. Аудитория популярных блогеров сравнима с аудиторией средств массовой информации, что, в свою очередь, способно влиять на то, что государства теряют привилегию на формирование мировоззрения. В киберпространстве степень общественной опасности деяний может определяться, в том числе, популярностью автора информации.

Вышеизложенное позволяет сделать ряд выводов. По нашему мнению, киберпространство можно считать самостоятельным криминологическим явлением, которое обладает набором характеристик, которые в значительной степени отличают его от физического пространства, определяют специфику его криминогенных и виктимогенных свойств, привнося новое значение в понятие пространственной мобильности человека. Современная криминологическая реальность требует уточнения существующих базовых уголовно-правовых положений, институтов уголовно-правовых запретов, криминализации новых общественно опасных деяний и дальнейшего изучения киберпространства в криминологических исследованиях.

УДК 343.3

А.В. Ивановский

ОБ ОЦЕНКЕ ПРИНАДЛЕЖНОСТИ К СОЦИАЛЬНОЙ ГРУППЕ

Устанавливая ответственность за возбуждение социальной вражды или розни по признаку социальной принадлежности ст. 130 Уголовного кодекса Республики Беларусь (УК), белорусский законодатель исходил из увеличения степени общественной опасности этих деяний в на-

стоящих условиях. В примечании к этой статье он также определил, что «принадлежность лица к определенной социальной группе определяется по признаку социально-групповой идентификации».

При расследовании уголовных дел о вражде и розни в рамках ст. 130 УК важно выявить критерии дифференциации социальных групп и подходы к определению принадлежности к ней групп лиц, исследовать связь социальной группы с обществом в целом, отдельными личностями, иными группами, общностями, институтами. Содержательная суть понятия «социальная группа» закреплена в словарях. Под группой понимают «любую относительно устойчивую совокупность людей, находящихся во взаимодействии и объединенных общими интересами и целями». Социальную группу необходимо рассматривать не только как «совокупность людей, объединенных по формальным или неформальным признакам, но и групповую социальную позицию, которую занимают люди». В настоящее время окончательного согласия среди специалистов по вопросу классификации социальных групп и принадлежности к ним пока нет. Известно даже мнение о нежелательности использования этого термина в правоохранительной деятельности из-за его «размытости».

Во всех «цветных революциях» социальные группы, оппозиционные власти, стремятся выступать в роли субъекта политических отношений. Они используют свои ресурсы для изменения характера функционирования государственной власти и управления, перехвата власти. Оппозиционная группа оказывает воздействие на органы власти для перераспределения социальных статусов и ресурсов в своих интересах и интересах главных заказчиков таких действий. В рассматриваемом случае критерием социально-групповой идентификации враждующих групп является законность права исполнять функции государственного управления, а также институциональные ценности. Основой вовлечения новых сторонников для оппозиции являются: оправдание законности требований и политического участия; процесс групповой самоорганизации; формирования своих представительных структур и их взаимодействие с действующей властью.

В.К. Потапов и А.В. Барков отмечают, что конфликтующие «социальные группы имеют различия, прежде всего мировоззренческого характера», и поэтому «за основу анализа следует брать понятие «экстремистская деятельность» и действия, к ней относящиеся. И учитывать не сам факт принадлежности потерпевших к какой-либо социальной группе, а стремление в данный момент разжечь вражду, неприязнь именно к этой группе, подчеркнуть ее неполноценность, вредность».

В ходе событий в Республике Беларусь в 2020 г. и в последующем в оппозиционных СМИ активно формировались, тиражировались и распространялись в обществе деструктивные (от лат. destructio – разрушение) информационные материалы, направленные на уничтожение социально-ориентированного белорусского общества. В том числе с помощью информационно-психологических воздействий сознательно разделялось белорусское общество на социальные группы: сторонников действующей Конституции и Президента Республики Беларусь; сторонников оппозиционных сил. Они вовлекали в противоправные действия и нейтральных не интересующихся в иные времена политикой лиц. В отдельных информационных материалах оппозиционных СМИ присутствовали высказывания и утверждения побудительного характера, призывающие к вражде и ненависти по отношению к объединенной по устойчивому признаку конструктивной общественно-политической ориентации группе (Президенту Республики Беларусь, сотрудникам правоохранительных органов, государственным служащим, представителям власти и их сторонникам). В текстах использовался язык вражды, высказывания были проникнуты неприязнью, ненавистью, сеялась рознь и вражда между всеми социальными группами, в высказываниях негативно оценивались как должностные лица государства, так и их сторонники. В сообщениях приводились утверждения и обоснования, оправдания и положительные оценки действий лиц, причиняющих вред государству и действующей системе государственного управления, призывающих к вражде и розни, ненависти по отношению к группе, защищающей конституционный строй; разделение граждан Беларуси на «своих» и «чужих»; создание в обществе атмосферы опасности и страха; представление протестных акций как действий, касающихся не только белорусов, но затрагивающих интересы их зарубежных покровителей; манипулирование с фактами (сознательные пропуски ключевых деталей при упоминании значимых событий, ошибки и искажения норм правовых актов, низкая достоверность сообщений и доводов, драматизация причин для недовольства).

В деструктивных высказываниях могут усматриваться признаки составов преступлений ст. 130 УК, и включающие умышленные действия, направленные на возбуждение социальной вражды или розни. В этой связи возникает проблема отнесения граждан к той или иной большой социальной группе.

М.И. Витковская предложила проводить иерархическую классификацию социальных групп по ряду оснований. Это позволило системно изучать их местоположение в общественной структуре; условия вступления в группу; количество индивидов в группе, характер, продолжительность и частоту взаимодействия; условия формирования и функционирования, времени устойчивой жизни групп; типа преобладающих отношений между индивидами, системы ценностей.

Таким образом, одним из подходов к решению обозначенной проблемы может быть выбор иерархического метода классификации социальных групп и последовательного распределения социальных групп на подчиненные классификационные объекты. Глубина классификации определяет количество уровней классификации, а ширина – число классификационных признаков. К достоинствам такой иерархической системы классификации можно отнести простоту построения и восприятия, возможность использования независимых классификационных признаков в различных ветвях иерархической структуры.

УДК 34. 047

А.В. Ивановский, Д.Д. Пашкевич

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

В условиях геополитического транзита все большую роль в развитии права начинают играть национальные интересы, государственное управление, активность социальных групп общества, информационные технологии, правовой опыт. Необходимость обработки интенсивно возрастающих потоков информации ведет к развитию новых организационно-правовых форм и методов ее обработки.

К одному из подходов к автоматизации процессов управления относят технологии искусственного интеллекта (ИИ). При этом в зависимости от степени зрелости конкретной технологии выделяют направление ее использования при принятии решений:

вспомогательное средство для выбора наилучшей альтернативы для решения; консолидации отчетности; предоставления данных управленцам в режиме реального времени;

разработка сценариев развития ситуации с применением когнитивных методов, прогнозирование последствий принятия решений;

выполнение функций управления, требующих больших объемов вычислений перед принятием решений. При этом люди используют полученные с помощью ИИ результаты в качестве основы для окончательного принятия решений;

высказывание самостоятельного мнения с помощью ИИ по проблемам, требующим решений;

выполнение функций верхнего уровня управления. Например, разработку стратегии, назначение на должности и т. п.

С учетом этого применения идей и технологий ИИ носит дискуссионный характер, связанный «с усложнением информационных отношений, при котором появляются новые информационные ценности и, как следствие, новые формы общественно опасных посягательств на них».

Под системой в ЕС ИИ понимается «система, которая:

принимает данные машинного и (или) человеческого происхождения и входные сигналы;

делает логические выводы о том, как достичь набора целей, определенных человеком, используя обучение, рассуждение или моделирование, которые реализуются посредством указанных ниже методов;

генерирует результаты в виде контента (генеративные системы ИИ), прогнозов, рекомендаций или решений, которые влияют на среду, с которой система взаимодействует».

К числу методов относят подходы, применяемые при разработке систем ИИ:

машинное обучение, включающее обучение с учителем, без учителя, обучение с подкреплением, с применением широкого спектра различных методов, включая глубокое обучение;

подходы, основанные на логике и на инженерии данных, включая представление знаний, индуктивное (логическое) программирование, базы знаний, механизмы вывода и дедукции, (символьное) формирование рассуждений и экспертные системы;

статистические подходы, байесовское оценивание, методы поиска и оптимизации.

А.А. Васильев, Ю.В. Печатнова отмечают, что ИИ нельзя считать классическим объектом правового регулирования, но и нельзя рассматривать как полноценный субъект права по следующим причинам:

традиционная концепция о субъектах права исходит из того, что участниками правоотношений являются физические и юридические лица;

попытки сравнения ИИ с физическими лицами не выдерживают критики с точки зрения физиологии;

когнитивные способности ИИ весьма ограничены в сравнении с человеческими функциями мозга.

Искусственная нейронная сеть, построенная по принципу функционирования нервных клеток живого организма, значительно уступает строению биологической нейронной сети по количеству слоев нейронов, кроме того в человеческом мозге обмен информацией между нейронами идет не последовательно, а параллельно и асинхронно.

Исследователи проблемы ИИ фокусируют внимание на правовой необоснованности признания ИИ субъектом права ввиду того, что ИИ не является носителем критически важных составляющих личности (души, свободного сознания, чувств, устремлений, личных интересов). Поэтому,

несмотря на сверхмощную скорость обработки информации, в разы превосходящую возможности человека, ИИ остается программой с привязанным к ней материально-техническим обеспечением. Ответственность за деятельность, связанную с применением ИИ, должны нести лица, использующие ИИ как объект повышенной опасности.

А.В. Макутчев, прогнозируя возможности и пределы внедрения ИИ в правоохранительную деятельность, выделяет три эволюционных этапа информатизации: трансформация всех процессов путем углубленного внедрения цифровой обработки данных; использование систем ИИ без непосредственного их участия в принятии решений; углубленное внедрение, когда система ИИ в той или иной степени заменяет собой сотрудников.

Очевидно, что внедрение систем ИИ в правоохранительную деятельность должно сопровождаться административными и организационными мерами. Однако основанием для наказания граждан могут быть только официальные юридические решения и документы.

УДК 378.6:004.45

И.С. Ивануха

ПОДГОТОВКА КАДРОВ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Активный рост киберпреступлений, совершенных с использованием информационно-телекоммуникационных технологий, наблюдаемый на территории России, так и во всем мире, порождает потребность в увеличении численности сотрудников органов внутренних дел (ОВД), способных эффективно решать задачи по предотвращению, выявлению, раскрытию и расследованию киберпреступлений с использованием и применением информационных технологий.

Киберпреступления в сфере компьютерной информации относятся к числу наиболее распространенных на сегодня видов преступлений. Следует отметить также, что методы совершения данных преступлений постоянно совершенствуются. Соответственно, вопрос противодействия и привлечения к уголовной ответственности лиц за совершение указанных противоправных деяний является весьма актуальным. Несмотря на широкое распространение преступлений в сфере компьютерной информации, на данный момент нет четкого определения в Уголовном кодексе Российской Федерации понятий «киберпреступность» и «киберпреступление».

Соответственно, вопросы противодействия и привлечения к уголовной ответственности лиц за совершение киберпреступлений являются весьма актуальными и нуждаются в подробной регламентации. При этом, несмотря на уменьшение зарегистрированных преступлений с использованием современных информационно-коммуникационных технологий, официальная статистика [1] не отражает объективную картину распространения киберпреступлений, показывая лишь незначительную часть реально совершенных. Происходит это из-за отсутствия единообразия в национальном уголовном законодательстве стран СНГ и негативно отражается на развитии методов эффективной борьбы с киберпреступностью – явлением, для которого не существует государственных границ. Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются киберпреступниками, орудующими в любом месте киберпространства, независимо от юрисдикции государств, с помощью компьютера и доступа в сеть Интернет. Отражается это и на эффективности международного сотрудничества в борьбе с киберпреступностью, которое невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой – уголовной ответственности не предусмотрено.

По данным правоохранительных органов, только за последний год распространенность преступлений различных видов, совершаемых с использованием информационных технологий, значительно увеличилась. Результаты анализа, проведенного Организационно-аналитическим департаментом МВД России, указывают на то, что количество зарегистрированных преступлений данной категории за девять месяцев 2022 г. и аналогичный период прошлого года снизилось на 4 %. При этом отношение числа раскрытых преступлений к общему числу преступных деяний, так называемая раскрываемость преступлений составила всего 30 %. Следует обратить внимание на то, что раскрываемость преступлений рассматриваемой категории весьма низкая.

Данная ситуация обусловлена тем, что сотрудники ОВД при расследовании таких преступлений допускают ошибки, которые в большинстве своем являются следствием их низкой профессиональной подготовки именно для раскрытия киберпосягательств. Например, минимальными знаниями по специальности «Информатика и вычислительная техника» обладают только 3,5 % сотрудников [5]. Стоит отметить, что невозможно эффективно предотвратить, выявить, раскрыть и расследовать киберпреступления без использования и применения информационных технологий.

К сожалению, существующая в нашей стране система противодействия преступлениям, которые совершаются с использованием современных технологий, в своем развитии еще заметно отстает [2]. Одна из основных причин низкой раскрываемости киберпреступлений – это низкая квалификация сотрудников ОВД во многих подразделениях. На наш взгляд, эта сложность обусловлена тем, что, несмотря на относительную дешевизну и повсеместную распространенность компьютеров, они недоступны для всех слоев населения. Считаем, что проблема кроется глубже, в школах недостаточное внимание уделяется дисциплине «Информатика и вычислительная техника». Поступая в высшее учебное заведение, многие впервые взаимодействуют с компьютером и впервые начинают получать базовые знания. Несмотря на то что в учебных заведениях МВД России и в рамках межведомственного взаимодействия с гражданскими вузами проводится повышение квалификации действующих сотрудников, специализирующихся на противодействии киберпреступлениям. Это не решает проблему в целом из-за недостаточной динамичности и гибкости системы образования в формировании компетентности специалистов юридического профиля к деятельности по противодействию киберпреступлениям [3]. Имеет место быть также низкое технологическое и программное оснащение образовательных организаций.

Вторая немаловажная причина – это отсутствие надлежащей подготовки и технологического оснащения действующих подразделений ОВД, которые непосредственно занимаются раскрытием киберпреступлений.

Например, по словам Саги Бар – генерального директора центра киберобразования в Израиле, в школах дети уже с первого класса учатся читать, писать и кодировать. В стране даже есть детские сады, где учат работе на компьютере и робототехнике. С четвертого класса ученики уже активно изучают программирование, а одаренные старшеклассники – технологии шифрования и методы борьбы с «черным хакерством» [4]. О том, насколько глубоки знания израильских школьников, можно судить по их развлечениям. Дети играют в игры, по условиям которых, например, взломана воображаемая компьютерная сеть, и у ребят есть 45 минут, чтобы узнать неизвестный компьютерный код, восстановить контроль за сетью и взломать систему злоумышленника, чтобы установить его личность.

В результате проведенного нами исследования, считаем, на современном этапе целесообразным сочетание подготовки соответствующих специалистов юридического профиля, а также одновременного повышения уровня базовой информационно-технической подготовки всех сотрудников ОВД. Определить специальные компетенции, которыми

должны обладать сотрудники ОВД, осуществляющие противодействие киберпреступности.

Считаем, что сотрудник должен обладать навыками и знаниями в области информационных технологий и кибербезопасности: архитектуры и организацией функционирования электронно-вычислительных машин; современных вычислительных систем и сетевых технологий; современных операционных систем; работы с большими данными; системы искусственного интеллекта; мониторинга информационных сетей; уязвимости современного программного и аппаратно-программного обеспечения; общих методов и средств обеспечения кибербезопасности; защищенных сетевых технологий глобального и локального назначения; функционирования электронных платежных систем. Понимание технологий реализации угроз кибербезопасности: атаки на информационные ресурсы, атаки на компьютерные сети, атаки на электронные платежные системы; поиск следов преступной деятельности и методика выявления (раскрытия) киберпреступлений. В области подготовки специалистов в данной сфере целесообразно определить направления работы по обеспечению образовательного процесса [5]: организация взаимодействия ОВД и участие в разработке учебных программ, организация работы филиалов кафедр, проведение совместных занятий, проведение стажировки, практики; совершенствование образовательного процесса с учетом изменяющихся подходов и перспектив в сфере противодействия киберпреступности; повышение уровня подготовки профессорско-преподавательского состава, организация повышения квалификации по данному профилю, стажировка в практических подразделениях ОВД, участие в тренингах, семинарах, конференциях; внедрение компьютерных технологий в образовательный процесс, применение в образовательном процессе специализированного программного и программно-аппаратного обеспечения, используемого в раскрытии киберпреступлений; создание практико-ориентированной среды в образовательном процессе; активизация научно-исследовательской работы по проблемам противодействия киберпреступности.

Список использованных источников

1. ЦСИ ФКУ ГИАЦ МВД России [Электронный ресурс]. – Режим доступа: http://10.5.0.16/csi/modules.php?name=Books&go=check&id=280. – Дата доступа: 25.10.2022.

2. Шевченко, Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. – 2015. – № 3. – 169 с.

3. Чукова, Д.И. Проблемы подготовки специалистов по расследованию компьютерных преступлений / Д.И. Чукова // Лучшая научно-исследовательская работа 2019 : сб. ст. – Уфа : ООО «Науч.-изд. центр «Вестн. науки», 2019. – С. 103–108.

4. [Электронный ресурс]. – https://vpk.name/news/329623_kiberbezopasnost_po-izrailski.html. – Дата доступа: 25.10.2022.

5. Шеремет, И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере / И.А. Шеремет // Вопр. кибербезопасности. – 2016. – № 5 (18). – С. 3–7.

УДК 004.838

В.В. Комерцов

ТЕХНОЛОГИИ МАШИННОГО ОБУЧЕНИЯ КАК ИНСТРУМЕНТ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Основная цель настоящего исследования – систематизировать опыт в области правового регулирования создания и использования искусственного интеллекта (ИИ) и смежных технологий, а также выделить и осветить основные тенденции и ключевые проблемы в этой сфере в правоохранительной деятельности. Возможно, что результаты данного анализа поспособствуют формированию необходимой основы для выработки конкретных методологических и нормативных рекомендаций, как на национальном, так и на международном уровнях.

Приоритетные направления развития и использования технологий ИИ определяются в России с учетом национальных целей и стратегических задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 2042 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Названные нормативно-правовые акты подчеркивают колоссальную государственную и общественную важность данной технологии в современной России [2].

Технологии ИИ постепенно охватывают современный мир. Технологии машинного обучения, основанные на обработке беспрецедентных массивов данных, выводят методы анализа информации на совершенно новый уровень, а робототехника выполняет действиями машин те задачи, которые раньше были прерогативой исключительно человека, потенциально делая жизнь людей более комфортной и создавая новые блага.

Закономерно, что технологические инновации, оказывающие такое глобальное воздействие на жизнь современного человека, несут в себе немалые риски. Осознание того, что технологии ИИ являются чрезвычайно сильными инструментами, способными принести обществу как большую пользу, так и серьезный вред, неизбежно приводит к мысли о

необходимости установления системы нормативных правил, принципов и ограничений, связанных с разработкой и применением систем с ИИ.

Феномен стремительного развития и распространения технологий ИИ далеко не всегда получает положительную оценку. С одной стороны, оптимистичный вариант развития ИИ предполагает органичное встраивание робототехнических устройств и сервисов ИИ в жизнь общества. С другой стороны, риски, исходящие от массового применения ИИ, порой рассматриваются как вызовы такого масштаба, который способен создать угрозу для самого существования человечества.

Безусловно, разработчики систем ИИ принимают ряд мер по минимизации рисков использования соответствующих технологий. Однако более глобальные риски социального, экономического и гуманитарного характера, как правило, намного труднее поддаются оценке [5].

Тем не менее представляется возможным выделить основные проблемные зоны индустрии ИИ, имеющие непосредственную связь с правом. Рассмотрим наиболее значимые, на наш взгляд, аспекты теоретических проблем правового регулирования разработки и применения ИИ и смежных технологий, которые обрели актуальность уже сегодня.

Развитие дискуссии о правовых аспектах ИИ и смежных технологий в значительной степени обусловлено ростом внимания к этическим проблемам машинного обучения и робототехники [4].

Само слово «робот» впервые появилось в научно-фантастической пьесе К. Чапека «R.U.R.» 1920 г., одной из центральных тем которой была этика использования мыслящих конструкторов в качестве рабочей силы. Впоследствии главным литературным символом этических аспектов эксплуатации роботов и ИИ стали знаменитые «Три закона робототехники» А. Азимова, впервые сформулированные автором в рассказе «Хоровод» 1942 г.

Сегодня обсуждение этических проблем, связанных с использованием интеллектуальных машин, вышло далеко за пределы научной фантастики и дало необходимую почву для формирования нового исследовательского направления, которое получило название «робоэтика» и стало частью более крупного направления – этики ИИ [1].

В 2004 г. в Италии состоялся Первый Международный симпозиум по робоэтике, после которого в том же году состоялось принятие в Японии Всемирной декларации о роботах. П. Асаро выделяет три составляющие понятия «робоэтика»: встроенные в роботов этические системы; этика людей, которые разрабатывают и используют роботов; этика обращения людей с роботами.

Министерство внутренних дел (МВД) России уже использует информационные системы и программное обеспечение в сочетании с технологией машинного распознавания изображений [3].

Кроме того, эти технологии могут идентифицировать лиц, находящихся в розыске или подозреваемых в совершении преступления, угнанные или подозрительные транспортные средства. Биометрическая система идентификации, разработанная МВД России, позволяет осуществлять поиск с помощью набора информации, содержащей фотографические изображения людей, в том числе: разыскиваемых и пропавших без вести; лиц, содержащихся в информационной системе МВД России.

Следует отметить, что в настоящее время разрабатывается программное обеспечение, которое позволит выявлять перспективные преступления из числа нераскрытых преступлений последних лет с целью их раскрытия. Этот механизм достигается путем создания прогностической модели для выявления преступности на основе наиболее важной информации, содержащейся в статистической таблице.

В качестве инструмента используется открытая библиотека ИИ, разработанная отечественными ИТ-компаниями. Еще одним важным направлением является развитие робототехники, в том числе систем управления наземными и воздушными роботизированными комплексами, а также возможностей беспилотных летательных аппаратов.

МВД России придает большое значение использованию беспилотных летательных аппаратов для поддержки деятельности органов внутренних дел по охране общественного порядка, обеспечению общественной безопасности, борьбе с преступностью, противодействию коррупции, экстремизму и терроризму.

Например, принцип их работы заключается в следующем. Система состоит из двух нейронных сетей. Первый обрабатывает поток изображений с камеры и определяет, есть ли там лицо. Она «вырезает» и «выравнивает» каждого из них. Современные нейронные сети могут просматривать 1 млрд изображений из базы данных менее чем за полсекунды с точностью почти до 100 %.

Второй набор сценариев, использующих системы ИИ, является более обыденным и фактически отражает автоматическое заполнение программных документов на основе содержимого ранее проанализированных документов.

В этом случае могут использоваться системы автозаполнения времени и места (для протоколов), исправления ошибок и стилистических неточностей, транскрибирование устной речи участников следственных действий. В этом случае задачи классификации и прогнозирования ИИ могут быть выполнены. Использование этих систем может предоставить исследователям более точные данные, тем самым повышая скорость и качество принятия решений.

Так, в некоторых частях Китая нашли потенциальных преступников с помощью ИИ до того, как они нарушили закон. Камеры с системами распознавания лиц следят за гражданами и сообщают правоохранительным органам, если в объектив попадает что-то подозрительное.

Например, если кто-то покупает слишком много удобрений за один раз – в конце концов, их можно использовать для подготовки к террористическим атакам. Человека, уличенного в сомнительном поведении, полиция имеет право арестовать или направить на принудительное перевоспитание.

В других странах также пытаются предсказать преступления. В некоторых регионах Соединенных Штатов Америки и Соединенного Королевства Великобритании и Северной Ирландии полиция использует компьютерные системы для определения места возможных инцидентов в ближайшем будущем. Они учитывают множество факторов: криминальную историю региона, его социально-экономический статус и даже прогноз погоды. Удивительно, но с появлением «Оракула» количество перестрелок в районе Чикаго, где он работал, сократилось примерно на треть.

Быстрое развитие и применение новых технологий требует тщательного контроля, особенно в вопросе ответственности. Виновен или не виновен, вот в чем вопрос. В будущем ИИ будет использоваться не только для решения текущих проблем, но и во всем мире, что может существенно повлиять на будущее человечества.

Очевидно, что по мере развития и расширения доступности технологий умного города, датчиков и Интернета вещей ИИ и машинное обучение будут по-прежнему внедряться в правоприменительную практику. Конечно, возможности систем ИИ не ограничиваются этим списком. Такая технология обладает большим потенциалом, в том числе для решения частных и общих задач правоохранительных органов.

Список использованных источников

1. Введенская, Е.В. Актуальные проблемы робоэтики / Е.В. Введенская // Науковедч. исслед. – 2019. – С. 88–101.

2. Караваева, А.В. Некоторые вопросы использования современных технологий в правоохранительной деятельности и предупреждении преступлений / А.В. Караваева // Вестн. Алт. акад. экономики и права. – 2021. – № 5–1. – С. 135–141.

3. Малина, М.А. Цифровизация российского уголовного процесса: искусственный интеллект для следователя или вместо следователя / М.А. Малина // Рос. следователь. – 2021. – № 2. – С. 29–32.

4. Рыжкова, Е.А. Искусственный интеллект как элемент цифрового отношения / Е.А. Рыжкова, Е.К. Рыжкова // Юрид. исслед. – 2022. – № 8. – С. 1–11.

5. Юдина, М.А. Индустрия 4.0: перспективы и вызовы для общества / М.А. Юдина // Гос. упр. Электрон. вестн. – 2017. – № 60. – С. 197–215.

УДК 343.985

С.А. Корнеев, Э.А. Лопатьевская

КИБЕРПРЕСТУПНОСТЬ И НЕКОТОРЫЕ ВОПРОСЫ ПОДГОТОВКИ ЮРИСТОВ

Одной из новых форм транснациональной преступности является киберпреступность. Когда речь заходит о «киберпреступлении» используются разные понятия – «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий» и др. Чаще всего совершаются преступления, связанные с неправомерным использованием персональных данных.

Согласно ст. 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано; предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц; распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц; субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Интернет стал средством обмена информацией по всему миру. Размещая в сети Интернет свою персональную информацию, гражданин может создать условия для совершения в отношении себя киберпреступлений.

Уголовная ответственность за киберпреступления предусмотрена в ряде статей Уголовного кодекса Республики Беларусь: ст. 212 «Хищение имущества путем модификации компьютерной информации»; ст. 349 «Несанкционированный доступ к компьютерной информации»; ст. 350 «Уничтожение, блокирование или модификация компьютерной информации»; ст. 352 «Неправомерное завладение компьютерной информацией»; ст. 354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»; ст. 355 «Нарушение правил эксплуатации компьютерной системы или сети».

В соответствии со ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации; информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Активное использование информационных технологий почти во всех сферах жизнедеятельности предполагает повышение требований к подготовке юристов.

По нашему мнению, в системе подготовки юридических кадров, наряду с необходимостью изучения требований по обеспечению надежности защиты информации на основе технических и программных средств, должны рассматриваться и правовые нормы, направленные на сохранность ведомственной информации и противодействие киберпреступности.

Следовательно, учебный анализ правовых норм должен предшествовать изучению методов по защите информации на основе технических средств и систем и противодействию киберпреступности.

Одним из направлений подготовки специалистов – юристов является включение в учебные программы вопросов по противодействию киберпреступлениям, предусматривающих не только теоретическую, но и практическую подготовку. Отдельные вопросы по противодействию киберпреступности можно включать в программу преддипломной практики.

Считаем также целесообразным вопросы по противодействию киберпреступности предусматривать в программах научно-практических конференций, приводимых на юридических факультетах с участием специалистов в данной сфере.

В заключение отметим, что в современных условиях важен системный, комплексный подход при подготовке специалистов, обладающих навыками по обеспечению сохранности ведомственной информации и противодействию киберпреступности.

УДК 393.985

В.В. Кравец

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Стремительное развитие информационных технологий, их широкая доступность и мгновенная возможность обмена информацией в сети Интернет, преобразует интернет-пространство в мощное оружие, целью которого является воздействие на сознание людей.

В Концепции национальной безопасности Республики Беларусь выделены основные национальные интересы белорусского государства в информационной сфере, которыми являются: «реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации; формирование и поступательное развитие информационного общества; равноправное участие Республики Беларусь в мировых информационных отношениях; преобразование информационной индустрии в экспортно-ориентированный сектор экономики; эффективное информационное обеспечение государственной политики; обеспечение надежности и устойчивости функционирования критически важных объектов информатизации». При этом для обеспечения реализации указанных выше национальных интересов в данной области в первую очередь правоохранительные органы должны обратить внимание на предупреждение распространения в сети Интернет фальсифицированной, недостоверной и запрещенной информации.

В Законе Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации» определен конкретный перечень информации, распространение которой в средствах массовой информации запрещено. Одним из пунктов выделяется запрет распространения «информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к такой деятельности, порнографии, насилия и жестокости, в том числе пропагандирующей или побуждающей к самоубийству, другой информации, распространение которой способно нанести вред национальным интересам Республики Беларусь или запрещено настоящим Законом, иными законодательными актами».

Опыт борьбы с экстремизмом был получен правоохранительными органами в 2020 г., когда экстремистские формирования в различных Telegram-каналах и чатах собирали аудиторию людей, где экстремистская деятельность преподносилась обывателям как законная деятельность. Проблема в первую очередь состояла в том, что простые люди, ввиду удобства использования мессенджера Telegram, очень быстро могли прочесть информацию именно в экстремистских Telegram-каналах, которые, с учетом материальной поддержки из-за рубежа, воздействовали на сознание граждан, и под предлогами «ложного патриотизма», возможности заработать, анонимности и возможности скрыться от правосудия побуждали людей к совершению противоправных деяний. В свою очередь, государственные каналы массовой информации не акцентировали внимание на распространение информации в мессенджере Telegram, а преимущественно использовали традиционные способы распространения информации по телевизионным каналам, размещении на официальном сайте, в газетах и других устоявшихся в нашем обиходе источниках, которые

предоставляют информацию в обусловленное программное время, а преимущество интернет-сообществ и чатов состояло именно в удобстве подачи информации в любое время суток. Экстремистские организации подталкивали людей, проживающих на территории белорусского государства, к активным антиобщественным действиям (забастовки, неповиновение и активное сопротивление сотрудникам милиции, несанкционированные массовые мероприятия и др.).

С помощью разнообразных интернет-ресурсов организованные экстремистские формирования обеспечивают идеологическую подготовку своих пользователей, осуществляют сбор средств и непосредственно подготовку к проведению и совершению преступлений экстремистской направленности. Контент основных интернет-ресурсов, носящий экстремистский характер, отличается продуманной теоретической базой, спектром методов информационно-психологического воздействия на пользователей. Исходя из вышеизложенного, можно сделать вывод: появилась новая форма экстремизма – киберэкстремизм, которая по своей сути никак не отличается от экстремистской деятельности, однако представляет собой новую возможность ее реализации.

Сегодня можно говорить о том, что государственные новостные каналы, а также органы внутренних дел активно используют в своей непосредственной деятельности социальные сети, интернет-сообщества и чаты для проведения активного патриотического воспитания и разоблачения фейковой информации. Осуществляется также оперативное противодействие уже имеющимся экстремистским формированиям, благодаря новой редакции Закона Республики Беларусь «О противодействии экстремизму», вступившей в силу с 16 июня 2021 г., Министерство внутренних дел Республики Беларусь и Комитет государственной безопасности Республики Беларусь имеют право признавать экстремистскими формированиями группы граждан, осуществляющих экстремистскую деятельность, либо оказывающих иное содействие такой деятельности.

Анализ опыта по противодействию киберэкстремизму позволяет сделать вывод о том, что для эффективного противостояния его влиянию необходимы создание и функционирование на постоянной основе популярных, легкодоступных интернет-ресурсов, посредством которых возможен постоянный диалог с людьми, проживающими на территории белорусского государства. На данный момент указанное направление деятельности активно развивается органами внутренних дел, однако стоит открытым вопрос создания заинтересованности и привлечения большего числа пользователей для постоянного ознакомления с предоставляемой информацией.

Таким образом, для непосредственной борьбы с уже функционирующими интернет-ресурсами экстремистского характера необходи-

мо наладить работу по мониторингу интернет-пространства с целью оперативного реагирования на размещаемые материалы, для признания их экстремистскими, разоблачения фейковой информации и, соответственно, привлечению лиц, разместивших данный контент, к установленной законом ответственности. Не следует забывать о необходимости информационно-просветительской работы с населением, в большей степени в среде подрастающего поколения, для популяризации патриотизма, уважения к истории своей страны, веротерпимости и законопослушности.

УДК 343.3

Д.К. Куаныш

ОСОБЕННОСТИ МОШЕННИЧЕСТВА В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одним из современных явлений, которое коренным образом повлияло на развитие глобальных процессов в мировом сообществе, стало интенсивное совершенствование информационно-коммуникационных технологий. Масштаб культурных, социальных, экономических, политических, правовых изменений, вызванных распространением сетевых компьютерных коммуникаций, позволяет многим ученым считать их отражением начала нового этапа в истории человеческой цивилизации. Использование глобальной компьютерной сети Интернет выступает одной из важнейших предпосылок глобализации межгосударственных отношений и построения информационного общества.

Избрав цель занять достойное место среди ведущих стран мира в области развития информационного общества, Республика Казахстан активно развивает собственную информационную и телекоммуникационную инфраструктуру, формирует адекватную политику по обеспечению информационной безопасности.

Киберпреступление – это преступление, совершенное дистанционно в киберпространстве, направленное на причинение вреда охраняемым законом разнородным общественным отношениям, совершаемое с использованием информационно-телекоммуникационных сетей, средств и устройств с доступом в киберпространство. Киберпреступление обязательно обладает такими признаками, как противоправность, общественная опасность, виновность и наказуемость.

Исследование признаков и особенностей киберпреступлений нередко вызывает определенные сложности. Во-первых, это отсутствие в юридической науке и правоприменительной практике устоявшегося терминологического аппарата для данной группы противоправных деяний.

Общественная опасность рассматриваемых уголовных правонарушений заключается прежде всего в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи [1].

Квалификация, раскрытие и расследование уголовных правонарушений в сфере информатизации и связи остается до сих пор нелегкой задачей для сотрудников правоохранительных и специальных органов Республики Казахстан. К причинам подобного рода можно отнести:

отсутствие обобщений следственной и судебной практики;

соответствующих научно обоснованных методических и криминалистических рекомендаций;

специального учебного курса, при подготовке в учебных заведениях системы МВД сотрудников следственно-криминалистической специализации, а также следователей, дознавателей, оперативных сотрудников на курсах повышения квалификации и переподготовки;

достаточной подготовленности сотрудников правоохранительных органов к работе со специфическим видом доказательственной информации, возникающей в результате совершения этих уголовных правонарушений, и рядом других факторов.

Для понимания и уточнения некоторых особенностей исследуемой нами киберпреступности необходимо остановиться на отдельных составах преступлений, где объектом выступают в первую очередь общественные интересы в сфере информационной безопасности.

Объектом уголовного правонарушения, предусмотренного ст. 205 Уголовного кодекса (УК) Республики Казахстан, являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и сетей телекоммуникаций. Предметом рассматриваемого уголовного правонарушения выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе информационная система государственных органов; сеть телекоммуникаций; государственные электронные информационные ресурсы.

Объективная сторона рассматриваемого уголовного правонарушения выражается в неправомерном доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций. Неправомерный доступ к охраняемой

законом информации, содержащейся на электронном носителе, выражается в получении возможности непосредственного завладения этой информацией и может быть осуществлен как с преодолением мер защиты, установленных собственником (владельцем) электронного носителя, так и без такового. Неправомерный доступ к сетям телекоммуникаций выражается в получении возможности непосредственного взаимодействия с входящими в нее информационными системами и их составляющими и осуществляется, как правило, с преодолением мер защиты. Доступ осуществляется только программно-техническими средствами.

Неправомерный доступ без преодоления защиты может осуществляться через компьютер, на котором открыт доступ (сеанс) лицом, имеющим право на это (администратор, пользователь системы и сети). Неправомерный доступ может осуществляться удаленно, в том числе через сеть Интернет.

Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий. Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий. Вредные последствия выражаются в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства. Согласно п. 14 ст. 3 УК Республики Казахстан, в котором дано понятие существенного вреда, здесь следует понимать, в частности:

нарушение конституционных прав и свобод человека и гражданина, прав и законных интересов организаций, охраняемых законом интересов общества и государства;

причинение значительного ущерба (т. е. ущерба на сумму, в сто раз превышающую месячный расчетный показатель);

нарушение нормальной работы организаций или государственных органов [2].

Между неправомерным доступом и наступившими общественно опасными последствиями должна быть установлена причинная связь.

С субъективной стороны рассматриваемое уголовное правонарушение может быть совершено только умышленно (прямой и косвенный умысел): виновный сознает, что он совершает неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникации, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления.

По отношению к причинению существенного вреда в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства возможен косвенный умысел, когда виновное лицо сознательно допускает эти последствия либо относится к их наступлению безразлично.

Мотивы и цели данного уголовного правонарушения разнообразны и на квалификацию не влияют, но они должны учитываться при индивидуализации наказания. В большинстве случаев это корыстный мотив.

В ч. 2 ст. 205 УК Республики Казахстан установлена ответственность за неправомерный доступ к национальному электронному информационному ресурсу или национальной информационной системе.

Национальными признаются информационные системы, состоящие из государственных электронных информационных ресурсов, имеющих важное стратегическое значение для экономики и безопасности государства. В ч. 3 ст. 205 УК Республики Казахстан предусмотрен особо квалифицирующий признак – тяжкие последствия. С учетом положений п. 4 ст. 3 УК Республики Казахстан к тяжким последствиям необходимо относить, в частности: самоубийство потерпевшего (потерпевшей) или его (ее) близкого (близких); причинение крупного или особо крупного ущерба. Эти последствия должны находиться в причинной связи с умышленным неправомерным доступом.

Проведя небольшой анализ ст. 205 УК Республики Казахстан, непосредственно к рассматриваемой нами области исследования, мы отнесли именно совершение неправомерного доступа к информации, в информационную систему или сеть телекоммуникаций именно удаленно, с компьютерного устройства через сеть Интернет, образующим киберпространство.

Во-вторых, затрудняет исследование киберпреступности отсутствие статистического учета преступлений, совершенных в киберпространстве, официальная статистика располагает данными только по перечисленным выше уголовным правонарушениям. Учитывая наш подход к определению киберпреступлений, значительный круг уголовных правонарушений находится в различных главах Особенной части УК Республики Казахстан. Использование информационно-телекоммуникационных сетей, средств и устройств с доступом в киберпространство является квалифицирующим признаком некоторых уголовных правонарушений в разрезе объектов посягательства [1].

Необходимо отметить, что с развитием высоких технологий и расширением сферы их использования, перечень уголовных киберправонарушений может постоянно расширяться, и не всегда уголовное законодательство будет своевременно реагировать на новые угрозы в киберпространстве.

Как правило, киберпреступления различают по своим целям, объектам воздействия, способам и средствам совершения преступного деяния.

В связи с этим имеющиеся проблемы в сфере обеспечения кибербезопасности не могут быть полноценно решены традиционными методами и средствами. Они требуют системного подхода при создании комплексного механизма безопасности, способной противостоять многочисленным киберугрозам. Во-первых, это координация усилий в данном направлении государственных органов, негосударственных структур, бизнеса и общества в целом. Во-вторых, это разработка адекватной системы противодействия киберпреступности, которая включает в себя широкий спектр мероприятий по анализу объективных условий и субъективных обстоятельств, порождающих киберпреступления, механизмов их совершения, способов выявления, пресечения, расследования, опыт судебного рассмотрения.

Список использованных источников

1. Борчашвили, И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (т. 2) / И.Ш. Борчашвили / под общ. ред. Генер. прокурора Респ. Казахстан, Гос. советника юстиции I класса А.К. Даулбаева. – Алматы : Жеті Жарғы, 2015. – С. 1120.

2. Уголовный кодекс Республики Казахстан [Электронный ресурс]. – Режим доступа: http://www.zakon.kz. – Дата доступа: 15.08.2022.

УДК 343

С.В. Кузьменкова

О ПРОТИВОДЕЙСТВИИ ВЫСОКОТЕХНОЛОГИЧНОЙ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Общественная деятельность современного мира характеризуется преобладанием информационных отношений, которые сложно представить без использования современных информационных технологий. Глобальная компьютеризация современного общества приводит к увеличению числа интернет-пользователей, которые не всегда способны удовлетворить свои потребности в силу ряда причин, в том числе и экономического характера, что приводит к увеличению преступности в сети Интернет. Совершение преступлений с использованием цифровых технологий является весьма актуальной проблемой белорусского государства, так как влечет не только появление новых рисков, но и огромную угрозу национальной безопасности. Соответственно, эффективность противостояния данному вызову оказывает непосредственное воздействие не только на защиту прав и интересов граждан, но и на обеспечение информационной безопасности общества и государства в целом.

Несмотря на меры, принимаемые на протяжении последних лет, в Республике Беларусь наблюдается рост количества регистрируемых преступлений в сфере информационных технологий. Так, в 2015 г. было зарегистрировано 2 440 преступлений, 2016 г. – 2 471, 2017 г. – 3 099, 2018 г. – 4 741, 2019 г. – 10 539, в 2020 г. – 25 561. Начиная же с 2021 г. отмечается относительное снижение числа рассматриваемых преступлений (за прошедший год было зарегистрировано 15 503 таких преступлений).

Международный опыт показывает, что для большинства стран мира также свойственно увеличение числа преступлений, совершенных с использованием информационных технологий. Например, на территории Российской Федерации только за последние годы число таких уголовно наказуемых деяний выросло на 73,4 %, а их удельный вес в структуре преступности составил 25 %.

В настоящее время в Республике Беларусь наиболее распространенными в числе рассматриваемых преступлений являются следующие: несанкционированный доступ к компьютерной информации (ст. 349 Уголовного кодекса Республики Беларусь (УК)); разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК), а также хищение путем модификации компьютерной информации (ст. 212 УК).

Целесообразно отметить, что известные методы оплаты в сети Интернет позволяют совершать платежи с помощью введения в компьютерную систему сведений о банковской платежной карточке, а при завладении персональными данными клиента – разрешают открывать и использовать счета. Механизмы завладения указанной информацией весьма разнообразны, что способствует злоумышленникам совершать различные платежи в сети Интернет, а также пользоваться счетами без ведома их владельцев. С целью завладения денежными средствами пользователей злоумышленники также создают и используют всевозможные учетные записи (аккаунт) в социальных сетях и различных мессенджерах.

В свою очередь, совершенно очевидно, что совершение рассматриваемых преступлений обусловливается множеством факторов. Так, несовершенство уголовного законодательства в сфере борьбы с высокотехнологичной преступностью приводит к тому, что до настоящего времени окончательно так и не решен вопрос оценки ущерба от данных преступных посягательств. Кроме этого, в следственно-судебной практике отсутствует единая точка зрения в понимании и применении уголовно-правовых норм правоохранительными органами, что приводит к назначению наказаний, не связанных с лишением свободы, либо прекращению уголовного производства по делу в связи с

деятельным раскаянием лица, примирением сторон и возмещением причиненного ущерба, что в последующем приводит к росту рецидива преступлений.

Полагается, что ряд проблемных вопросов противодействия цифровой преступности в глобальной компьютерной сети Интернет заключается в следующем: недостаточное поступление в правоохранительные органы количества заявлений потерпевших о совершении рассматриваемого вида преступлений; уровень квалификации сотрудников и финансирование подразделений в сфере борьбы с цифровой преступностью требует определенного повышения; отсутствие на законодательном уровне положений, всесторонне рассматривающих порядок расследования данных преступлений и пр.

Таким образом, сегодня перед государством стоит стратегически важная задача, заключающаяся в разработке эффективных способов противодействия высокотехнологичной преступности в сети Интернет.

Применительно к Республике Беларусь особое внимание целесообразно уделять тщательной предварительной подготовке при проведении осмотра места происшествия, обыска или выемки, использованию специальных технических устройств и программного обеспечения, а также принятию мер по обеспечению сохранности компьютерной информации. Например, проведение такого следственного действия, как прослушивание и запись переговоров (ст. 214 Уголовно-процессуального кодекса Республики Беларусь) по уголовным делам, если имеются достаточные основания полагать, что эти переговоры содержат сведения о преступлении, либо имеющие значение для дела, может способствовать установлению мест нахождения используемой компьютерной техники, иных незаконных предметов, документов (в частности электронных).

Кроме того, весьма важно предусмотреть и специальные меры предупреждения преступлений, совершенных с использованием информационных технологий в сети Интернет. К числу данных мер относятся: повсеместное введение и обеспечение достаточной и обязательной идентификации личности пользователя (включая места общественного пользования интернетом); разработка для каждого пользователя сети Интернет программы предоставления электронного сертификата, в котором будут содержаться все сведения, идентифицирующие личность пользователя; введение процедуры заключения в письменном виде договора с провайдером, способствующее предотвращению регистрации неподписанных электронных ящиков.

Однако противодействовать рассматриваемому роду преступности лишь на национальном уровне малоэффективно, так как принцип территориальности практически неприменим к глобальной компьютерной

сети Интернет. В этой связи одним из важнейших вопросов в сфере противодействия преступлениям, совершаемым с использованием цифровых технологий в сети Интернет, является совершенствование международного взаимодействия в сторону его упрощения, что, в свою очередь, окажет положительное влияние, например, на оперативность исполнения запроса о правовой помощи, а соответственно, и на эффективность противодействия вышеуказанной преступности.

Резюмируя изложенное, очевидно, что противодействие высокотехнологичной преступности в сети Интернет является одним из наиболее злободневных вопросов, стоящих перед современным обществом и государством. Совершенствование порядка расследования, сбора и оценки доказательств, повышение уровня научно-методического обеспечения, а также развитие международного сотрудничества является основой противодействия рассматриваемой преступности.

УДК 343.92

В.В. Лавренов, М.А. Лохницкий

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИ ПОСТРОЕНИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

На нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах.

Наблюдается рост преступности с использованием информационно-коммуникационных технологий. Появился новый вид преступности – киберпреступность. Киберпреступность – это любая преступная деятельность, нацеленная на компьютер, компьютерную сеть или подключенное устройство или использующая ее.

Математическое моделирование является одним из новых направлений в борьбе с преступностью, и за последнее время был предложен ряд моделей, в которых используются различные подходы. Они варьируются от моделей на основе метода когнитивного моделирования до дифференциального моделирования.

При применении метода моделирования выделяют пять этапов:

1) создание репрезентативной среды;

2) тестирование, исследование и оценка;

3) обучение и упражнения;

4) анализ и оценка рисков;

5) изучение роли людей в области кибербезопасности.

Существует тесная связь между этими этапами исследований. Создание репрезентативной среды относится к созданию сетей и подключенных систем. Исследования в области кибербезопасности требуют платформы для тестирования. Для реализации сетевой среды моделирования используются библиотеки и инструменты сетевого моделирования с открытым исходным кодом и коммерческие.

Этап тестирования, исследования и оценки подразумевает, что программные сетевые симуляторы и алгоритмы сетевого трафика могут быть использованы для тестирования конкретных типов кибератак. Это практика запуска симулированных кибератак против программного обеспечения с сетевого трафика, чтобы получить представление обо всех возможных уязвимостях, которыми могут воспользоваться настоящие киберпреступники.

Тестирование на проникновение в киберпространство фокусируется на том, как киберпреступник попытается взломать вашу программную систему, от API-интерфейсов до интерфейсных и внутренних серверов, чтобы выявить слабые места в приложении. Выявление этих слабых мест позволит устранить угрозу безопасности и улучшить программное приложение и сетевую инфраструктуру.

На этапе обучения и упражнения предлагается создание специальных подразделений для проведения тренингов и учений по кибербезопасности. Вопросы необходимости обучения кибербезопасности определены в постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» и в ряде других нормативных правовых актов Республики Беларусь.

Основная цель оценки киберрисков – информировать заинтересованные стороны и поддерживать надлежащие меры реагирования на выявленные риски.

Поэтому на этапе анализа и оценки рисков необходимо определить:

наиболее важные критические объекты информационных технологий;

какая утечка данных окажет серьезное влияние на кибербезопасность (будь то вредоносное программное обеспечение, кибератака или человеческая ошибка);

можно ли выявить все источники угроз;

каков уровень потенциального воздействия каждой выявленной угрозы;

каковы внутренние и внешние уязвимости;

каковы последствия использования этих уязвимостей;

какова вероятность эксплуатации;

какие кибератаки, киберугрозы или инциденты безопасности могут повлиять на способность функционирования системы;

какой уровень риска может быть принят.

Если ответить на эти вопросы, то можно определить, что защищать. Это означает, что могут быть разработаны средства управления ИТ-безопасностью и стратегии защиты данных для устранения рисков.

Заключительный этап – изучение роли людей в области кибербезопасности. Люди – злоумышленники, аналитики по кибербезопасности, системные администраторы и обычные пользователи системы взаимодействуют, формируя киберпространство. Поэтому при изучении кибербезопасности необходимо учитывать каждого из них. Злоумышленниками могут быть дети-скриптеры, хакеры, организованные преступные группы, злоумышленники-инсайдеры, любители или террористы. Их роль в киберпространстве определяется их навыками, знаниями, ресурсами, доступом и мотивами. Технологии улучшили защиту киберсистем; однако защита по-прежнему сильно зависит от того, кто управляет системой, и кто имеет к ней доступ.

Таким образом, на современном этапе развития общества в целом возрастает функция математической науки. Методы математического моделирования в русле этой тенденции должны быть ориентированы на решение многообразных задач киберпреступности и кибербезопасности на ближайшее и отдаленное будущее. Для этого математическая наука должна быть обогащена методологическим арсеналом изучения этих проблем. Анализ применяемых методов математического моделирования позволяет сделать обобщающий вывод о том, что эти методы постоянно обогащаются и развиваются. Применение методов математического моделирования позволит решить прикладную задачу по минимизации рисков от угроз и инцидентов в сфере кибербезопасности.

УДК 004:34 (476)

Д.Н. Лахтиков

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная сфера очень сильно эволюционировала, став важной составной частью общества и государства, при этом проблемы криминализации в этой сфере приобрели характер национальных и международных. Преступники используют результаты научного и тех-

нического прогресса в своих целях, что обусловило формирование самостоятельного вида преступлений – киберпреступления.

В настоящее время в белорусском законодательстве в Концепции национальной безопасности Республики Беларусь рост преступности с использованием информационно-коммуникационных технологий определен в качестве внутреннего источника угроз национальной безопасности информационной сфере. При этом в гл. 16 Концепции информационной безопасности Республики Беларусь также подчеркивается, что информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными. В качестве одного из наиболее вероятных источников угроз кибербезопасности рассматривается противоправная деятельность отдельных лиц и преступных групп.

Анализ состояния криминогенной ситуации свидетельствует о том, что по подавляющему большинству преступлений против компьютерной безопасности лица, их совершившие, не установлены. Обусловлено это тем, что преступления данного вида, как правило, носят трансграничный характер и большое количество противоправных деяний совершается с использованием, например, компьютерных систем и интернет-ресурсов, находящихся за пределами страны.

Справедливо отмечает М.А. Простосердов, что в перспективе возможно ожидать дальнейшее нарастание в информационной сфере угроз, как во всем мировом сообществе, так и в отдельном государстве. Недостаточная защищенность информационных ресурсов создает угрозы национальной и международной безопасности в целом, может вести к частичной или полной потере государственного информационного суверенитета. Государство должно быть в состоянии эффективно противостоять им, руководствуясь продуманной комплексной стратегией эффективных скоординированных действий по самым различным направлениям, целенаправленно используя весь имеющийся в его распоряжении арсенал сил и средств, что обусловливает не только определение самих угроз национальной безопасности, но и источников этих угроз.

В свою очередь, киберпреступность в настоящее время является не столько источником угроз информационной безопасности, сколько непосредственно самостоятельной угрозой. Источником угрозы информационной безопасности является фактор или совокупность факторов, способных при определенных условиях привести к возникновению самой угрозы. С одной стороны, преступность как сложное социальное явление детерминируется определенными явлениями, факторами, обстоятельствами, которые, в свою очередь, взаимодействуют друг с другом при активном влиянии самой преступности; с другой – киберпреступления, совершаемые с использованием информационно-коммуникационных технологий, охватывают такие преступления, как, например, преступления против компьютерной безопасности; вымогательство, мошенничество, совершение которых сопряжено с преступлениями против компьютерной безопасности, и др. Подобные преступления характеризуются рядом признаков, среди которых можно выделить следующие: взаимосвязь с другими видами преступности; высокотехнологичный характер (совершение с использованием информационно-коммуникационных технологий, средств компьютерной техники, носителей компьютерной информации, которые выступают орудиями и средствами совершения преступлений); высокая степень латентности, обусловленная различными факторами; трансграничность (позволяет преступнику с территории одного государства совершать преступления в отношении лиц, находящихся в другом государстве); постоянное совершенствование существующих и создание новых информационно-коммуникационных технологий, используемых в качестве орудий и средств совершения преступлений. К таким признакам можно отнести также особые структурные характеристики преступных формирований, дистанционный способ совершения преступлений, связь не только с иными видами преступлений, но и с целым рядом негативных социальных отклонений.

Общественная опасность заключается и в том, что негативные последствия приводят к серьезным финансовым потерям, нарушениям функционирования инфраструктур, реальным жертвам и т. д. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Хотя киберпреступления рассматриваются в качестве новой специфической формы преступлений, они способны причинить вред различным охраняемым уголовным законом общественным отношениям, и это довольно широкая категория, которая охватывает значительный круг разнородных деяний в информационной сфере.

В свою очередь, необходимо отметить, что масштабы киберпреступлений достигли таких размеров, что позволяют называть их на современном этапе самостоятельной угрозой информационной безопасности.

Детерминантами киберпреступлений, как отмечают А.Л. Гогаева, А.С. Лолаева, являются следующие факторы. Возможность извлечения дохода при минимальных затратах и относительно невысоком риске; низкий уровень осведомленности в области информационной безопасности у пользователей систем дистанционного банковского обслуживания и иных средств интернет-платежей; определенная степень ано-

нимности пользователей глобальной компьютерной сети Интернет, существование иных анонимных информационно-телекоммуникационных сетей, таких как сеть Tor и других средств и методов анонимизации пользователей; определенная степень анонимности финансовых операций, проходящих в информационно-телекоммуникационных сетях; наличие программных уязвимостей разного уровня в экономически значимых информационных системах глобальной компьютерной сети Интернет, позволяющих нейтрализовать систему защиты, используя вредоносное программное обеспечение.

Перечисленная совокупность признаков отражает высокую степень общественной опасности данных преступлений и предопределяет потенциальную и реальную возможность нанесения ущерба национальным интересам Республики Беларусь в информационной сфере, т. е. угрозу информационной безопасности.

Таким образом, анализ основных подходов к рассматриваемой проблеме позволяет предложить рассматривать киберпреступность в качестве самостоятельной угрозы информационной безопасности Республики Беларусь. При этом трансформации преступности не только порождают необходимость совершенствования законодательства, но изменения организации и тактики предупреждения, выявления и пресечения киберпреступлений.

УДК 343.2.7

О.О. Лемешевский

О НЕКОТОРЫХ ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СЕТИ ИНТЕРНЕТ

Развитие информационного общества, переход Республики Беларусь к цифровизации, затрагивающей все сферы общественной жизни, неразрывно связанным с усилением значения достоверности информации и культуры общения в сети. В связи с этим появляется большое количество информационных площадок, социальных сетей, форумов, видео- и фотохостингов, обеспечивающих доступ к актуальной информации.

Каждый гражданин Республики Беларусь, в том числе и сотрудники органов внутренних дел, военнослужащие внутренних войск, имеют возможность получать информацию, общаться, обсуждать повестку дня, оставлять комментарии. Следовательно, наличие авторов контента, имеющих умысел доводить недостоверную (часто заранее заготовленную) информацию до своих подписчиков, имеют возможность влиять на эмоциональное состояние людей, их мнение и взгляды на те или иные вопросы.

На данную проблему указал Президент Республики Беларусь Александр Лукашенко 21 сентября 2022 г., принимая с докладом Государственного секретаря Совета Безопасности Республики Беларусь. Он отметил: «Сейчас идет война, прежде всего в сфере информационной безопасности. И здесь подключены должны быть все – от журналиста до Президента. Война войной. Информационная война – это очень опасно в современном мире. Начиная, опять же, от «газеты-районки» и прочей какой-то частной газеты и заканчивая Интернетом. Везде должны активно работать.».

Привлекает внимание в аспекте проблематики нашего исследования положение Концепции национальной безопасности Республики Беларусь, в частности к угрозам национальной безопасности относится «деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам».

Заслуживает внимания в рассматриваемой сфере также Концепция информационной безопасности Республики Беларусь, которая раскрывает такое понятие, как «информационный суверенитет Республики Беларусь».

Информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

Основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

В этой связи следует сделать вывод: лица, которые публикуют на информационных порталах недостоверную информацию или оскорбляют граждан в сети (в частности, сотрудников органов внутренних дел и военнослужащих внутренних войск), нарушают информационный суверенитет Республики Беларусь, угрожают национальным интересам и должны понести весомую ответственность согласно законодательству.

Анализ действующего законодательства Республики Беларусь и правоприменительной практики показывает наличие соответствующих

статей в Уголовном кодексе Республики Беларусь (УК), регламентирующих общественные отношения, касающиеся информационной безопасности, защиты персональных данных, чести и достоинства граждан и вопроса о «фейках» в сети. Приведем их ниже.

Так, в соответствии со ст. 369 «Оскорбление представителя власти» УК предусмотрена уголовная ответственность за оскорбление представителя власти или его близких в связи с выполнением им служебных обязанностей, совершенное в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, размещенной в глобальной компьютерной сети Интернет.

Статьей 391 УК предусмотрено, что оскорбление судьи или народного заседателя в связи с осуществлением ими правосудия наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет.

В соответствии со ст. 19.11 Кодекса Республики Беларусь об административных правонарушениях предусмотрена административная ответственность за распространение информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность, а равно изготовление, хранение либо перевозка с целью распространения такой информационной продукции.

Таким образом, необходимо подчеркнуть, что главным инструментом воздействия на Республику Беларусь является информационно-психологическое воздействие. В этих условиях отсутствие контроля за информационными ресурсами, телеграм-каналами может привести к ложному восприятию информации отдельными гражданами и совершению преступлений. Следовательно, работу по изучению способов ведения информационной войны и совершения киберпреступлений необходимо продолжать. Актуальным остается вопрос о создании военизированных подразделений для противодействия информационным атакам.

УДК 342.732

П.В. Лутович

АКТУАЛЬНЫЕ АСПЕКТЫ РАЗВИТИЯ МЕХАНИЗМОВ ЗАЩИТЫ ГРАЖДАН ПРИ РЕАЛИЗАЦИИ ИМИ ПРАВ И СВОБОД В ИНФОРМАЦИОННОЙ СФЕРЕ

Уровень демократического развития общества определяется не только формальным признанием приоритета прав и свобод человека и

гражданина и их закреплением в национальном законодательстве, но и наличием реальной возможности реализации всего комплекса прав и свобод, гарантированных международными договорами в области прав человека.

Потребности современного общества обусловливают создание эффективно действующего государственно-правового механизма охраны и защиты прав и свобод человека, позволяющий индивиду воспользоваться существующими правовыми и организационными процедурами с целью фактической реализации своих прав и свобод.

Сегодня существующие проблемы защиты прав человека выходят далеко за пределы отдельного государства. Сформировались и получили всеобщее признание международные нормы и принципы в области прав человека, являющиеся стандартом, к достижению которого должны стремиться все государства. Среди основополагающих прав человека ключевую роль в формировании (воспитании) всесторонне развитой личности играет свобода информации, под которой следует понимать группы прав и свобод, включая «свободу выражения убеждений, свободное функционирование средств массовой информации, право общества на получение от государственных служб информации, имеющей общественное значение, свободу распространения информации любым законным способом».

Доступность информации в современных общественных отношениях рассматривается как фактор экономического развития. Особенно это актуально для развивающихся стран, где существуют ограничения по распространению данных в отдельных сферах деятельности. Отсутствие или ограничение предоставления информации создает дополнительные препятствия для функционирования конкурентоспособной экономики, создания эффективного государства и институтов его управления.

Развитие информационных технологий не только облегчают жизнь рядовым гражданам, но и способствуют созданию и производству высокотехнологичных, конкурентоспособных продуктов, пользующихся высоким спросом на международных рынках. Сегодня можно сделать вывод о значительном повышении времени, проводимого различными категориями лиц, в сети Интернет, что объясняется следующим. Современные технологии обеспечивают не только качественное ведение бизнеса, выполнение трудовых обязанностей, но и позволяют эффективно выстраивать коммуникацию.

Вместе с тем в качестве побочного негативного эффекта инновационные процессы способствуют появлению новых угроз противоправного характера, на которые необходимо своевременно реагировать соответствующим правоохранительным органам.

В законодательстве Республики Беларусь имеется ряд нормативных правовых документов, актов, регулирующих отношения, возникающие при использовании информационных ресурсов, включая и интернет-сайты. Так, согласно Указу Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» на государство возложена обязанность обеспечения защиты интересов личности, общества и государства в информационной сфере, а также создание необходимых условий для дальнейшего развития национального сегмента глобальной компьютерной сети Интернет. Подобный подход закреплен и в Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», согласно которому информационная безопасность рассматривается как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

В этой связи Республика Беларусь берет на себя обязательства по обеспечению информационной безопасности, проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности нашему государству, разрабатывает меры, направленные на предотвращение, отражение и нейтрализацию информационных угроз.

Исследование современного состояния правоприменительной практики позволяет сделать вывод о наличии тенденции к увеличению числа зарегистрированных преступлений в сфере высоких технологий. Причины роста носят отчасти организационный характер и обусловливаются многообразием форм возможной противоправной деятельности в сети Интернет, а также непрерывным совершенствованием преступниками новых способов и путей для совершения противоправных деяний.

Резюмируя, отметим необходимость совершенствования существующей системы защиты информационной среды, принятия мер превентивного характера в исследуемой сфере. Это может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами. При этом, разумеется, необходимо соблюдать действующее законодательство, чтобы избежать нарушения личных прав человека и гражданина, гарантированных не только национальными нормативными правовыми актами, но и рядом универсальных международных соглашений.

УДК 343.98.06

П.В. Лутович, Д.Д. Зык

АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Бурное развитие информационных технологий предопределило их использование в преступных целях. Развитие информационных технологий также предопределило использование мер защиты информации от несанкционированного доступа, например, криптографии, используемой различные методы шифрования данных. Для их понимания проведем анализ их развития и внедрения в повседневное пользование.

Симметричное шифрование – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До появления асимметричных шифров (1970-е гг.) выступало единственным криптографическим методом. Однако такие простейшие шифры легко взломать – например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

Асимметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей – открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи представляют собой многорядные числа, связанные между собой определенной функцией.

Электронно-цифровая подпись (ЭЦП) – это последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности. Электронная подпись содержит в себе сведения о владельце сертификата. В ней также может указываться информация о том, когда и во сколько был подписан документ. Чтобы придать юридическую силу документу и доказать момент создания подписи, пользователь обращается к службе штампов времени. Дата и время появляются на документе при подписании электронной подписью в момент, когда программное

обеспечение ЭЦП обращается к службе штампов времени. При этом сохраняется конфиденциальность, так как служба не видит содержимого документа.

Обладая познаниями в данной сфере, злоумышленники могут предпринимать попытки анонимизации и противодействия правоохранительным органам, а также использовать уязвимости мессенджеров, поддерживающих сквозное шифрование с использованием Signal Protocol и XMPP (например, WhatsApp или Viber) для несанкционированного получения доступа к информации. В то же время использование программного обеспечения, обеспечивающее защиту информации методами полного шифрования, существенно затрудняет процесс сбора данных для их использования в качестве доказательств.

При производстве следственных действий могут быть использованы технические средства и способы обнаружения, фиксации и изъятия следов и вещественных доказательств преступления. На текущий момент внедрение дистанционных методов получения компьютерной информации путем доступа к устройствам памяти, установленным на компьютере, является наиболее перспективным.

Представляется целесообразным использовать возможности, предоставленные Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» для получения и исследования зашифрованной информации, имеющей юридическое значение, а также технологическое совершенствование арсенала специальных средств, применяемых оперативными сотрудниками. С учетом активного развития информационно-коммуникационных технологий, их использования в преступных целях, представляется актуальным при проведении криминалистических исследований рассматривать возможность удаленного получения и анализа зашифрованной информации, а также последующего использования результатов ее исследования в уголовном процессе.

УДК 343.985.8

В.Ю. Мезяк

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КРИМИНАЛЬНОГО АНАЛИЗА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Приоритетным направлением служебной деятельности оперативных подразделений органов внутренних дел (ОВД) является выявление, предупреждение и пресечение преступлений. Ключевой составляющей в этой деятельности является «криминальный анализ», который представляет собой деятельность по выяснению и пониманию сущности отношений между криминальными и другими данными, потенциально значимыми для ОВД. Целью криминального анализа является поиск оперативно значимой информации в многочисленном потоке данных, а также использование в борьбе с преступностью.

Научные основы криминального анализа были впервые сформулированы в работе Д. Кеннеди-Коллар «Руководство для детективов», подготовленным в целях оказания помощи в совершенствовании навыков у представителей правоохранительных органов. Автором были представлены и обоснованы следующие типы криминального анализа: криминалистическая картография (Crime Mapping); административный и операционный анализ (Administrative and Operational Analysis); стратегический криминальный анализ (Strategic Crime Analysis); разведывательный анализ (Intelligence Analysis); уголовно-следственный анализ (Criminal Investigative Analysis); географическое профилирование (Geographic Profiling); тактический анализ преступлений (Tactical Crime Analysis).

По мнению автора, под криминальной картографией следует понимать создание визуального представления о характеристике места преступления (нанесение на карту, выполненную в цифровом виде, информации о географическом расположении места происшествия в целях анализа влияния на причины противоправных деяний, окружающей обстановки). Сущность административного анализа заключается в визуализации статистических данных о совершенных преступлениях в определенных местах. Стратегический анализ был представлен аналитической обработкой криминалистической информации, содержащейся в базах данных, для установления моделей деятельности правоохранительных органов и их оценки. Уголовно-следственный анализ предусматривает создание профиля неустановленного преступника для его идентификации либо сужения круга лиц, которые могли быть причастны к совершению преступления. Под географическим профилированием понимается оказание помощи правоохранительным органам в идентификации подозреваемых или сужения круга таких лиц, путем анализа сведений о месте совершения преступления.

С учетом приведенной классификации проводимую в настоящее время информационно-аналитическую работу оперативных подразделений ОВД в определенной степени можно соотнести с криминальным анализом. Вместе с тем нужно отметить, что работа в данном направлении зависит от профессиональных интеллектуальных аналитических качеств оперативного сотрудника в выделении необходимой информации из больших массивов данных, направленных на выявление пре-

ступной деятельности. Криминальный анализ применим при выявлении наркопреступлений, киберпреступлений, коррупционных преступлений, различных хищений и осуществляется на основании сведений, полученных из различных массивов данных (результаты проведенных оперативно-розыскных мероприятий, сведения о телефонных и иных соединениях, информация о перемещении лиц, сведения о движении денежных средств по банковским счетам, сведения Фонда социальной защиты населения и т. п.). Конечной целью криминального анализа является установление признаков противоправной деятельности лиц, представляющих оперативный интерес, их родственных и деловых связях, о связях с иными объектами, перемещениях лиц, хозяйственной деятельности, а также роли каждого внутри определенной системы.

Сегодня ни одно оперативное подразделение ОВД не обходится без аналитической составляющей в деятельности по борьбе с преступностью. Однако конкретные методики по анализу больших массивов данных, полученных из различных источников для выявления признаков преступлений, требуют постоянного совершенствования, а работа в этом направлении в основном базируется на трудоемкой ручной обработке данных с применением своих «специфических» методов анализа, которые в отдельных случаях не имеют системного характера. Применение несистемных методов работы не только затрудняет работу оперативных сотрудников по анализу информации, но и предопределяет их неполноту и фрагментарность. Трудоемкость сбора и анализа информации может вынудить оперативного сотрудника «идти на компромисс», уменьшая объем исходных данных в ущерб качеству исследовании , что не позволяет в полной мере говорить о наличии полноценной системы анализа.

Аналитическая деятельность начинается, как правило, с постановки задачи или выявления проблемы для анализа. Затем осуществляется сбор и анализ информации, относящейся к конкретной тематике. Объектами анализа в первую очередь являются различные противоправные деяния и связанные с ними криминально активные лица. Кроме того, объектами криминального анализа могут быть социальные и экономические процессы, влияющие на оперативную обстановку в рассматриваемой области.

Проведение криминального анализа осуществляется по схеме: «Сбор данных» – «Формирование таблиц» – «Обработка и анализ» – «Выводы и принятие решения». При этом современное распространение информационных технологии меняет парадигму анализа данных, которая должна выглядеть таким образом: «Подключение к массивам данных» – «Структурирование информации и создание баз данных» – «Создание информационной модели обработки и анализа данных, анализ» – «Выводы и принятие решения». Соответственно, для того, чтобы разобраться в этих изменениях, стоит рассмотреть такое направле-

ние информационных технологии , как аналитические системы, предназначенные для интеллектуального анализа данных.

Аналитические системы, как инструменты анализа, сегодня активно применяются в различных сферах, активнее всего в бизнес-аналитике, и позволяют анализировать данные на наличие закономерностей. Наиболее популярными аналитическими системами в настоящее время являются: Microsoft Power BI, OLAP-куб, MS Excel Power Query, Pyramid Analytics, SaaS, Datazen, SAP Lumira, а также отечественные разработки, например, ОАО «Центр банковских технологий» продукт – «Рост-универсальные отчеты».

Комплекс приложений Power BI является системой для анализа и представления информации, которая доступна в том числе в MS Excel и позволяет анализировать большие объемы информации, точнее больше десятка миллионов строк и визуализировать данные.

Аналитическая система Power BI состоит из трех надстроек: Power Query (PQ) – для получения данных, Power Pivot – для связи и анализа данных, Power View – для визуализации, которые повышают удобство бизнес-анализа данных, упрощая их обнаружение, доступ, совместное использование. Для географической визуализации есть Power Maps, она используется реже. PQ является технологией подключения к данным, которая позволяет эффективно, в режиме реального времени, проводить анализ данных с учетом их изменчивости.

Использование PQ оперативным сотрудником открывает возможность в работе с данными, размещенными в разных источниках. Это могут быть базы данных (SQL Server, Access, Oracle, IBM DB2, MySQL, PostgreSQL etc), веб-саи ты (публичные источники данных и корпоративные репозитории данных (встроена поддержка ETL)), файлы Excel (Excel, CSV, XML, текст или папка с метаданными и ссылками), из ряда других источников SharePoint List, OData feed, Active Directory, Facebook etc и др. В сочетании с Power BI PQ объединяет описанные данные из нескольких источников и создает взаимосвязанные массивы данных, позволяющие эти данные эффективно обрабатывать и делать различные вычисления. Кроме того, с использованием PQ имеется возможность анализировать данные, часто требующие выполнения ряда подготовительных действий, в частности фильтрация, сортировка, удаление ненужных сведений, разделение или создание таблиц.

Таким образом, использование аналитических систем в деятельности оперативных подразделений криминальной милиции Республики Беларусь является актуальным и перспективным направлением. Кроме того, деятельность оперативного сотрудника при проведении анализа больших массивов данных можно рассматривать не только как аналитическую работу, но и как целевой сбор и осмысление информации – ее предметное толкование и интерпретацию, нахождение в ней рацио-

нального, позволяющего формулировать предложения, имеющие профессиональную полезность.

Безусловно, криминальный анализ может эффективно дополнить классическую работу по получению информации оперативным путем с целью изобличения преступников. Использование в повседневной работе оперативным сотрудником аналитических систем может решить большое количество задач по анализу данных, что в определенной степени влияет на профессиональные качества оперативных сотрудников в выявлении латентной составляющей конкретных преступлений, а именно: факторов, тенденции , закономерностей, противоречии и т. д.

УДК 34.047

А.А. Мельник

ТЕНДЕНЦИИ РАЗВИТИЯ «НОВЫХ МЕДИА» В БЕЛОРУССКОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ

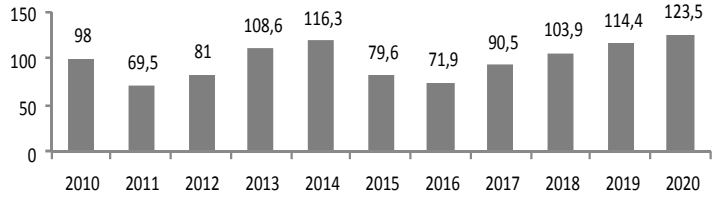
Современное общество характеризуется динамичным развитием масс-медиа, в которых с появлением сети Интернет происходит значительная трансформация. СМИ «печатной эры» мутируют в «новые медиа», продолжая работу в формате веб-сайтов. Социальные средства массовой коммуникации – форумы и блоги, соцсети и мессенджеры, видеохостинги и блогеры, а также множество других видов и форм интернет-ресурсов – создают контент прямо в процессе обмена им, с возможностью участия в этом создании каждого человека.

В 2022 г. Беларусь находилась на 58-м месте в рейтинге ООН готовности государств к электронному правительству, что свидетельствует о сохранении динамичного развития и цифровизации белорусского общества и сферы медиакоммуникации в целом. По данным агентства We are Social на 2022 г., из 9,44 млн жителей нашей страны интернетом пользуются 8,03 млн (85,1 %), что на 3 % больше, чем год назад. За последние десять лет количество интернет-пользователей в Беларуси выросло в два раза, а в 2012 г. их было всего 3,73 млн.

Одной из национальных особенностей Беларуси является высокая доля трафика со стационарных устройств – 57 %, хотя за последние два года она снизилась на 30 %. Мобильный трафик составил 42,04 % и за анализируемый период прибавил 13 %. При этом мобильный трафик заметно изменился – доля устройств Apple продолжает прибавлять в стране, и теперь 22,09 % интернет-потока дают мессенджеры этого бренда, и только 77,54 % составляют устройства, использующие операционную систему Android.

Социальными сетями пользуются 4,35 млн белорусов (46,1 % населения). В 2021 г. эта цифра была меньше – 3,9 млн, или 41 %. Таким образом, за предыдущий год количество пользователей соцсетей увеличилось на 0,45 млн, или 11 %, и, по оценке специалистов, темпы дальнейшего роста будут оставаться высокими.

Развитие рекламного рынка Беларуси.
Объем медиаинвестиций, млн $



Динамика расходов на интернет-рекламу в Беларуси, в млн $

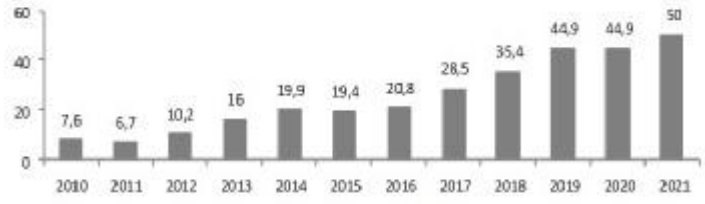


Рис. 1

Активную динамику роста демонстрирует рынок интернет-рекламы в Беларуси, в том числе электронных СМИ и новых медиа (рис. 1). Учитывая специфику аудитории и новые формы взаимодействия в социальных сообществах, значительная роль уделяется особенностям подачи, обработки и интерпретации информации. Анализ динамики рекламного рынка в белорусском сегменте сети Интернет свидетельствует о наличии определенных закономерностей.

Фактически «новые медиа» как элемент интернет-среды представляют важную функцию во всех сферах жизнедеятельности, в том числе и общественно-политической. Так, в период избирательной кампании 2020 г. «новые медиа», в числе которых мессенджер Telegram, играли значительную роль в реализации деструктивного информационного воздействия на органы власти и управления.

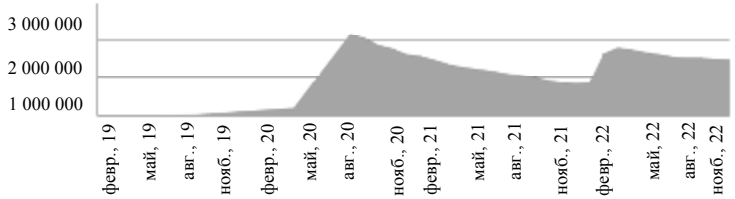
Деструктивное информационное воздействие включало осуществление информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, причинения иного ущерба национальной безопасности.

Анализ статистики посещений деструктивных сайтов показывает, что количество белорусов, пользующихся мессенджером, стало расти с сентября 2017 г. В 2019 г. наблюдался устойчивый рост (в два раза относительно предыдущих лет), который сменился взрывным ростом в марте 2020 г. (рис. 1).

Наш анализ показывает, что Telegram лидировал в наиболее молодой группе пользователей в возрасте 15–24 года: по состоянию на 2019 г., 50 % опрошенных этой возрастной категории пользовались этим мессенджером. Уже в 2019 г. рост популярности Telegram был связан с увеличением числа телеграм-каналов, в первую очередь фиксирующих внимание на общественно-политической повестке, а в 2020 г. они стали еще и средством массовой организации и самоорганизации, в дальнейшем произошел спад внимания пользователей к данной повестке дня (рис. 2, примеры 1 и 2).

На основании данных нашего исследования можно выделить ряд следующих тенденций развития «новых медиа». Рост цифровой грамотности населения, развитие мобильных коммуникаций способствуют распространению смарт-устройств и приложений, способных увеличить интерактивность информационных потоков.

Пример 1. Изменение числа подписчиков одного из деструктивных телеграм-каналов



Пример 2. Изменение числа подписчиков одного из деструктивных телеграм-каналов

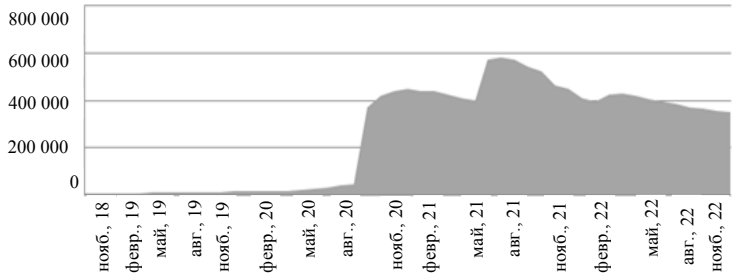


Рис. 2

«Новые медиа» создают технологические условия для развития персонализированного контента для целевой аудитории, они уже способны учитывать форматы подачи информации, вероятно появление новых форм взаимодействия с аудиторией на основе метаданных. Изменяются способы подачи информации «новыми медиа», получают развитие форматы «клипового мышления», при которых человек воспринимает информацию фрагментарно, асинхронно, на коротких интервалах с привлечением ярких образов. С учетом специфики распространения информации в среде «новых медиа», их возможностей по манипулированию, дезорганизации, дезинформации, пропаганде, сложности правового регулирования сохранится их роль как инструмента деструктивного информационного воздействия в условиях гибридных конфликтов.

УДК 004:34

Е.Н. Мисун, А.А. Ластовский

РОЛЬ ПРОФИЛАКТИКИ В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Информационное общество, формируемое сегодня активными способами, представляет собой новый этап развития цивилизации. Повсеместное внедрение и использование компьютерных информационных технологий создает возможности для более эффективного развития экономики, политики и общества в целом. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы

и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства. Глобальное проникновение цифровых технологий во все сферы жизни ставит вопрос о необходимости актуализации существующих механизмов правоохранительной деятельности в сфере противодействия преступности в информационном пространстве.

Республика Беларусь, как и все мировое сообщество, ориентирована на развитие и популяризацию безналичных расчетов, сопровождающихся увеличением количества устройств, ростом числа пользователей электронных платежных систем и сети Интернет. Повсеместное и нарастающее использование различных форм дистанционного обслуживания рассматривается одной из основных причин значительного количества регистрируемых киберпреступлений, а ключевым моментом их совершения – недостаточная информационная грамотность населения.

В этой связи актуальным направлением в противодействии киберпреступности рассматривается полноценное и всеобъемлющее использование профилактического инструментария. Этот тезис также был озвучен заместителем Министра внутренних дел – начальником криминальной милиции генерал-майором милиции Г.А. Казакевичем. Так, в мае 2022 г. на заседании Брестского облисполкома он заявил, что, несмотря на положительную динамику снижения количества хищений посредством модификации компьютерной информации, поводов для самоуспокоения нет, поскольку структура преступности меняется. Больше стало преступлений, связанных с применением методов социальной инженерии, направленных на отдельные категории граждан, как правило, социально не защищенные (пенсионеры и одиноко проживающие люди, которые не владеют компьютерной грамотностью). Руководитель отметил, что профилактика подобного вида правонарушений – задача не только милиции, но и местной власти, образования, здравоохранения, социальных служб.

Данное мнение полностью коррелирует с основополагающим нормативным правовым актом в сфере обеспечения информационной безопасности. Так, в соответствии со ст. 76 Концепции информационной безопасности Республики Беларусь одним из приоритетных направлений деятельности уполномоченных государственных органов является профилактика киберпреступности, основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в СМИ и сети Интернет в целях формирования безопасной национальной информационной экосистемы.

В качестве примера такой работы можно отметить комплекс профилактических мероприятий, проводимых Министерством внутренних

дел (МВД) Республики Беларусь на протяжении двух последних лет, – декаду кибербезопасности (далее – Декада). Инициаторами проведения данной акции выступило руководство главного управления по противодействию киберпреступности и управления информации и общественных связей МВД Республики Беларусь. Основание для этого – возрастающие информационные риски для населения и экспоненциальный рост киберпреступности.

Проведению каждой Декады предшествовал продолжительный организационный этап. К проведению Декады подготовили документы, разъяснили цели и задачи территориальным подразделениям, достигали договоренности о привлечении к проведению мероприятий заинтересованные государственные органы и др. Основными мероприятиями в ходе проведения Декад являлись выступления в трудовых коллективах и учреждениях образования, а также выступления в средствах массовой информации.

Особого внимания заслуживает практический опыт проведения Декады «Киберкидз» с 23 мая по 1 июня 2022 г. Ее главной целью стало обучение основам безопасного поведения в цифровой среде во время летних каникул учащихся, их родителей, педагогического состава учреждений образования. Проведена широкомасштабная работа по доведению профилактической информации до населения посредством средств массовой информации (выступления на телеканалах «Беларусь-1», «ОНТ», «СТВ», на интернет-портале «Спутник», на радиостанциях «Сталіца», «Мир», «Альфа Радио»). Всего было проведено свыше 9 тыс. выступлений в средствах массовой информации, большая часть из которых пришлась на интернет-выступления (7,8 тыс.). Территориальными органами внутренних дел в соответствии с компетенцией активно был задействован весь допустимый ресурс ведомств и организаций для распространения в подростковой среде информации о мерах по соблюдению цифровой гигиены. Информационно-профилактическая работа активно осуществлялась сотрудниками органов внутренних дел в трудовых коллективах (5,6 тыс. выступлений) и учреждениях образования (4 тыс.).

Пристальное внимание было уделено распространению наглядной агитации, размещаемой в местах массового присутствия граждан в самых посещаемых объектах транспортной инфраструктуры и социального назначения. Информационные материалы в массовом порядке звучали из радиоприемников, транслировались на мониторах в торговых объектах и автозаправках, в общественном транспорте и объектах транспортной инфраструктуры.

Активно проводились встречи с обучающимися и профессорско-преподавательским составом учреждений высшего образования, при-

чем как в формате реального присутствия, так и в режиме онлайн-конференций. Главная их цель – в преддверии летних каникул довести до обучающихся основные виды киберугроз и меры по защите от них.

В целом проведение указанного комплекса профилактических мероприятий позволило достичь поставленных целей, всесторонне и качественно довести необходимую информацию до населения (в особенности до молодежи). С высокой степенью эффективности были задействованы заинтересованные государственные органы и организации, предприятия, социальная, транспортная и спортивная инфраструктура, мобильные операторы сотовой связи.

Как свидетельствует статистика, проведение данных широкомасштабных профилактических мероприятий весьма существенным образом сказываются на формировании положительной динамики в противодействии киберпреступности. Массированным информированием граждан всеми доступными способами о самых актуальных способах хищений денежных средств правоохранительные органы достигают главной цели: обеспечение превентивной самозащиты населения от преступных киберпосягательств. Вместе с тем важнейшее значение в противодействии киберпреступности имеет консолидация и партнерские отношения между правоохранительными органами, организациями государственного и частного секторов, образовательными и научными учреждениями.

Таким образом, профилактическая работа, направленная на правовое просвещение населения, и впредь должна носить системный характер с привлечением всех заинтересованных структур органов государственного управления.

УДК 343.9.01

И.С. Митряев

ВЛИЯНИЕ КИБЕРПРОСТРАНСТВЕННОЙ АНОНИМНОСТИ НА МОТИВАЦИЮ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ IT-ТЕХНОЛОГИЙ

Совершенствование информационных систем упрощает доступ к информации, предлагает ее разновидности. В то время как безопасность личных данных подвергается высокому риску, анонимность, невидимость и сокрытие следов преступления становятся большой проблемой в сфере интернет-отношений между людьми.

Киберпреступность во многом отличается от традиционных преступлений, в том числе универсальностью и сложностью, в частности

анонимностью, сокрытием и незаметностью. Анонимность киберпространства делает отслеживание личности серьезной проблемой, которая создает препятствия для обнаружения и расследования.

Анонимизация киберпространства делает отождествление личности глобальной проблемой, которая создает препятствия для расследования данного рода преступлений и поимки преступников.

Киберанонимность оказывает влияние на преступную мотивацию и явление виктимизации, которое представляет из себя процесс или конечный результат превращения в жертву преступного посягательства лица или группы лиц, поэтому решать эту задачу необходимо на разных уровнях, включая технологии и правоохранительные органы.

Анонимное общение – отличительная особенность интернет-пространства. При использовании интернета анонимность может сохраняться от начала до конца. Но при этом данный тип общения может нести достаточно серьезную угрозу конфиденциальности личных данных пользователей, организаций. Интернет повсюду. Но достаточно часто его используют в торговых центрах, ресторанах, барах, аэропортах и т. п. Из-за особенности распространения интернета злоумышленники часто пользуются этим, взламывая средства связи обычных пользователей, которые подключены к одной общественной сети.

Существуют специальные программы и сервисы, которые позволяют полностью сохранить свою анонимность в сети Интернет. Этот механизм затрудняет установление личности пользователя. Ведь посредником может являться программа. Но вполне реально отследить данный путь посредством следования процессам прямо противоположным передачам.

Анонимное подключение представляет собой фундаментальное субъективное право, необходимое каждому посетителю интернета. В определенных случаях это отдельные компьютерные сети, созданные для достижения анонимности в сети Интернет. Особенность таких сетей в том, что они сочетают в себе определенную степень защищенности пользователя, легкость использования и наличие «прозрачности» для конечного пользователя.

Наиболее известным примером программ для обеспечения анонимности является браузер Tor и VPN, что позволяет добиться полной анонимности в сети Интернет. Следует отметить, что использование данных программ законодательно не регламентируется, то пользоваться такими программами может любой желающий.

Статистика о количестве киберпреступлений в России за 2021 г. говорит о 518 тыс. киберпреступлений, что на 1,4 % больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 г. В частности,

количество заявлений о мошенничестве (хищение с обманом жертвы) выросло на 5,1 %, превысив 249 тыс. Однако количество заявлений о возбуждении уголовных дел в связи с компьютерными преступлениями со взломом сократилось на 10,6 %, до 157 тыс. Около четверти преступлений было связано с другими составами, в том числе незаконной организацией и проведением азартных игр. Эксперты оценили ущерб России от действий хакеров в 150 млрд р. по итогам 2021 г. В интернете имеется также статистика о распространении киберугроз по всему миру. Согласно данной информации Россия стала лидером по объему теневых операций с криптовалютой.

В мировой практике право на соблюдение конфиденциальной информации стало неотъемлемой частью процесса реализации основополагающих прав человека в период активного развития различного рода компьютерных технологий, прежде всего – право на конфиденциальность приватной жизни, право на свободу выражения собственного мнения. Данные аспекты затрудняют законодательное ограничение использования программ, скрывающих или шифрующих настоящую личность пользователей. В этом состоит парадокс. Так как в современном мире «право на анонимность» прямо не указано ни в одном акте международного характера, который подлежит обязательному исполнению странами. Встречаются лишь рекомендации независимых международных организаций и стейкхолдеров (это физическое либо юридическое лицо, которое прямо или косвенно воздействует на работу организации или располагает определенными ожиданиями от результатов ее деятельности), и большинство процессов опираются на судебную практику.

Например, в Соединенных Штатах Америки в первой поправке к Конституции 1787 г. закреплено право на высказывание мнения анонимно, а фундаментальная необходимость в защите этого права была признана Верховным судом США.

Однако в России некоторые правоотношения по этому поводу регулируются. Например, в 2014 г. российское законодательство затронуло анонимные платежи. В соответствии с Федеральным законом Российской Федерации от 5 мая 2014 г. № 110 «О внесении изменений в отдельные законодательные акты Российской Федерации» максимальная планка анонимных интернет-платежей стала 15 000 р., что позволило сократить объем транзакций, проводимых киберпреступниками.

Но даже некоторые ограничения не повлияли на распространение киберугроз. В 2022 г. появилась информация об утечке личных данных пользователей из сервиса «Яндекс.Еда». В эти данные входили Ф.И.О. заказчиков еды, их адрес проживания, вплоть до квартиры, номер их телефона, сумму которую они потратили за полгода. Как следствие – сервис оштрафовали лишь на 50 000 тыс. р., что невероятно мало за такую утечку информации.

Количество киберпреступлений и преступников неизбежно будет увеличиваться. Дешевая составляющая киберпреступлений и сложность обнаружения и сбора доказательств создают стимулы для потенциальных преступников. Виртуальный интеллект, транстерриториальность и высокий уровень латентности киберпреступлений затрудняют обнаружение и расследование случаев. С другой точки зрения, киберпреступность превосходит нынешние возможности государственных органов по контролю за правопорядком. Риски и затраты в киберпреступности ниже, чем в традиционной преступности, а выгода выше. Эта рентабельность еще больше укрепляет намерения преступника совершить киберпреступление.

Подводя итог вышеизложенному, можно отметить, что киберанонимность оказывает большое влияние на возникновение киберпреступлений, в основном снижая потенциальную вероятность обнаружения и, следовательно, связанные с этим затраты. На самом деле, анонимность может в какой-то степени побудить потенциальных преступников пойти на риск. Огромной проблемой является также то, что отсутствует нормативная база, которая следит и регулирует деятельность людей в интернете. Это приводит к увеличению количества киберпреступлений, ведь преступники могут руководствоваться тем, что если законодатель четко не определил рамки дозволенного в киберпространстве, то они могут делать что и как угодно. Следовательно, необходимо создать полную нормативную базу, которая затрагивала бы все сферы интернет-отношений, устанавливала бы юридическую ответственность за интернет-мошенничество, нелегальный спам, кражу криптовалюты и т. п.

УДК 343.97

А.В. Морозов

АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ПРОФИЛАКТИКИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Наиболее проблематичным в современном мире считается именно сложность того, что в действительности достаточно тяжело не только отклонить существующие угрозы различного уровня, но даже предотвратить их в информационной области. И это глобальная проблема XXI в. не только на национальном, но и на международном уровне.

Под национальной и информационной безопасностью следует понимать базовые определения складывающихся современных общественных отношений не только на внутригосударственном уровне, но и на международном.

Сегодня киберпреступность, которая, по сути, перестала иметь уже государственные границы в рамках конкретного государства, является реальной угрозой первостепенной важности, которая направлена прежде всего на урегулирование вопросов национальных интересов и безопасности в рамках взаимодействия различных государств. Но в существующих условиях взаимодействия мировое информационное пространство не может не являться ареной для конфликтных ситуаций разных государств, юридических и физических лиц.

В научном сообществе киберпреступления, в широком смысле, обозначены как общественно опасные деяния, посягающие, помимо компьютерных систем, на иные объекты, к основным из которых относятся: национальная и мировая безопасность (кибертерроризм), имущество, имущественные права индивидов и их коллективных образований (это и кражи, и мошенничество, совершенные посредством компьютерных систем или в киберпространстве, а также посягательства на авторские права (плагиат и киберпиратство), на личную безопасность (явления кибербуллинга и секстинга, груминга и троллинга) и пр. [1, с. 6].

Цифровую грамотность можно определить как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктах и услугах, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

В Указе Президента Республики Беларусь от 29 июля 2021 г. № 292 «Об утверждении программы социально-экономического развития Республики Беларусь на 2021–2025 годы» определена цифровая трансформация белорусского государства. Инструментом выполнения поставленных задач станет реализация Государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы, иных государственных программ и программ социально-экономического развития административно-территориальных единиц, региональных комплексов мероприятий в части мероприятий в сфере информатизации.

В свою очередь, например, в 2022 г. в Российской Федерации уже запущена долгосрочная программа повышения цифровой грамотности жителей страны. В рамках данной программы будут созданы новые образовательные сервисы для различных групп граждан, в том числе для студентов, пенсионеров и детей.

Представляется необходимым с учетом имеющегося российского опыта принятие Государственной программы Республики Беларусь «Цифровая грамотность», поскольку на сегодня личная цифровая грамотность становится важным условием работы в онлайн-среде.

Прежде всего необходимо определить и законодательно закрепить понятие «цифровая грамотность». В связи с чем предлагается определить «цифровую грамотность населения» как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктах и услугах, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

Недостаточность законодательства, регулирующего борьбу с преступлениями в сети Интернет, отвечающего современным потребностям правоприменения, не позволяет объективно оценивать масштабы киберпреступности, связанной с новыми коммуникационными технологиями.

Помимо несовершенной законодательной основы противодействия киберпреступности одной из основных проблем является недостаточность компетентных лиц, выявляющих и предотвращающих киберпреступления. Часто осведомленность преступников в сети Интернет превышает осведомленность сотрудников правоохранительных органов [2, с. 142].

Деятельность государственных органов по предупреждению преступлений, совершаемых в сфере цифровой экономики, должна носить многоуровневый характер и учитывать проблемы квалификации таких преступных посягательств. Во-первых, необходимо научное обеспечение деятельности по предупреждению преступности, т. е. использование результатов научно-исследовательской работы в правоприменительной практике. Во-вторых, целесообразно методическое обеспечение деятельности по предупреждению преступности, состоящее в совершенствовании подзаконных актов, которые способствуют оперативному реагированию на ситуации совершения преступлений в сфере цифровой экономики и эффективному применению законодательных актов. В-третьих, необходимо принятие организационно-управленческих мер, состоящих в подготовке сотрудников правоохранительных органов и в переходе от территориального принципа их работы к функциональному.

Таким образом, целесообразно определить и законодательно закрепить понятие «цифровая грамотность», дополнив Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» статьей, определяющей понятие «цифровая

грамотность», определив ее как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктов и услуг, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

Считаем целесообразным с учетом имеющегося российского опыта принятие Государственной программы Республики Беларусь «Цифровая грамотность», поскольку на сегодня личная цифровая грамотность становится важным условием работы в онлайн-среде. Посещение небезопасных сайтов, невозможность распознать откровенно мошеннические действия и фейковую информацию в сети Интернет приносят серьезные неприятности пользователю и тем самым создают дополнительную нагрузку на правоохранительные органы.

Список использованных источников

1. Абламейко, М.С. Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика : автореф. дис… канд. юрид. наук : 12.00.14 / М.С. Абламейко ; Белорус. гос. ун-т. – Минск, 2012. – 28 с.

2. Жуков, А.З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права / А.З. Жуков // Проблемы экономики и юрид. практики. – 2019. – № 4. – С. 141–143.

УДК 343

Р.Р. Насыров

О ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ

Информационные технологии внедряются во все сферы жизни человека, и преступная сфера не является исключением. Информационно-телекоммуникационная сеть Интернет и информационные технологии позволили наркобизнесу выйти на новый уровень и привлечь внимание огромного количества людей.

Информационно-телекоммуникационные технологии на современном этапе развития активно способствуют развитию и модернизации наркосети, посредством которой осуществляется розничная и оптовая продажа наркотических средств, психотропных веществ и их аналогов. К тому же преступный элемент постоянно повышает меры конспирации, зашифрованность электронных терминалов и сетевых ресурсов, которые служат для перевода денежных средств за наркотики. К наиболее распространенным интернет-площадкам и мессенджерам относятся DarkNet, LegalRC, Iklad, DarkWeb, AlphaBay Market, Daffy Duck, Silkkitie, AS, Lambo, Ramp, Dream Market, Silk Road, Hansa, BigRC.biz, Telegram.

Рассматривая маркетплейсы в теневом сегменте сети Интернет, стоит отметить, что на них перевод денежных средств между продавцом и покупателем допускается посредством платежных систем (например, Яндекс.Деньги, Qiwi, WebMoney и др). Как правило, в Qiwi открывается несколько счетов, на которых аккумулируются денежные средства. Впоследствии данные счета используются для проведения финансовых операций по приобретению различных криптовалютных форм в рублевом эквиваленте на Ethereum, Биткоин, Monero, Litecoin, Zcash, Ripple, Dash. Криптовалюта активно используется лицами, осуществляющими незаконную продажу наркотиков в теневом сегменте сети Интернет. Она обладает огромными преимуществами, так как под ней понимаются виртуальные денежные средства, не имеющие материального выражения и физической формы. Тем самым для криптовалюты характерен уровень анонимности, независимость от национальной валюты, защищенность, необратимость операций, автономность и условность.

Ко всему этому в противодействии криптовалютной наркоторговле большое значение приобретает проблема отсутствия у сотрудников правоохранительных органов необходимых знаний, касающихся криптовалюты и работы с ней. На практике возникает немало вопросов обнаружения и изъятия виртуальных цифровых денежных средств. Именно поэтому важно повышать знания и подготовку сотрудников в области информационных технологий и программирования. Следствием вышеуказанных проблем является отсутствие зарегистрированных случаев изъятия криптовалюты в качестве нелегального дохода от сбыта запрещенных в гражданском обороте средств и веществ.

В Стратегии Государственной антинаркотической политики Российской Федерации на период до 2030 года указано, что возникновение новых и модернизация уже имеющихся способов совершения преступлений организованными группами с использованием инновационных коммуникационных технологий и сетей выступает одной из самых злободневных угроз национальной безопасности в сфере контроля и противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов (Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года».

В научных трудах рассматривается и анализируется точка зрения, которая предполагает внедрение и последующее использование современных технологий интеллектуального анализа в разработке информационно-аналитических сетей, позволяющие осуществить высокоэффективный мониторинг информационно-телекоммуникационной сети Интернет по вопросам наркоситуации в Российской Федерации и выдвижении методик борьбы с данными видами преступлений.

О подобной практике, которая успешно используется в зарубежных странах, пишет И.А. Завьялов в статье «Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений». Так, например, ученые Американского Корнеллского университета в 2017 г. создали программную систему искусственного интеллекта, которая позволяет по публикациям, лайкам и аккаунтам пользователей всемирной сети Интернет установить наличие у них склонности к потреблению алкогольных напитков, табачных изделий, а также наркотических средств, психотропных веществ и их аналогов. Благодаря применению данной системы уже имеются положительные опыты выявления наркозависимых лиц и предупреждения незаконному обороту наркотиков. Следовательно, создание и применение систематизированного механизма нейросетевых технологий позволит правоохранительным органам оперативно и эффективно осуществлять установление даркнет-маркетплейсов и наркомаркетов по продаже наркотиков в сети Интернет. К тому же, это будет способствовать повышению результативности противодействия незаконному обороту наркотических средств и понижению уровня наркотизации населения.

УДК 343

И.С. Нестер

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Современный этап развития общественных отношений характеризуется активным научно-техническим прогрессом, скорость которого постоянно возрастает. Еще 20 лет назад мы вели речь о таком понятии, как «компьютеризация», а сегодня это считается обыденностью.

В настоящий момент на первый план выходит цифровизация, которая представляет собой внедрение цифровых технологий в различные сферы деятельности человека: образование, промышленность, наука, искусство, спорт и т. д. Само понятие цифровизации рассматривается

преимущественно в контексте экономического развития государства, служит своеобразным «драйвером», позволяет ускорить производственные процессы, снизить себестоимость продукции. Тем не менее в последнее время появилось достаточно большое количество научных публикаций о внедрении цифровых технологий в иные сферы, например, образование, здравоохранение и т. д.

В сложившейся ситуации все чаще звучат слова о внедрении цифровых технологий в правоохранительную деятельность. Несмотря на то что методы, используемые для защиты прав и свобод граждан, носят достаточно специфический, иногда карательный характер и не всегда позволяют применять передовые цифровые технологии в полной мере, их проникновение в данную деятельность не остается незамеченным.

Цифровизация правоохранительной деятельности не носит массовый, повсеместный, необдуманный характер. Внедрению современных цифровых технологий предшествует глубокий анализ, в процессе которого определяется множество их особенностей и характерных черт: эффективность технологии, возможность и необходимость ее внедрения, совместимость продукта с уже внедренными достижениями науки и техники, возможность обучения сотрудников правоохранительных органов использованию данных технологий и многое другое. Именно по этой причине уже внедренные средства цифровизации демонстрируют достаточно высокий результат, доказывают тем самым свою эффективность. Примечательным остается тот факт, что правоохранительные органы не останавливаются на достигнутом, анализ новых технологий по обозначенным критериям происходит на постоянной основе.

Ярким примером цифровизации в правоохранительной сфере является внедрение биометрических паспортов. Этот документ позволяет гражданину выполнять отдельные операции (открыть или закрыть банковский счет, покупать товары, оплачивать услуги, получать информацию, содержащую персональные данные в госорганах и многое другое) без непосредственного посещения соответствующего учреждения, т. е. удаленно. При этом идентификация гражданина происходит одновременно несколькими алгоритмами (отпечатки пальцев, распознавание голоса, изображение лица и т. д.). Одновременно с предоставлением гражданам широкого перечня возможностей реализации своих прав, биометрические документы упрощают идентификацию человека.

Немаловажное значение имеет работа правоохранительных органов с гражданами, организациями, общественными объединениями в рамках реализации принципа открытости в своей деятельности. Например, сайт Министерства внутренних дел Республики Беларусь содержит наиболее актуальную информацию о работе данного органа исполнительной власти, позволяет своевременно получать достоверные сведения об измене-

нии законодательства и многое другое. Постоянно набирает популярность возможность осуществления административных процедур в рамках функционирования общегосударственной автоматизированной информационной системы.

Система внутреннего функционирования правоохранительной сферы также подвержена цифровизации. Оптимизации уровня документооборота способствует ведомственная система электронного документооборота «Дело», позволяющая распространять информацию от вышестоящего органа всем подчиненным подразделениям, а также осуществляющая передачу информации в любые министерства или ведомства. Основными достоинствами данной системы является оперативность при передаче информации, возможность ее обработки, систематизации, хранения и поиска. Тем не менее реализация работы в рамках системы «Дело» все еще имеет нерешенные вопросы. Несмотря на наличие правовой базы, регулирующей работу в данной системе, каждое ведомство имеет свои ведомственные приказы, часто противоречащие друг другу и не позволяющие в отдельных случаях использовать возможности «Дела» в полной степени. Нередко отдельные ведомства требуют от своих подразделений дублировать информацию, получаемую с помощью обозначенной системы электронного документооборота в печатном виде, что никак не способствует снижению документооборота и приравнивает возможность системы к обыкновенной электронной почте. Обозначенные проблемные вопросы требуют решения в части создания единого методического обеспечения функционирования системы электронного документооборота.

Сотрудники правоохранительных органов отмечают наличие и иных недостатков, среди которых следует выделить: недостаточную оснащенность современной компьютерной техникой (особенно на уровне местных территориальных органов), недостаточную пропускную способность локальных сетей, несовершенство программного обеспечения, ненадежность оборудования, отсутствие долгосрочной технической поддержки со стороны разработчиков и т. д.

Стремится к повышению уровня цифровизации и служебная деятельность правоохранительных органов. Здесь можно выделить создание и функционирование ведомственной локальной сети, автоматизацию ведения оперативно-справочных, оперативно-розыскных и криминалистических учетов, использование возможностей мессенджеров с функцией видеозвонков. Цифровизации также подвержены научно-технические средства, применяемые для проведения оперативно-розыскных мероприятий. Далеко не первый год ведутся дискуссии о необходимости внедрения электронного уголовно-процессуального судопроизводства. Приведенный нами перечень не является исчерпывающим, поскольку, как нами ранее было обозначено, цифровизация является постоянным и непрерывным процессом.

Таким образом, анализируя применение современных информационных технологий в деятельности правоохранительных органов, можно выделить основные направления внедрения цифровизации в обозначенной сфере. Данными направлениями является: внешняя деятельность ведомства, направленная на предоставление гражданам своевременной и достоверной информации; межведомственное взаимодействие; служебная и профессиональная деятельность.

УДК 343.9

К.А. Новакова

ПОДПИСЬ, ВЫПОЛНЕННАЯ НА ПЛАНШЕТЕ, КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Подпись является одним из наиболее распространенных объектов почерковедческого исследования, так как она является обязательным реквизитом документа и, выполняя удостоверительную функцию, придает ему юридическую силу. С развитием технологий в различных сферах нашей жизни стали появляться новые способы придания документу юридической силы, например, выполнение подписи в электронном документе при помощи дигитайзеров. Такая возможность предусмотрена рядом нормативных актов, определяющих правила использования электронной подписи, к которой законодателем отнесены подписи, выполненные на некоторых планшетах [1].

Электронная подпись, выполненная собственноручно, может быть воспроизведена на графических планшетах нескольких видов, которые условно можно разделить:

на бытового назначения;

профессионального назначения;

специализированные.

Бытовые и профессиональные графические планшеты представляют собой устройство для ввода информации, созданной от руки, непосредственно в компьютер. Состоит из пера (стилуса) и плоского планшета, чувствительного к нажатию или близости пера.

Графические планшеты применяются как для создания изображений на компьютере способом, максимально приближенным к тому, как создаются изображения на бумаге. Кроме того, их удобно использовать для переноса (отрисовки) уже готовых изображений в компьютер.

Специализированные планшеты имеют существенное различие от бытовых и профессиональных, заключающееся в способности первых регистрировать дополнительные параметры, которые сохраняются в подписанном документе, и в случае необходимости могут быть использованы для идентификации лица не только по традиционным признакам почерка, но и по ряду биометрических показателей. Данные параметры строго регламентированы Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ (в ред. от 14 июля 2022 г.) «Об электронной подписи». Подписи, полученные на технических устройствах, не соответствующих данному регламенту, не имеют юридической силы и не могут выполнять удостоверительную функцию в официальных документах.

В настоящее время специализированные графические планшеты могут регистрировать и сохранять как основные почерковые признаки подписи, так и следующие биометрические данные:

сила нажатия пера;

угол наклона пера;

ускорения/замедления темпа движений;

регистрация точек начала и окончания движения;

вибрации;

временные интервалы между касаниями.

Исходя из вышеизложенного, можно сделать вывод, что существенное различие между планшетами бытового, профессионального назначения и специализированными графическими планшетами заключается в способности последних регистрировать дополнительные параметры, которые необходимы для идентификации лица не только по традиционным признакам почерка, но и по ряду биометрических показателей, которые строго регламентированы законодательством. Само изображение подписи и те параметры, которые сохраняют специализированные графические планшеты, делают возможным решение диагностических и идентификационных задач экспертом-почерковедом как самостоятельно, так и совместно со специалистом по компьютерно-технической экспертизе.

Подписи, выполненные с применением дигитайзеров, стали неотъемлемой частью окружающего материального мира благодаря стремительному развитию современных технологий. При этом непривычный пишущий прибор и материал письма оказывают специфическое влияние на проявление как диагностических, так и идентификационных признаков подписного почерка исполнителя, определяя тем самым необходимость разработки методики криминалистического исследования подобных объектов [2–4].

Анализируя вышеизложенное, можно сделать вывод, что, во-первых, далеко не всегда использование каких-либо технических средств является признаком подделки рукописных реквизитов документа, в связи с чем остро возникает проблема исследования таких подписей и решения вопроса о способе их выполнения. Во-вторых, в системе объектов криминалистического исследования появляется новый вид объектов – это подписи, выполненные на планшетах (дигитайзерах). Однако в настоящее время в специальной литературе отсутствуют какие-либо сведения о специфике выполнения таких подписей и, соответственно, об особенностях их исследования в рамках почерковедческой экспертизы.

Появление новых форм реализации подписи в удостоверительных целях, к которым относится выполнение подписи с помощью дигитайзеров, требует внимания со стороны правоохранительных органов, их глубокого изучения и разработки новейших методик исследования таких объектов для профилактики и пресечения преступлений. Готовность к решению различного рода задач по данному виду объектов экспертно-криминалистическими подразделениями во многом зависит от информирования, наличия методик и обучения экспертов-криминалистов в образовательных организациях.

Список использованных источников

1. Об электронной подписи [Электронный ресурс] : Федер. закон Рос. Федерации, 6 апр. 2011 г., № 63-ФЗ : (в ред. от 14.07.2022 г.). – Режим доступа: http://www.consultant.ru. – Дата доступа: 25.10.2022.

2. Бодров, Н.Ф. Современные возможности распознавания технического воспроизведения подписи [Электронный ресурс] / Н.Ф. Бодров // Актуальные проблемы российского права. – 2011. – № 2. – URL: https://cyberleninka.ru/article/n/sovremennye-vozmozhnosti-raspoznavaniya-tehnicheskogo-vosproizvedeniya-podpisi (дата обращения: 25.10.2022).

3. Шлыков, Д.А. Установление фактов нерукописного воспроизведения почерковых объектов: современное состояние и перспективы развития [Электронный ресурс] / Д.А. Шлыков // Научно-практический журнал «Энциклопедия судебной экспертизы». – М., 2017. – URL: http://www.proexpertizu.ru/theory_ and_practice/ ted/756/ (дата обращения: 25.10.2022).

4. Торопова, М.В. Значение комплексного судебно-почерковедческого и судебно-технического исследования документов в современных условиях развития цифровых технологий печати / М.В. Торопова // Теория и практика судебной экспертизы в современных условиях : материалы 2-й Междунар. науч.-практ. конф. – М., 2009. – С. 401–405.

УДК 343.98

С.В. Петлицкий

ИНСТИТУТ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Государственный комитет судебных экспертиз Республики Беларусь (ГКСЭ) в соответствии с возложенными на него задачами проводит судебные экспертизы по материалам заявлений (сообщений) о преступлениях, уголовным делам, реализует мероприятия по поддержанию на надлежащем уровне качества и своевременности проведения экспертных исследований, ведет криминалистические учеты и коллекции, осуществляет другие функции в сфере судебно-экспертной деятельности (СЭД).

Наряду с этим, сотрудники ГКСЭ участвуют в следственных и процессуальных действиях, оперативно-розыскных мероприятиях, выполняя функции специалиста. Сегодня в Республике Беларусь технико-криминалистическая деятельность продолжает вносить огромный вклад в работу правоохранительных органов по раскрытию и расследованию преступлений. Как показывает практика, специалистам (криминалистам) приходится работать на местах происшествий по различным категориям и видам дел. Порой ими устанавливаются обстоятельства, существенно отличающиеся от первичной информации, поступившей в орган уголовного преследования. Поэтому сложно заранее предугадать, с каким преступлением, способом его совершения придется столкнуться лицу, осуществляющему экспертно-криминалистическую деятельность (ЭКД) в дежурные сутки.

Особенно, на наш взгляд, это актуально в современных условиях, когда последним приходится иметь дело с высокотехнологичной преступностью и на этом же уровне обеспечивать реализацию специальных знаний и профессиональных навыков в борьбе с ней. Осознавая всю сложность противодействия преступности в киберпространстве, ГКСЭ активно ведет подготовку и повышает на постоянной основе квалификацию судебных экспертов, основной деятельностью которых является проведение компьютерно-технических и иных экспертиз, связанных с исследованием цифровых носителей информации. Общая штатная численность таких сотрудников относительно невелика, но их значение для СЭД и правоохранительной деятельности в целом трудно переоценить.

Анализ правоприменительной деятельности по преступлениям в сфере высоких технологий показал, что в большинстве случаев использование специальных знаний и научно-технических возможностей таких экспертов осуществляется на последующем этапе их предварительного расследования. В то же время на первоначальном этапе основное внимание уделяется деятельности следователя по проведению им осмотра и изъятию цифрового носителя информации, на котором сохранились так называемые компьютерные улики. Для этих целей последние могут привлекать дежурных специалистов ГКСЭ, обладающих универсальной экспертно-криминалистической подготовкой.

Однако, даже несмотря на это, эффективность первоначального этапа, который, отметим, предопределяет результативность последующего, напрямую зависит от уровня знаний и подготовки следователя или лица, осуществляющего ЭКД, в области IT-технологий и информационной безопасности. Из-за непонимания сути происходящих процессов в цифровом пространстве реальная следовая картина преступления может быть искажена или не в полной мере отражена в протоколе следственного действия.

Как верно в своих трудах отметил А.Ф. Волынский: «цифровизация, будучи социальным явлением и длящимся во времени процессом, предполагает формирование высокотехнологичной системы реализации норм права и положений обширного круга наук. Для создания такой системы необходимы не ситуативное формальное взаимодействие между учеными-правоведами и представителями таких научных сфер, как прикладная математика, информатика, кибернетика, а их совместная деятельность, результаты которой могут использоваться в подготовке кадров для нужд правоохранительных органов страны в борьбе с киберпреступностью».

Другими словами, организация раскрытия и расследования высокотехнологичных преступлений проявляется через широкое использование цифровых средств фиксации, сохранения, автоматизированной обработки и исследования доказательственной и ориентирующей информации, а также через новые виды криминалистически значимой информации, фиксируемой в компьютерных средствах, системах, сетях. Для формирования новых инновационных профессиональных компетенций при подготовке следователей или специалистов необходима интеграция юридических знаний и знаний в области IT-технологий.

Как нам представляется, одной из перспективных возможностей адекватного ответа правоохранительных служб на современные вызовы такой преступности является повсеместная специализация следователей, оперативных сотрудников и, конечно же, судебных экспертов, выполняющих в дежурные сутки функции специалиста. Внедрение такой специализации в работу отечественных субъектов раскрытия и расследования преступлений должно сопровождаться, во-первых, со-

ответствующей правовой регламентацией, во-вторых предусматривать первоначальную профильную подготовку.

В этой связи представляется интересной позиция Е.Р. Россинской, которая в курс такой подготовки современного следователя или специалиста включает изучение следующих базовых направлений: 1) общие принципы работы компьютерных устройств, осведомленность об основных компонентах и их функциях; наиболее распространенные виды вычислительных устройств: компьютеры, мобильные и игровые устройства, «умные» вещи (IoT), серверы; 2) общие принципы устройства электронных носителей информации, их виды, а также осведомленность о способах хранения информации, например, на сервере в RAID-массиве, на «облаках» и пр.; 3) общее понятие о файловой системе как средстве для хранения и поиска данных; 4) принципы построения локальных сетей, понимание того, как устроена сеть Интернет (на аппаратном уровне передачи сетевого трафика и общее понимание сетевых протоколов); 5) общее понимание задач информационной безопасности как состояния защищенности компьютерной информации, таких ее свойств, как конфиденциальность, целостность, доступность, подлинность, подотчетность, безотказность и достоверность способов, методов ее обеспечения.

Исходя из вышеизложенного, на наш взгляд, заслуживает внимания опыт Следственного комитета Российской Федерации, где сохранился институт следователей-криминалистов и их специализированная подготовка. Находясь непосредственно в штатной численности следственных подразделений, они обеспечивают комплексное, системное технико-криминалистическое сопровождение расследования преступлений. При этом такие участники уголовного процесса не озадачены проведением каких-либо экспертиз, что позволяет использовать их потенциал в организации раскрытия и расследования сложных «цифровых преступлений». Несмотря на то что их деятельность, пока не нашла своего детального отражения в Уголовно-процессуальном кодексе Российской Федерации, их навыки могут положительно использоваться в отечественной следственно-экспертной практике по организации борьбы с киберпреступностью.

В заключение подчеркнем, что СЭД и ЭКД – как автономные, но взаимосвязанные виды деятельности во многом определяют эффективность всей организации раскрытия и расследования преступлений. Их развитие и совершенствование – задача государственной важности, а потому качественное ее решение не может быть обеспечено на узковедомственном (моносистемном) уровне.

УДК 343.985

А.А. Петрович

ПОВЫШЕННАЯ ЛАТЕНТНОСТЬ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С каждым днем растет количество разнообразной информации о лицах, организациях и событиях, распространение которой третьим лицам, в зависимости от ее использования, может повлечь негативные последствия, в том числе общественно опасные последствия, предусмотренные Уголовным кодексом Республики Беларусь.

В результате развития информационной сферы любого государства, в том числе и Республики Беларусь, количество преступлений, совершенных в сфере информационной безопасности, растет волнообразно. Данное явление обусловлено самим процессом развития, в результате которого введение новых информационных технологий, переход тех или иных правоотношений в информационное пространство порождает возможность использования благ в корыстных, преступных и иных целях. Снижение же роста преступлений в данной сфере обусловлено совершенствованием введенных информационных технологий, организационными мероприятиями, снижающими виктимность пользователей, а также профилактическими мероприятиями.

При этом все больше электронных устройств, имеющих в своей структуре накопители информации и управляемые операционными системами различных видов, задействованы в общественных отношениях и хранят данные ограниченного распространения (персональные данные, сведения, относящиеся к коммерческой тайне, результаты работы специалистов в сфере проектирования, разработки в различных сферах, сведения о банковских реквизитах, контактных данных организаций и лиц и др.). Помимо этого, для повышения эффективности работы юридического лица указанные устройства часто подключены к локальным сетям, а они в последующем подключены к сети Интернет. Данный фактор существенно ускоряет обмен информацией и в целом повышает эффективность работы, но и порождает риски хищения информации или иных противоправных действий. Описанные выше устройства чаще всего становятся целью злоумышленников, так как главная цель злоумышленника – это завладение данными для последующего их использования или сбыта.

Одним из способов атаки подобных устройств является применение вредоносного программного обеспечения. При этом даже сам факт

разработки, распространения, использования и согласно уголовному законодательству Республики Беларусь является уголовно наказуемым деянием независимо от наступивших последствий. Однако количество преступлений, совершенных с использованием вредоносного программного обеспечения в общем числе преступлений в сфере противодействия киберпреступности невелико. Связано это в первую очередь с трудоемкостью изготовления качественного вредоносного программного обеспечения, а также с высоким уровнем латентности данного вида преступлений. Помимо этого, в настоящее время в процедуре проведения проверки, проводимой по сообщениям и заявлениям о преступлениях и уголовным делам, расследуемым по признакам состава преступлений, предусмотренных ст. 212 и гл. 31 Уголовного кодекса Республики Беларусь, совершение которых сопряжено с использованием вредоносного программного обеспечения, имеются отдельные правовые и процессуальные проблемы.

Латентность данного вида преступлений обусловлена в первую очередь неочевидностью наступления последствий в результате совершения преступлений с использованием вредоносного программного обеспечения. Чаще всего пострадавшие не осознают происходящего заражения устройств и утечки данных, а последующее использование похищенных данных часто не позволяет связать его с предшествующим хищением данных. Таким образом, совершенное преступление остается безнаказанным и при этом влияет на формирование волн новых преступлений других видов (мошенничеств, хищений денежных средств путем модификации компьютерной информации, вымогательств и др.). Ввиду большого количества информационных систем потенциально подверженных угрозам со стороны злоумышленника, использующего вредоносное программное обеспечение, находящихся во владении частных лиц и организаций, необходимо осуществление дополнительного контроля за соблюдением организациями, работающими с персональными данными, реквизитами банковских платежных карточек и счетов и иными критически важными данными, Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» и приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных».

Второй и наиболее важный проблемный вопрос касается процесса проведения исследований для выявления вредоносного программного обеспечения. Современная практика сложилась таким образом, что оперативный сотрудник или следователь при выбытии на место происшествия по сообщению или заявлению о преступлении производит

осмотр места происшествия и в случае выявления достаточных данных о заражении устройства осуществляет изъятие накопителей информации устройства и в последующем направление их в Государственный комитет судебных экспертиз для проведения компьютерно-технической экспертизы. При этом заключение эксперта не позволяет дать ответ на вопрос о наличии или отсутствии вредоносного программного обеспечения. Экспертиза предоставляет лишь информацию о том, определяется ли тот или иной файл, хранящийся на исследуемом объекте антивирусным программным средством как вредоносное программное обеспечение. Получение данной информации не требует специальных познаний, и она может быть получена в ходе проведения осмотра компьютерной информации. Ввиду чего полноценное исследование вредоносного программного обеспечения не производится. К тому же отсутствие программы в базе данных вирусных сигнатур может привести к отрицательному ответу при даче оценки программному продукту как вредоносному, что в последующем приведет к принятию незаконного решения по материалу проверки или уголовному делу. При проведении полного исследования вредоносного программного обеспечения, с процессом изучения его возможностей, возможно установление принципа работы исследуемого программного продукта, способа внедрения, результата работы. В случае использования программного средства с целью хищения данных возможно установление данных об узле получателя данных. Вся эта информация окажет существенную помощь в раскрытии подобного вида преступлений. Следовательно, необходимо совершенствование системы экспертного исследования вредоносного программного средства.

УДК 343.985

А.А. Петрович, Д.Н. Лахтиков

ТЕХНОЛОГИЯ BIG DATA И СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ЕЕ ПРИМЕНЕНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

За последние несколько десятков лет объемы цифровых данных в мировой цифровой сфере растут в геометрической прогрессии. Сегодня количество информации, хранящейся на устройствах пользователей, серверах различных ресурсов и иных материальных носителях цифровой информации исчисляется в зеттабайтах. Это связано с неуклонно растущей ролью сети Интернет и цифрового пространства в

повседневной жизни современного человека, повсеместным внедрением облачных технологий, подразумевающих распределенное хранение данных и осуществление удаленного доступа к ним. Это обусловлено также постоянным совершенствованием технологий удаленной передачи данных и в целом развития сферы информатизации, порождающей новые виды цифровой информации, объем и разнообразие которых создают определенные сложности их обработки. Все эти факторы привели к появлению такого явления, как большие данные.

Термин «большие данные» до настоящего времени окончательно не сформировался в научной литературе. Его понимание лежит в области возникших на современном этапе развития проблем, связанных с обработкой информации. Сегодня принято определять термин «большие данные» исходя из основных характеристик цифровых данных:

большого объема;

разнообразия данных;

высокой скорости их изменения.

Однако такой подход является отчасти не полным и в большей степени унифицированным для понимания. Технология «Большие данные» имеет большое разнообразие вариантов применения, реализации и решаемых задач. Однако все варианты реализации включают в себя помимо самих данных и их характеристик еще два ключевых аспекта: технологии хранения данных и их анализа. В целом все указанные аспекты являются взаимосвязанными элементами технологии и напрямую влияют на ее возможности и эффективность.

К технологиям анализа следует отнести большой спектр технологий осуществления автоматизированной обработки данных. Основными перспективными направлениями в данной сфере являются: машинное обучение, статистический анализ и поиск аномалий.

Исходя из вышеназванных аспектов технологии «Большие данные», необходимо сделать вывод, что под данным термином следует понимать взаимосвязанную систему технологий хранения, структурирования и анализа большего объема цифровых данных, направленную на получение определенного результата.

К преимуществам технологии «Большие данные» относится возможность решения разнообразных задач анализа данных, обширный сектор сбора информации, относительная автономность и высокая скорость обработки данных. К недостаткам рассматриваемой технологии можно отнести высокую стоимость необходимого оборудования, а также необходимость в высококвалифицированном персонале обслуживания.

Сфера применения технологии «Большие данные» весьма разнообразна с учетом постоянно развивающего информационного простран-

ства. Рассматриваемая технология используется в медицине, генетике, метеорологии и иных направлениях, в том числе и в сфере правоохранительной деятельности.

Растущее внедрение информационных технологий во все сферы жизни также способствовало появлению различных схем совершения преступлений, с использованием так называемых фишинговых ссылок. Данные преступления чаще всего совершаются с использованием созданных злоумышленником поддельных интернет-страниц проверенных сервисов, внешне неотличимых от официальных ресурсов. В настоящее время такое направление особенно актуально ввиду невозможности постоянного мониторинга сети Интернет с целью выявления поддельных интернет-ресурсов и их оперативного блокирования с целью пресечения совершения преступлений в отношении граждан. Возможности технологии «Большие данные» с применением машинного обучения позволяют осуществлять постоянный мониторинг сети Интернет на предмет выявления поддельных ресурсов и подготовку оперативного решения о принятии мер по блокировке указанного ресурса. В перспективе имеется возможность автоматизации данного процесса от момента сбора информации до блокировки ресурса. Помимо этого, такое направление применения технологии «Большие данные» дает возможность осуществления операций мониторинга сети Интернет на предмет содержания ресурсами деструктивной информации, запрещенной законодательными актами государства к распространению, и принятия дальнейших решений в отношении указанного ресурса.

Учитывая, что в современной жизни каждый человек оставляет множество следов своего присутствия в сети Интернет, а объем и разнообразие подлежащих к анализу данных для выявления этих следов невообразимо огромны, методы ручного сбора информации о лице в интернете становятся слишком продолжительными. Существующие же технические решения не позволяют осуществить достаточно полный и глубокий анализ информации о лице. В связи с этими трудностями применение технологии «Большие данные» приобретает актуальность и в данной сфере и позволит деанонимизировать лицо, совершившее преступление.

Одним из наиболее значимых направлений правоохранительной деятельности является профилактика преступлений и правонарушений. Данное направление неразрывно связано с анализом и прогнозированием криминогенной обстановки. Работа по формированию эффективной организации деятельности органов внутренних дел на территории обслуживания с учетом криминогенной обстановки является одним из важнейших критериев, способствующих снижению уровня преступности в любом государстве. Постоянные процессы урбаниза-

ции и изменения обстановки в зависимости от огромного множества факторов, а также отсутствие возможности ее глобального отслеживания в режиме реального времени не позволяет эффективно принимать меры контроля оперативной обстановки на обслуживаемой территории. При этом при проведении анализа оперативной обстановки не всегда в полной мере возможно охватить все факторы ее формирования и изменения. Часто не учитываются социальные процессы в обществе, современные тенденции и экономическое состояние определенной территории. Технология «Большие данные», в зависимости от ее реализации, способна в режиме реального времени собирать и анализировать информацию о текущей обстановке на территории обслуживания органа внутренних дел и подготавливать оперативные прогнозы изменения криминогенной обстановки.

Таким образом, основным преимуществом использования рассматриваемой технологии в правоохранительной деятельности является формирование оперативного прогнозирования, способного оказать помощь сотрудникам органов внутренних дел в реагировании на формирующиеся изменения, касающиеся предупреждения, выявления и пресечения преступлений.

УДК 343.3

В.И. Пикта

НЕКОТОРЫЕ АСПЕКТЫ РАСПРОСТРАНЕНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Обеспечение защищенности информационных систем является одним из самых важных аспектов обеспечения информационной и национальной безопасности. Информация, в нынешних реалиях, является самым ценным объектом, который требует особого режима защиты. В таких условиях широкое распространение информации как ресурса послужило появлению вредоносного программного обеспечения, основной целью которого является компрометация информации и информационных систем.

Вредоносное программное обеспечение – это любое программное обеспечение, которое негативным образом влияет на работу персонального компьютера или радиоэлектронного устройства. Вредоносное программное обеспечение может быть представлено в виде всплывающего окна, которое не позволяет пользователю получить доступ к основному функционалу интернет-ресурса или к программному обеспечению, копирующему финансовую информацию с компьютера жертвы.

Согласно исследованиям «Лаборатории Касперского» в последние годы число новых семейств и разновидностей вредоносного программного обеспечения стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Под угрозой находятся как домашние пользователи, так и крупные компании, банки, критическая инфраструктура, государственные организации, промышленные предприятия, использующие автоматизированные системы управления технологическими процессами.

Среди огромного ландшафта угроз в сфере распространения вредоносного программного обеспечения одним из лидеров выступают программы-вымогатели (шифровальщики). Данная угроза свойственна всем сферам функционирования информационных систем государственного и частного сектора. По статистическим сведениям, за 2021 г. мировой ущерб от распространения программ-вымогателей составляет около 20 млрд долл. США в связи с выплатой выкупов вымогателям и простоями.

Программа-вымогатель (от англ. ransomware – компиляция слов ransom – выкуп и software – программное обеспечение) является разновидностью вредоносного программного обеспечения, предназначенного для блокирования доступа к компьютерным системам или предотвращения считывания компьютерной информации (преимущественно с использованием методов шифрования), после чего от жертвы за дешифрование информации требуется выплатить денежные средства.

В научной литературе программы-вымогатели определяются как тип вредоносного программного обеспечения, которое поражает компьютерные системы, ограничивая доступ пользователей к данным, хранящимся в скомпрометированных системах. Восстановление измененной информации является трудоемким процессом, и многие жертвы выплачивают выкуп в целях получения ключей дешифрования. Однако выплата выкупа не гарантирует, что файлы будут дешифрованы или программа-вымогатель будет отключена или удалена для предотвращения повторения заражения информационных систем в будущем.

Угрозы, исходящие от программ-вымогателей, зависят от типа вируса, вследствие чего представляется возможным выделить две основные категории указанных программ: программы-блокировщики и программы-шифровальщики.

Программа-блокировщик – тип программ-вымогателей, предназначение которых блокировать работу персонального компьютера или мобильного устройства, с целью последующего требования выкупа. В отличие от программ-шифровальщиков, блокировщик не шифрует компьютерную информацию, а блокирует доступ к основному функционалу компьютерной системы. Предметом посягательства данного ви-

да программ-вымогателей может выступать как устройство в целом, так и отдельное программное обеспечение, например, веб-браузер.

Программа-шифровальщик – тип программ-вымогателей, которая модифицирует пользовательские данные, путем использования различных алгоритмов и техник шифрования. После кодирования информации вредоносное программное обеспечение инициирует подключение к удаленному рабочему столу и пересылает информацию об идентификаторе зашифрованного устройства, для последующего восстановления модифицированной компьютерной информации.

Указанные типы вредоносного программного обеспечения могут распространяться по следующим векторам: перенаправление трафика; вложения электронной почты; ботнеты.

Перенаправление трафика. Данный вектор является наиболее распространенным способом побудить пользователя перейти по ссылке на вредоносную рекламу или перенаправить веб-трафик пользователя на другой интернет-ресурс, на котором размещено вредоносное программное обеспечение в виде набора различных эксплоитов. Чаще всего это встречается на интернет-ресурсах с порнографическим содержимым, пользователя с указанных сайтов перенаправляют на портал, предлагающий бесплатные игры или обновления для пользовательских приложений. При загрузке указанного контента вредоносное программное обеспечение использует уязвимости устройства пользователя, что приводит к блокировке либо шифрованию пользовательской информации.

Вложения электронной почты. Электронные письма с вложениями или ссылками побуждают пользователей открывать и получать доступ к веб-ресурсам, содержащим программу-вымогатель. На первый взгляд жертве кажется, что электронное письмо отправлено подлинным корреспондентом, так как вложения могут содержать электронный счет за потребляемую электроэнергию, налоговую или юридическую документацию, или даже содержат информацию от лиц, ищущих работу с просьбой открыть вложение или перейти по ссылке, чтобы актуализировать информацию о пользователе.

Ботнеты. В последние годы особую популярность приобрел данный вид вредоносного программного обеспечения, так злоумышленники стремятся взять под контроль миллионы устройств по всему миру и таким образом управлять огромной сетью устройств, которые можно использовать для осуществления атак типа «отказ в обслуживании» (DDoS), тем самым блокируют доступ к информационным системам. Распространяется данный вид вредоносного программного обеспечения при помощи загрузчиков путем компрометации пользовательских компьютерных систем и сетей, после чего загружается вредоносное программное обеспечение в качестве второго шага. Загрузчики пред-

ставляют собой легальное программное обеспечение, такое как бесплатные игры и инструменты, которые не содержат вредоносного кода, а загружает его позже.

В данной ситуации для получения необходимой информации о распространителе вредоносного программного обеспечения важно проанализировать данные, хранящиеся в журналах обращений к сетевому оборудованию, либо оперативного взаимодействия с организациями, представляющими услуги в качестве хостинг- и интернет-провайдера.

Данный перечень угроз не является исчерпывающим. Преступность не ограничивается существующими решениями, а постоянно совершенствует инструменты для проведения кибератак с целью компрометации компьютерных систем и сетей.

Подводя итог изложенному, важно особо отметить необходимость в разработке научно-методических и научно-практических рекомендаций для сотрудников правоохранительных органов по грамотному и эффективному извлечению следов активности программ-вымогателей, и сохранению данных следов для последующего изучения и использования в суде в качестве доказательства.

УДК 343.985.8

С.В. Пилюшин

О НЕКОТОРЫХ ПРОБЛЕМАХ МЕТОДОЛОГИИ КАТЕГОРИАЛЬНО ПОНЯТИЙНОГО АППАРАТА АНАЛИТИКИ В СИСТЕМЕ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Изменения, происшедшие за последние годы в социальной, экономической жизни общества, законодательстве, возникновение новых форм проявления преступности, в том числе основывающихся на использовании информационных технологий, оказывают существенное влияние на процессы принятия управленческих решений, постоянное усложнение которых объективно требует максимального включения в оперативно-розыскную практику современного аналитического инструментария, формирования и развития аналитических компетенций.

Очевидно, что в сложившихся условиях борьбы с преступностью назрела необходимость глубокого понимания и осмысления сущностного содержания аналитики как особого вида деятельности, обоснования используемой в процессе выявления и раскрытия преступлений ее определенной модели конкретными оперативными подразделениями.

Применительно к деятельности оперативных подразделений органов внутренних дел категория «аналитика» характеризуется следующими понятиями и терминами: «аналитическая работа»; «аналитическая деятельность»; «информационно-аналитическая деятельность»; «инициативная аналитика»; «оперативно-розыскная аналитика»; «аналитическая разведка»; «аналитический поиск»; «оперативно-розыскной мониторинг»; «управленческое решение»; «аналитическое решение» и др.

Наиболее распространенными являются представления об аналитике как об элементе получения знания, как творческой деятельности, как виде специфической деятельности. В основном в научных публикациях аналитика отождествляется с категориями «информационно-аналитическая деятельность» или «аналитическая работа», которыми принято определять разновидность деятельности сотрудников оперативных подразделений, направленной на получение нового знания об объектах, представляющих оперативный интерес, путем анализа разобщенных сведений.

Несмотря на то что основные концептуальные положения аналитической работы (информационно-аналитической деятельности) в сфере оперативно-розыскной деятельности принято считать устоявшимися, проведенный анализ содержания научных трудов, показал разобщенность трактовок отдельных категорий и понятийных характеристик, используемых при описании аналитических процессов, связанных с получением, анализом, накоплением оперативно-розыскной информации, принятием на ее основе управленческих решений.

Так, например, деятельность сотрудников оперативных подразделений, связанная с поиском и предварительной аналитической обработкой добытой информации, в научной литературе определяется терминами «аналитический поиск» либо «аналитическая разведка». Вместе с тем в одних случаях «разведка» отождествляется с «поиском», в других – рассматривается в качестве его разновидности. Однако веских аргументов, на основании которых представляется возможным сделать однозначные выводы о синонимичности данных терминов либо усмотреть в их содержании наличие существенных различий, в большинстве случаев не приводится.

В том числе, результаты научных исследований практики применения сотрудниками оперативных подразделений методик сбора и аналитической обработки информации, с использованием возможностей информационных технологий, показывают, что «аналитическая разведка», в свою очередь, дублируется целым рядом сходных по содержанию терминов. Фактически речь идет о «компьютерной разведке», «компьютерном поиске», «компьютерном мониторинге», «киберразведке», а также «аналитической разведке средствами Интернет», «оперативно-розыскном мониторинге информационных ресурсах глобальных компьютерных сетей», «информационно-аналитической работе в Интернете» и др.

Безусловно, введенные в научный оборот новые понятия и термины расширяют теоретические представления о рассматриваемом виде деятельности, отражают уровень знания об объектах и явлениях объективной реальности, выступают средством их дальнейшего углубленного познания. Вместе с тем их избыточность, собственно говоря, интерпретация однотипных по содержанию действий, не только не способствует формализации знаний, но и может ввести в заблуждение относительно верного восприятия содержания тех или иных процессов.

Таким образом, категория «аналитика» в деятельности оперативных подразделений характеризуется достаточно широким перечнем понятий и терминов, преимущественно определяющих ее как специфический вид проводимой работы, сопряженной с процессами поиска и обработки добытых сведений, извлечением новых знаний, принятием на их основе оптимальных управленческих решений.

В разрезе существующих в настоящее время научных представлений о сущности и содержании аналитических процессов, полагаем, что ряд разработанных научных понятий и терминов требует более тщательной научной разработки, апробирования, что позволит их отличать друг от друга, исключить дублирование, разобщенность трактовок.

УДК 343.985

Ю.В. Полковниченко

О СЛЕДОВОЙ КАРТИНЕ В ХОДЕ ОСМОТРА КОМПЬЮТЕРНОЙ ТЕХНИКИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ ОБ УБИЙСТВАХ

Одним из первых табу во всех источниках моральных норм человека является запрет на убийство человека. Во всех странах мира убийство законодательно признано наиболее тяжким преступлением, в связи с чем охрана права человека на жизнь является одной из важнейших норм уголовного законодательства и одной из важнейших задач правоохранительного блока любого государства. Процесс сбора доказательств по рассматриваемой категории преступлений, по своей сути, является классическим и представляет собой совокупность материальных следов, зафиксированных, в первую очередь, в ходе осмотра места происшествия, а в дальнейшем – при проведении проверок показаний на месте и иных процессуальных действий. Идеальными же следами считаются показания участников процесса, так называемые отпечатки событий в сознании памяти преступника, потерпевшего, свидетелей и других людей.

Однако с учетом общей тенденции к информатизации общества, начатой в XXI в., важнейшими и практическими неоспоримыми источниками доказательств являются следы, зафиксированные с помощью информационно-коммуникационных технологий. Практика свидетельствует о том, что наиболее частыми следами по делам об убийствах являются видеозаписи, которые могут быть сняты как самими участниками процесса, так и зафиксированы на видеокамеры, установленные физическими или юридическими лицами в помещениях или на зданиях. Участники процесса часто оставляют также информационный след в своих мобильных телефонах, иных информационно-коммуникационных устройствах, которыми они постоянно пользуются. Вместе с тем для анализа информационного следа необходимо учитывать обстоятельства конкретного преступления и личность преступника, поскольку информационный след у криминальной группировки или тщательно готовящегося к преступлению преступника может быть представлен, в том числе, в виде детально проработанного плана, который хранится на домашнем компьютере или мобильном телефоне. Кроме того, в случае если преступником является лицо, совершившее «бытовое» убийство, то из его информационно-коммуникационных устройств можно получить информацию о его передвижении в интересующий период времени, о лицах, с которым преступник общался до или после совершения преступления, и иную криминалистически значимую информацию.

Полагается, что данные следы могут являться одной из важнейших отправных точек для расследования конкретного преступления, поскольку при их тщательном анализе устанавливается достоверная и неопровержимая информация, которая может выступать как самостоятельное доказательство или способствовать получению иных доказательств.

Стоит также отметить, что при осмотре же видеозаписей необходимо уделить внимание тому, не имеет ли она каких-либо следов модификации, при наличии сомнений в оригинальности видеозаписи необходимо назначать экспертизу для определения наличия или отсутствия следов монтажа. Таким образом, в протоколе необходимо детально фиксировать обстоятельства нанесения телесных повреждений, совершения иных насильственных действий, подробно описывая действия каждого из участников с последующим составлением таблицы фотоснимков. С учетом того, что при совершении насильственных преступлений часто наносятся удары, которые невозможно зафиксировать одним скриншотом, следует с помощью видеоредактора «разбить» фрагмент записи по кадрам, и, в последующем, поместить в таблицу фотоснимков несколько скриншотов, отображающих полный механизм нанесения травматического воздействия (замах, направление удара, место приложения травмирующей силы, дальнейшее местоположение

ударившего и потерпевшего), что, в свою очередь, окажет положительное воздействие на качество судебно-медицинской, медико-криминалистических экспертиз.

Становится очевидно, качественный осмотр мобильного телефона может дать следователю огромное количество информации, которая используется при расследовании преступлений. Даже если при осмотре указанной информации не будет зафиксировано прямых доказательств совершения преступления, устанавливается огромный массив информации, необходимый для определения личности преступника, с помощью которой корректируется тактика расследования уголовного дела, проведения отдельных следственных действий.

Считается, что по делам об убийствах целесообразным является незамедлительный осмотр мобильных телефонов преступника и потерпевшего, или только телефона потерпевшего, при отсутствии преступника.

В ходе осмотра мобильного телефона преступника необходимо уделять внимание информации, содержащейся в фотогалерее, с помощью которой можно с привязкой ко времени определить местонахождение преступника до совершения преступления, в период совершения преступления и после совершения преступления.

Анализ переписок в социальных сетях также позволяет установить круг общения лица, в следственной практике имелись случаи, при которых в ходе анализа переписок в социальных сетях устанавливались ценные свидетели, которым достоверно известно о совершенном преступлении, а также непосредственно сообщения, в том числе голосовые, в которых злоумышленник сам рассказывает обстоятельства совершенного преступления.

С помощью современных компьютерных средств, как в рамках проведения экспертизы, так и с помощью программного обеспечения, имеющегося в Следственном комитете Республики Беларусь, при необходимости есть возможность восстановить удаленную информацию, благодаря чему удается восстанавливать фотоизображения, видеозаписи, аудиозаписи, которые имеют серьезное доказательственное значение. По всей вероятности, в случае если незамедлительно проверена телефонная книга и в кратчайшие сроки допрошены люди, которые контактировали с потерпевшим или преступником незадолго до или после совершения преступления, данные допросы будут являться наиболее качественными, поскольку у человека в памяти сохранилось значительно больше обстоятельств контакта с потерпевшим и преступником и при даче показаний он с меньшей долей вероятности упустит какие-либо важные детали.

Таким образом, информационные следы в настоящее время являются важнейшим источником доказательств. При грамотном их исполь-

зовании устанавливаются дополнительные доказательства совершенного преступления, что позволяет наиболее полно установить следовую картину совершенного преступления с помощью использования компьютерной техники, в руках следователя появляется неоценимая информация о личности участников процесса, что в своей совокупности помогает принимать законное решение по уголовному делу.

УДК 343.534 + 343.35

П.О. Полторжицкий

ОТГРАНИЧЕНИЯ ПРЕДМЕТА КИБЕРПРЕСТУПЛЕНИЙ ОТ НЕКОТОРЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ И ИНТЕРЕСОВ СЛУЖБЫ: ВОПРОСЫ КВАЛИФИКАЦИИ

Реализация современных нужд и потребностей человечества через развитие информационных технологий одновременно представляет и широкую предметную область для преступной деятельности. Такая динамика исторически характерна для любой сферы общественных отношений вне зависимости от ее субъекта, территории, активности организации. Это объясняется тем, что необходимость правовой регуляции любой новой деятельности, как правило, наступает после ее «апробации» обществом.

Совершенствование способов обработки информации способствовало развитию мирового сообщества, однако при этом сама информация стала предметом преступных посягательств.

В настоящее время Уголовным кодексом Республики Беларусь (далее – УК Республики Беларусь) предусмотрено пять составов преступлений, отнесенных к преступлениям против компьютерной безопасности. Защита прав субъектов обеспечивается при несанкционированном доступе, уничтожении, блокировании, модификации и неправомерном завладении компьютерной информацией (ст. 349, 350, 352 УК Республики Беларусь). Ответственность также предусмотрена за разработку, использование и сбыт вредоносных программ (ст. 354 УК Республики Беларусь) и нарушение правил эксплуатации компьютерной системы (ст. 355 УК Республики Беларусь).

Отметим, что информация, в том числе компьютерная, выступает предметом целой группы преступлений, таких как умышленное разглашение государственной, служебной, коммерческой тайны, коммерческий шпионаж (ст. 254, 255, 373–375 УК Республики Беларусь).

По нашему мнению, в уголовном законе реализован не исчерпывающий перечень преступлений, предметом которого может выступать информация. Согласно диспозиции ст. 430 УК Республики Беларусь предметом получения взятки являются материальные ценности или выгоды имущественного характера. Анализ научной литературы и практики реализации уголовных дел против интересов службы показывает проблематику квалификации деяния при истребовании должностным лицом предмета нематериального мира или неимущественного характера. Не разрешает этот вопрос и наличие ссылки на выгоды «иного характера», указанной в п. 2 постановления Пленума Верховного Суда Республики Беларусь от 26 июня 2003 г. № 6 «О судебной практике по делам о взяточничестве». Получение должностным лицом какой-либо информации в своих интересах, в том числе представляющей возможность материального обогащения при решении вопроса, достигнутого в обусловленности, который непосредственно в момент деяния не причинил ущерб или вред, может квалифицироваться как получение взятки, равно как и злоупотребление или превышение власти.

Интересно отметить, что при квалификации получения взятки информация не представляет также признак объективной стороны. Например, сведения о товаре или услуге участника, переданные третьим лицам. Это может повлечь ограничение конкуренции и, как следствие, ущерб, как для участника процедуры, так и источника финансирования. Вопрос о квалификации по ст. 430 УК несостоятелен, в том числе при исполнении обусловленности и получении вознаграждения. Отсутствует состав преступления и по ст. 424, 426 УК Республики Беларусь, если в момент совершения деяния ущерб еще не наступил. Проблематика показывает возможность предотвращения ущерба только через отмену результата процедуры, а оценку деяния только как коррупционный проступок, что существенно снижает ответственность. Решение о необходимости квалификации деяния должностного лица, объективная сторона которого, равно как и предмет, не имеют фактического или первичного стоимостного выражения, остается в компетенции представителей нормотворчества и законодательства. По нашему мнению, квалификация данного узкого примера как преступления не нанесет ущерба уголовному праву и процессу, расширит понимание объекта получения взятки, представит более развитый спектр истребуемых должностным лицом выгод как предмета взятки и действий, обусловливающих преступность деяния, расширит ответственность должностных лиц, что будет способствовать предотвращению развития коррупционной преступности. Реализация настоящих предложений возможна в диспозиции ст. 430 УК Республики Беларусь в редакции: «получения выгод имущественного и неимущественного характера».

Одновременно вызывает интерес резонанс в области оценки объекта охраняемого имущества и предмета взятки. Так, в практике органов уголовного преследования стран СНГ представлены уголовные дела, где в качестве предмета взятки рассматривается цифровая валюта. В Республике Беларусь теоретический и законодательный фундамент позволяет оценивать предмет получения взятки криптовалютой по причине фактической возможности ее реализации.

Законодательно определение понятия «криптовалюта» установлено Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», где криптовалюта определена как биткоин, иной токен, обладающий признаками универсального средства обмена, используемого в международном обороте.

Согласно ст. 128 Гражданского кодекса Республики Беларусь к объектам гражданских прав в том числе отнесены деньги, иное имущество. Реализация цифровой валюты позволяет оценить ее в национальной валюте, что представляет возможность характеризовать как предмет взятки; само преступление будет считаться оконченным при появлении фактической возможности распорядиться как всей суммой взятки, так и ее частью. Однако оценка действий, направленных на завладение цифровой валютой, вызывает ряд вопросов. В этих целях преступник совершает несанкционированный доступ к компьютерной информации (ст. 349 УК Республики Беларусь), а после – хищение. Практика квалификации представленных деяний разнится. Объектом преступных посягательств хищения цифровой валюты выступают отношения в сфере компьютерной безопасности и отношения в сфере собственности; квалифицируется по ст. 212 УК Республики Беларусь – хищение имущества путем модификации компьютерной информации. Следует учитывать, что хищению предшествует взлом криптокошелька, который характеризуется не только этапом приготовления к завладению, но при этом, по нашему мнению, квалифицирующим признаком хищения цифровой валюты. Распространенным способом хищения выступают фишинговые, т. е. поддельные сайты, которые формируют как копии с веб-страниц биржи. При входе в аккаунт на фишинговом сайте пользователь вводит логин и пароль, которые преступники используют на веб-странице настоящей биржи. По нашему мнению, действия преступников следует квалифицировать как хищение путем мошенничества, совершенное посредством размещения поддельных сведений о веб-сайте биржи. На практике такой способ хищения квалифицируют по ст. 212 и реже по ст. 349 УК Республики Беларусь, что не учитывает способ завладения имуществом. Адрес и цифровой код фишинговой страницы видоизменены, что приводит поисковую систему пользователя на мошеннический ресурс, его веб-выражение также точно соответствует оригиналу, что и вводит пользователя в заблуждение. Поскольку между преступником и пользователем отсутствует прямой контакт, следует говорить об отдельном виде мошенничества в киберпространстве, что также необходимо относить к квалифицирующим признакам ст. 212 УК Республики Беларусь.

Таким образом, считаем необходимым внести редакцию квалифицирующих признаков ст. 212 УК Республики Беларусь: «путем взлома хранилища цифровых валют или получения доступа к такому хранилищу мошенническим путем» и квалифицировать хищение цифровой валюты по ч. 2 ст. 212 УК Республики Беларусь.

УДК 343.35

А.А. Санукевич

ПРИЗНАКИ И ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕВЫШЕНИЯ ВЛАСТИ ИЛИ СЛУЖЕБНЫХ ПОЛНОМОЧИЙ (ст. 426 УГОЛОВНОГО КОДЕКСА РЕСПУБЛИКИ БЕЛАРУСЬ)

Преступления, связанные с превышением власти или служебных полномочий, подрывают доверие к власти и ее авторитет, посягают на установленный порядок несения службы, на гарантированные Конституцией Республики Беларусь права личности, общества и государства. По статистическим данным, о деятельности судов общей юрисдикции по осуществлению правосудия за 2017 г. в Республике Беларусь число осужденных лиц, в том числе за превышение власти или служебных полномочий (ст. 426 УК), составило 34 человека. В 2018 г. за данный вид преступления были осуждены 43 человека, в свою очередь, в 2019 г. эта цифра возросла до 72 человек. За превышение власти или служебных полномочий по ст. 426 УК в 2020 г. было осуждено 56 лиц, однако в 2021 г. можно заметить снижение по количеству осужденных до 24 человек. В 1-м полугодии 2022 г. 21 лицо осуждено за преступления, предусмотренные ч. 2, 3 ст. 426 УК, – на 47,6 % больше, чем в 1-м полугодии 2021 г. (10 лиц).

В соответствии с п. 13 постановления Пленума Верховного Суда Республики Беларусь от 16 декабря 2004 г. № 12 «О судебной практике по делам о преступлениях против интересов службы (ст.ст. 424–428 УК)» (далее – Пленум № 12) превышение власти или служебных полномочий – это преступление, представляющее собой совершение должностным лицом по службе действий, явно выходящих за пределы предоставленных ему полномочий. Следует обратить внимание, что явность в данном

определении означает бесспорное совершение должностным лицом действий, которые не входят в круг его должностных полномочий.

Сущность преступления, предусмотренного ст. 426 Уголовного кодекса Республики Беларусь (УК), заключается в совершении должностным лицом незаконных действий, так как он юридически не наделен правом на их совершение. Исходя из этого, можно отметить, что при рассмотрении состава превышения власти или служебных полномочий следует установить, что совершенные должностным лицом действия явно выходили за пределы предоставленных ему полномочий. Соответственно, уголовная ответственность за превышение власти или служебных полномочий будет исключена в том случае, если должностное лицо превысило полномочия вследствие нечеткого определения круга служебных обязанностей или недостаточно четкого распределения полномочий между вышестоящими и нижестоящими должностными лицами.

С субъективной стороны превышение власти или служебных полномочий (ст. 426 УК) характеризуется умышленной виной, в виде прямого или косвенного умысла. Для данного преступления с материальным составом характерен прямой либо косвенный умысел. В свою очередь, для преступления с формальным составом – только прямой умысел. Субъектом преступления, предусмотренного ст. 426 УК, выступает специальный субъект, а именно должностное лицо.

Преступным последствием, согласно ч. 1 ст. 426 УК, являются: а) причинение ущерба в крупном размере; б) причинение существенного вреда правам и законным интересам граждан либо государственным или общественным интересам. Крупным размером (ущербом в крупном размере) признается размер (ущерб) на сумму, в двести пятьдесят и более раз превышающую размер базовой величины, установленный на день совершения преступления.

Согласно п. 19 постановления Пленума № 12 при решении вопроса о том, является ли вред, причиненный правам и законным интересам граждан либо государственным или общественным интересам, существенным (ч. 1 ст. 426 УК), судам нужно учитывать степень отрицательного влияния противоправного деяния на нормальную работу организации, число потерпевших граждан, тяжесть причиненного физического или морального вреда и т. п. Р.Н. Ключко отмечает, что последствия в виде существенного вреда правам и законным интересам граждан либо государственным и общественным интересам являются одним из криминообразующих признаков объективной стороны состава преступления, выступающим одновременно в качестве альтернативного условия для привлечения должностного лица к уголовной ответственности.

Совершенные должностным лицом действия явно выходят за пределы предоставленных ему полномочий, если это лицо понимает, что

его действия не входят в круг должностных полномочий. Для того чтобы определить, выходят ли действия должностного лица за пределы его прав и полномочий, необходимо установить объем этих прав и обязанностей, а именно специальные полномочия должностного лица. Исходя из постановления Пленума № 12, под специальными полномочиями понимается тот круг обязанностей, которыми наделено лицо по распоряжению вышестоящего должностного лица или органа. Следовательно, для того чтобы установить, что должностное лицо совершило действия, явно выходящие за пределы его прав и полномочий, необходимо определить, какими правовыми актами они регулируются и какие положения этих актов были нарушены.

Приведем следующий пример из судебной практики.

Судом Лидского района 10 февраля 2022 г. рассмотрено уголовное дело в отношении Б., обвиняемого в совершении преступления, предусмотренного ч. 3 ст. 426 УК. Обвиняемый Б., работая директором частной транспортной компании, в мае 2021 г., находясь по месту работы, допустил конфликт с юрисконсультом транспортной компании З., в ходе которого, имея единый умысел на умышленное причинение З. телесных повреждений, из иной личной заинтересованности, выразившейся в демонстрации личного и физического превосходства над подчиненным, на рабочем месте в кабинете и в дальнейшем в бытовом помещении подверг избиению З., нанеся ему не менее двенадцати ударов руками по голове и другим частям тела, в результате чего потерпевшему были причинены телесные повреждения, относящиеся к категории менее тяжких. Приговором суда обвиняемый Б. признан виновным в умышленном совершении должностным лицом действий, явно выходящих за пределы прав и полномочий, предоставленных ему по службе, повлекших причинение существенного вреда правам и законным интересам граждан (превышение власти или служебных полномочий), совершенных из иной личной заинтересованности, умышленном совершении должностным лицом действий, явно выходящих за пределы прав и полномочий, предоставленных ему по службе, сопряженных с насилием.

Уголовная ответственность за преступления против интересов службы способствует защите общества и граждан от коррупции и общественно опасных деяний должностных лиц, совершаемых по службе посредством использования или ненадлежащего исполнения предоставленных им служебных полномочий. Можно выделить следующие признаки, характерные для преступлений против интересов службы: данный вид преступлений совершается должностным лицом с использованием служебных полномочий вопреки интересам службы; в результате совершения преступления причиняется существенный вред

или ущерб в крупном размере; между причинением вреда или ущерба всегда имеется причинная связь с действиями, совершенными должностным лицом.

УДК 343.98

А.Е. Середа, И.И. Лузгин

ГЕОГРАФИЧЕСКОЕ ПРОФИЛИРОВАНИЕ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Географическое профилирование – это методология расследования, которая использует географически зафиксированные места совершения как взаимосвязанных, так и единичных случаев преступлений для определения наиболее вероятного района проживания преступника или статистического прогнозирования совершения преступления. Оно эффективно применяется в случаях раскрытия и расследования серийных убийств, изнасилований, поджогов, грабежей и актов терроризма.

Американские исследователи серийных убийств Кеппель и Вайс рассматривают расследование убийств как целое, состоящее из следующих компонентов: 1) место, где жертва была в последний раз замечена; 2) место первоначального контакта жертвы с убийцей; 3) место нападения на жертву; 4) место совершения преступником убийства; 5) место обнаружения и извлечения тела. По мнению исследователей, эта информация влияет на разрешение дел двумя способами: во-первых, чем больше известно мест совершения преступлений, тем вероятнее, что дело будет раскрыто; чем ближе расстояние между местами совершения преступлений, тем более вероятным представляется успешное раскрытие дела и привлечение виновного к ответственности. В данной связи становится очевидной категорическая роль географического профилирования в расследовании серийных преступлений.

Задачей географического профилирования выступает составление географического профиля преступлений или преступника, что стало распространенной практикой зарубежных правоохранительных органов в 2022 г. Возможность точного отображения криминалистически значимых пространственных данных, связанных с преступлениями, является результатом точности и доступности географической информационной системы.

Географическая информационная система – это автоматизированная система для сбора, хранения, извлечения, анализа и отображения пространственных данных. Понятие геоинформационной системы также используется в более узком смысле – как инструмента (программного продукта), позволяющего пользователям искать, анализировать и редактировать как цифровую карту местности, так и дополнительную информацию об объектах. Результатом применения таких систем является графически выраженная географически закодированная криминалистически значимая информация.

Географически закодированная криминалистически значимая информация используется для выявления вероятного места проживания преступника, места его работы или досуга, а также установления маршрутов его передвижения. В совокупности с психологическим портретом с высокой долей вероятности представляется возможным использование подобной информации для пресечения преступной деятельности серийного убийцы, поджигателя, террориста и т. д. и привлечения его или ее к ответственности.

Географическое профилирование создает карту вероятности в виде растровой сетки, которая показывает вероятность расположения местонахождения преступника в каждой ячейке сетки на карте. Эта карта называется географическим профилем (или сокращенно геопрофилем). Это часто представляется в виде цветовой карты, где цвет соответствует определенному показателю.

Статистически установленные пространственное значение и расстояние между местами совершения преступлений в связном ряду являются переменными, которые обычно используются для определения вероятного региона для совершения последующего преступления (как единичного, так и последующего в серии преступлений) – этот процесс называется геоанализом. Однако географическое профилирование фокусируется на использовании уже имеющихся данных о местах совершения преступлений для определения места пребывания (жительства, работы) преступника.

Исходя из практики применения данного метода, было установлено, что в простейшем и крайне редком случае места жительства преступников находятся едва ли не в центре их преступных схем (речь, по большей части, идет о преступниках с неустойчивой психикой и душевными заболеваниями, носящими антисоциальный характер). Однако наблюдается крайне агрессивная тенденция в сторону усложнения ввиду беспрецедентной мобильности внутри страны и за рубежом, а также доступной информации.

Канадский криминолог Ким Россмо разработал компьютеризированный алгоритм географического профилирования под названием Criminal Geographic Targeting, который оценивает пространственные характеристики преступлений. Он анализирует географические координаты преступлений преступника и создает цветную карту, которая присваивает вероятности различным точкам для наиболее вероятного

района проживания преступника. Criminal Geographic Targeting был запатентован и интегрирован в специализированный программный продукт для анализа преступности под названием Rigel. Данный продукт разработан компанией-разработчиком программного обеспечения Environmental Criminology Research Inc. Другими известными автоматизированными системами географического профилирования являются CrimeStat и Gemini. Входные данные системы – это адреса или координаты места преступления, часто вводимые через географическую информационную систему. Результатом является поверхность опасности (трехмерная поверхность вероятности) или цветной геопрофиль, на котором изображены наиболее вероятные районы проживания преступника или поисковая база. Эти программы помогают криминалистам и следователям более эффективно концентрировать свои ресурсы, выделяя важнейшие географические районы.

Примером успешного применения географического профилирования в раскрытии и расследовании преступлений является дело расследования серийных убийств Анджела Буоно (в рамках расследования данного дела был установлен так называемый эффект угольного мешка (coal-sack effect, англ.), который заключается в том, что у подобных преступников есть тенденция избегать совершения преступления вблизи места своего проживания). В ходе расследования американский криминалист Барретт задокументировал несколько наблюдений правоохранителей относительно связи между местами совершения преступлений и районом проживания преступника. Если места убийства и захоронения тел разные, то убийца, вероятно, живет в том районе или недалеко от него, где было совершено нападение. И наоборот, если жертва была оставлена на месте убийства, то убийца, вероятно, не местный.

Барретт также говорит о том, что если место преступления находится рядом с дорогой общего пользования, это указывает на то, что преступник, возможно, не из этого района, в то время как место преступления вдалеке от дороги предполагает, что преступник местный. Сокрытое тело жертвы может означать, что преступник, вероятно, может повторно использовать место захоронения, в то время как брошенное в открытом месте тело может означать то, что преступник не местный и его не интересует обнаружат ли жертву.

Иным примером успешного использования географического профилирования в раскрытии и расследовании преступлений является расследование серии изнасилований Джона Даффи. Географическое профилирование позволило правоохранителям обнаружить предположительное место проживания преступника на основе расположения известных мест преступления и составления психологического портрета преступника и провести спецоперацию по его задержанию.

Раскрытие и расследование преступлений с использованием географического профилирования в общих чертах может быть разделено на следующие этапы: 1) установление факта совершения преступлений; 2) начало процесса расследования; 3) выявления связи между совершенными преступлениями (установление серийного характера); 4) осуществление психологического профилирования с выявлением психологического портрета преступника; 5) проведение географического профилирования с выявлением географического профиля расследуемой серии преступлений; 6) разработка новых путей и стратегии расследования.

В современных условиях для поддержания правопорядка и привлечения к ответственности лиц, совершивших преступления, правоохранительным органам требуется применять в своей практике новейшие достижения науки и техники, чем являются на данный момент автоматизированные системы географического профилирования. В рамках обеспечения национальной безопасности требуется как можно быстрее выявить и обезвредить преступников, совершающих серийные преступления, в особенности преступления против жизни и здоровья граждан – серийных убийц, насильников, разбойников и террористов. С этой целью обоснованным представляется дальнейшее исследование и усовершенствование географического профилирования на основе автоматизированных программ и разработанных под них алгоритмов в контексте расследования серийных преступлений.

УДК 343.98

О.А. Слащинин

ВИРТУАЛИЗАЦИЯ КРИМИНАЛИСТИЧЕСКИХ ОБРАЗОВ, ПОЛУЧЕННЫХ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ИЗЪЯТЫХ ПО УГОЛОВНОМУ ДЕЛУ

В настоящее время органы уголовного преследования при производстве предварительного следствия, дознания по уголовному делу все чаще сталкиваются с электронными устройствами (далее – устройство) и содержащимися в них электронными носителями информации (далее – носитель). Это связано с непрекращающимся научно-техническим прогрессом, цифровизацией общественных отношений и ростом оборота указанных устройств у потенциальных участников уголовного процесса. Последние, используя в своей жизнедеятельности компьютерную технику, смартфоны и иные устройства, могут аккумулировать в их носителях сведения об обстоятельствах, имеющих значение для правильного раз-

решения уголовного дела. В связи с этим указанные носители должны рассматриваться органами уголовного преследования как возможный источник доказательств в соответствии с ч. 2 ст. 88 и ч. 2 ст. 100 Уголовно-процессуального кодекса Республики Беларусь (УПК) [1].

Получив в свое распоряжение упомянутые устройства с носителями, органы уголовного преследования должны обеспечить извлечение из них всех имеющихся цифровых доказательств. Однако сам порядок сбора и фиксации указанных доказательств в УПК не закреплен, что может вызвать проблемы с их последующей проверкой и оценкой согласно ст. 104 и 105 УПК. В свою очередь, существуют общепринятые стандарты работы с носителями и содержащейся на них компьютерной информацией. Данные стандарты устанавливаются как международными организациями в области компьютерной криминалистики [2, 3], так и отечественными судебными экспертами [4].

Упомянутые стандарты можно кратко изложить в следующих поэтапных положениях, которые могут применяться и в рамках уголовного процесса:

1) безопасное подключение осматриваемого носителя в аппаратном или программном режиме «только-для-чтения», исключающем запись на него новых данных, а также изменение или удаление уже имеющихся;

2) подключение дополнительного очищенного носителя с емкостью памяти, количественно равной или большей осматриваемого носителя;

3) снятие побитовой копии (образа) осматриваемого носителя с возможностью ее верификации посредством проверки контрольной суммы, а также запись копии (образа) на дополнительный носитель (создание отдельного файла-образа или полное клонирование осматриваемого носителя);

4) отключение осматриваемого носителя, его последующая упаковка и опломбирование в целях защиты от несанкционированного доступа к нему;

5) дальнейшее взаимодействие лишь с вышеуказанной побитовой копией (образом), записанной на дополнительном носителе.

Вышеуказанные положения направлены на извлечение максимального объема цифровых доказательств и защиту от их возможной перезаписи или уничтожения самого оригинального носителя. Этот объем может обеспечиваться в результате частичного восстановления ранее удаленной компьютерной информации, а также сохранения целостности и доступности уже зафиксированных данных в самой копии (образе).

Полученный образ носителя монтируется к компьютерной технике органа уголовного преследования, в результате чего появляется возможность осматривать его содержимое с помощью файлового менеджера. Современное программное обеспечение (ПО) позволяет создавать также криминалистические образы различных форматов (например,*.e01, *.001, *.aff), поддерживающих их фрагментацию, сжатие и шифрование. Вышеуказанная копия (образ) полностью реплицирует свойства физического носителя, его логические разделы, каталоги и электронные файлы, в том числе скрытые, зашифрованные и ранее удаленные (фрагментарно).

Компьютерная информация, осматриваемая посредством файлового менеджера без поддержки графического интерфейса самой операционной системы (ОС) и ПО оригинального носителя, не всегда может быть достаточно информативной. В отдельных случаях извлечение необходимых данных возможно только при их осмотре с помощью графического интерфейса ОС и иного ПО в динамике (например, экранные формы и элементы, логика организации взаимодействия пользователя с файловой системой и процессами). Однако запуск оригинального носителя, в том числе посредством изъятых у участника уголовного процесса устройств, неизбежно приведет к изменению содержащейся на нем компьютерной информации. Факт нарушения ее целостности может стать основанием для признания полученных цифровых доказательств недостоверными или недопустимыми в соответствии со ст. 105 УПК. Для решения указанной проблемы компьютерные криминалисты (форензисты) предлагают виртуализировать получаемые образы, что позволяет осматривать компьютерную информацию в ее аутентичной форме, т. е. аналогичной запуску носителя с оригинального устройства участника уголовного процесса [5, 6].

Виртуализация криминалистического образа осуществляется посредством выполнения на компьютерной технике, используемой органом уголовного преследования, следующих последовательных действий:

1) полученный для целей виртуализации образ монтируется с помощью программного эмулятора (например, Arsenal Image Mounter, AccessData FTK Imager) с обязательным созданием временных дифференциальных файлов, препятствующих последующей модификации оригинального образа;

2) эмулированный криминалистический образ посредством гипервизора (например, VMware Workstation, Oracle VM VirtualBox) идентифицируется как физический носитель, подключенный к компьютерной технике;

3) на основе идентифицированного носителя производится создание виртуальной машины и его гибкая настройка в зависимости от свойств устройства, которое было изъято у участника уголовного процесса;

4) осуществляется запуск виртуальной машины, полностью имитирующей содержание и работу первоначального носителя в составе устройства.

Несмотря на имеющиеся практические руководства по виртуализации криминалистических образов, их реализация на практике достигается не всегда. Это зависит от вида виртуализируемой ОС (например, Windows, Linux, Android), емкости и доступности самого носителя, а также характеристик ранее используемого с ним устройства. Невзирая на имеющиеся проблемы, данный подход собирания цифровых доказательств можно признать перспективным для органов уголовного преследования и требующим дальнейшей разработки.

Список использованных источников

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : в ред. Закона Респ. Беларусь от 20.07.2022 г. № 199-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Association of chief police officers – Good Practice Guide for Digital Evidence (March 2012) [Electronic resourse]. – Mode of access: www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. – Data of access: 08.12.2022.

3. National Institute of Standards and Technology – Guide to Integrating Forensic Techniques into Incident Response (August 2006) [Electronic resourse]. – Mode of access: tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875. – Data of access: 08.12.2022.

4. Методика исследования компьютерной информации : метод. рекомендации / Гос. ком. судеб. экспертиз Респ. Беларусь. – Минск, 2016.

5. Форум ИБ – Codeby.net: Виртуализация криминалистических образов в Windows [Электронный ресурс]. – Режим доступа: codeby.net/threads/ virtualizecija-kriminalisticheskix-obrazov-v-windows. 64120. – Дата доступа: 08.12.2022.

6. Security is FUN: Booting up evidence E01 image using free tools [Electronic resourse]. – Mode of access: www.securityisfun.net/2014/06/booting-up-evidence-e01-image-using.html. – Data of access: 08.12.2022.

УДК 343.98.06

Е.Н. Соболевский

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новые тенденции в развитии информационных технологий создают новые риски для информационной безопасности любого государства. Цифровой мир стремительно расширяется, он становится мобильным,

управляет производством и технологическими процессами, охватывает всю среду обитания человека – от бытовых приборов до умных офисов и интеллектуального транспорта. Все больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастает поток данных и объемы хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как «Интернет вещей» (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через сеть станут доступны почти все предметы, окружающие человека.

По мере развития технологий в окружающем человека мире появляется все больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, все больше атак будет направлено не только на программное, но и на аппаратное обеспечение (сетевые карты, USB-устройства), входящее в инфраструктуру «интеллектуального транспорта», «умных домов», автоматизированных систем управления производством и др.

Возможности коммуникаций, которые стали доступны государствам, юридическим и физическим лицам после возникновения глобальной компьютерной сети Интернет, привели к кардинальному преобразованию общества и его экономической реальности. Интернет сегодня – это среда, используемая для всевозможных форм взаимодействия всех субъектов экономики. Высокая степень необходимости интернета как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества, воздвигает его в ряд необходимых элементов социально-экономического развития общества. По состоянию на текущий год в мире насчитывается более 5 млрд пользователей сети Интернет – это 63 % от общего населения Земли. Об этом свидетельствуют данные отчета April Global Statshot report, подготовленного при участии We Are Social и Hootsuite.

Приоритетную важность представляет собой переход различных государственных отраслей экономики в цифровое пространство – электронное правительство. Предоставление цифровых услуг населению, создание государственных информационных систем и ресурсов, формирование межгосударственных каналов передачи данных сегодня представляют собой повсеместные практики.

На текущий момент 80 % организаций, прошедшие стадию цифровых преобразований (внедрение технологий «Индустрия 4.0»: промышленный Интернет вещей, большие данные, 3D-принтеры и др.), смогли существенно увеличить свою прибыль. Ежегодная прибыль компаний Samsung, LG, Huawei и др. оценивается в десятки млрд дол-

ларов США, что демонстрирует не только успешность цифровизации бизнес-процессов компаний, но и актуальность разрабатываемой ими продукции – технических средств и средств связи.

Сеть Интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран. Так возникла экономика совместного использования (Sharing economy) – переход к платформенным решениям. Изначально базирующиеся на цифровых рынках платформы Google, Facebook (США), Amazon (США), Uber (США), Alibaba (Китай), Яндекс (Россия) являются гигантами цифрового мира и имеют исключительное конкурентное преимущество как на глобальном, так и на местном уровне.

В современных реалиях цифровая экономика стала мощным фундаментом развития государств: страны с более развитой цифровой экономикой получают большую долю своего ВВП за счет высокотехнологичных секторов. Предполагается, что к 2025 г. цифровая экономика может достичь показателя в 50 % глобального ВВП, а в развитых странах превысить его.

Киберугрозы сегодня нацелены на все области, использующие цифровые данные: здравоохранение, образование и науку, банковскую сферу, государственные органы, представителей бизнеса и многое другие. В большинстве случаев цель злоумышленников – хищение персональных данных: номера банковских счетов и кредитных карточек, паспортные данные, медицинские карты, данные об объектах интеллектуальной собственности, а также информация, относящаяся к государственной, коммерческой и военной тайне.

При рассмотрении области киберугроз на уровне государств можно отметить, что кибератакам подвержены как страны с высоким уровнем экономического развития (США, Китай, Канада и т.п.), так и с низким уровнем.

Наиболее актуальными угрозами можно считать:

социальную инженерию – это технологии манипулирования людьми в сети Интернет;

DDoS-атаки или отказ от обслуживания – это поток ложных запросов, блокирующих ресурс;

шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя (чаще всего через сеть Интернет при введении жертвы в заблуждение методами социальной инженерии). Данные программы блокируют доступ пользователей к их устройствам или блокируют доступ к файлам до тех пор, пока не будет выплачена денежная сумма или выкуп.

киберфизические атаки представляют собой взлом электрических сетей, транспортных систем, водоочистных сооружений и т. д.;

атаки на IoT (Интернет вещей) – это заражение устройства, подключенного к интернету;

киберпропаганду (дезинформация) и хактивизм (форма политической активности, при которой навыки компьютерного взлома широко используются против влиятельных коммерческих институтов и правительств, других целей).

Существующие и вновь возникающие угрозы кибербезопасности сегодня направлены на все структуры, имеющие выход в сеть Интернет: частные и государственные организации, производства, медицинские и образовательные учреждения, учреждения здравоохранения, финансовые и банковские структуры, а также многое другое.

Отсутствие необходимых навыков кибербезопасности активно влияет на ситуацию с киберпреступностью. В результате увеличения пропускной способности устройства, подключенные к Интернету вещей, стали более уязвимыми для кибератак. Многие устройства IoT не разработаны с учетом требований безопасности и могут иметь недостатки и уязвимости, которые легко используют злоумышленники. Если хакеры могут получить контроль над устройствами IoT в организации, они потенциально могут использовать их для доступа к остальной части ИТ-системы.

Таким образом, использование сети Интернет влечет за собой определенные риски, которые необходимо учитывать при проектировании, разработке и внедрении сетевых технологий. Полагается, что не стоит бояться использовать сеть Интернет, однако нужно использовать ее грамотно. Требуется вывести общество из состояния, вызванного опасностью использования сети, сформировать у граждан цифровую грамотность.

УДК 004.056.57; 004.89

М.Н. Сорокин, Д.С. Рябенко

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАЗВИТИИ АНАЛИТИКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В ходе становления информационного общества процесс информатизации является одним из основных факторов его развития на современном этапе. Благодаря процессу информатизации субъект (человек, общество) включается в глобальное информационное пространство, становясь при этом его частью. Наиболее точно данный эффект можно сопоставить с нынешним состоянием технологии ис-

кусственного интеллекта и машинного обучения, когда в основе множества повсеместных технологических процессов содержатся множества приложений искусственного интеллекта. Распространенные приложения искусственного интеллекта в современных технологиях включают распознавание голоса, обнаружение мошенничества, фильтрацию спама в электронной почте, обработку текста, рекомендации по поиску, анализ видео и т. д. Кроме того, эти современные технологии, совершенствуясь ежедневно, подпитываются все более широким анализом данных и получают новые качественные результаты, которые не были заложены их разработчиками.

Невероятные темпы роста данных за последние несколько лет привели к появлению нового термина «большие данные», что может означать много данных, достаточных для специального исследования того, как хранить, передавать, управлять и анализировать информацию, в том числе с применением ставших более доступными облачными вычислениями. Достижения в области облачных вычислений имеют важное значение для обеспечения огромных вычислительных мощностей экономически эффективным способом, помогая решать ресурсоемкие вычислительные задачи.

Наряду с благами объединения субъекта (человека, общества) в единое информационное пространство под управлением искусственного интеллекта, возникают и новые опасности, обусловленные необходимостью обеспечения информационной безопасности. Например, негативное информационное воздействие на сознание человека в результате может привести к изменению его мировоззрения и переориентации ценностей. В связи с этим проблема информационной безопасности должна быть достаточно глубоко осмыслена.

Исследуя проблемы информационной безопасности, возможно определение двух факторов, которые определяют возможность применения технологии искусственного интеллекта для отрасли. Во-первых, сбор и хранение больших объемов данных в области информационной безопасности ведется уже давно. Специалисты по информационной безопасности (далее – специалисты) применяют множество автоматизированных инструментов, предназначенных для сортировки, нарезки и добычи этих данных в целях решения возникающих прикладных задач обеспечения защиты информации. Во-вторых, на настоящий момент существует нехватка квалифицированных, опытных специалистов для успешной защиты информационной инфраструктуры и систем. Кроме того, прогнозируемый спрос на специалистов в сфере информационной безопасности и защиты информации будет продолжать расти. Учитывая эти факторы, технологии искусственного интеллекта отлично подходят для повышения эффективности информационной безопасности.

Обеспечение информационной безопасности представляется сложным, многофункциональным процессом, зависящим от различных внешних и внутренних факторов. Это обусловлено тем, что современный этап развития общества связан с освоением и использованием новых глобальных возможностей информационной сферы, таких как сеть Интернет, виртуальное пространство, новейших беспроводных средств коммуникации и т. д.

Рассмотреть влияние на информационную безопасность применения технологии искусственного интеллекта возможно на примере проведения анализа реагирования специалистом на инцидент взлома информационной сети. Предположим, что с целью несанкционированного получения конфиденциальной информации была взломана информационная сеть и размещено вредоносное программное обеспечение на отдельных вычислительных машинах сети. В этом случае специалист должен решить следующие частные задачи: выяснить, какая именно информация была украдена; каким образом осуществлена кража; восстановить систему, чтобы предотвратить подобные атаки снова.

Сроки физического обнаружения уязвимостей и решения выявленных проблем для специалиста весьма велики. Чтобы выяснить, какая именно информация была украдена, специалисту необходимо проверить журналы доступа к файлам или сетевой трафик, анализируя доступ к конфиденциальным файлам или большим объемам данных, выходящим из сети. Далее может потребоваться анализ диска на наличие вредоносных программ, чтобы попытаться отследить известные образцы вредоносных программ с использованием имеющихся сигнатур. Возможно, в рамках реагирования на инцидент необходим анализ работающей системы с целью поиска необычных процессов или другого аномального поведения информационной сети.

Благодаря технологии искусственного интеллекта большинство из представленных задач могут быть автоматизированы и даже развернуты в режиме реального времени, что позволит установить действия до того момента, как будет нанесен какой-либо ущерб. Например, с помощью хорошо обученной нейронной сети возможно выявление подозрительного трафика в сети и отключение этих соединений по мере их возникновения. Нейронные сети могут идентифицировать новые образцы вредоносного программного обеспечения, ранее не включенные в имеющиеся сигнатуры.

Сегодня подавляющее большинство технологий искусственного интеллекта в информационной безопасности применяется в качестве типа вспомогательной системы «предупреждения». В любом случае окончательное решение принимает человек. Это обусловлено тем, что используемые нейронные сети недостаточно точны по сравнению с типичным аналитиком-человеком.

В сфере информационной безопасности на данный момент ответ на вопрос, следует ли доверять искусственному интеллекту, а не человеческому анализу – часто «нет». В некоторой степени должен произойти сдвиг в том, каким образом мы оцениваем современные технологии и их возможности, прежде чем в полном объеме доверим принятие решения развитым технологиям искусственного интеллекта.

Следующие несколько лет будут интересны в контексте информационной безопасности. Огромные объемы данных, которые могут быть сгенерированы, наряду с проблемами проведения крупномасштабного анализа, для принятия оптимального решения, являются идеальным сочетанием для обширных и успешных архитектур обучаемых нейронных сетей.

УДК 343.3

Н.С. Сорокун, Р.А. Карапетян

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРИЧИН И УСЛОВИЙ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ОСНОВА ПРОФИЛАКТИКИ ТАКИХ ДЕЯНИЙ

В настоящее время наблюдается активное преобразование всех сфер жизнедеятельности граждан. Не остается без внимания и область информационных технологий, развитие которых стремительно возрастает. Становится невозможно уследить за всеми событиями в данной сфере. Создание современной техники, различных программ и приложений приводит к тому, что совершается множество преступлений в информационной среде. Данные обстоятельства ведут к неблагоприятным условиям в обществе. Уровень воспитания и нравственности становится низким, в результате чего падает и уровень развития людей. Современные технологии помогают не только развиваться и совершенствоваться, но и терять те качества, которые необходимы любому человеку для хорошей жизни.

Вопрос раскрытия и расследования преступлений, совершаемых с использованием компьютерных технологий, становится очень остро в последнее время. Прежде всего данный факт обусловлен необходимостью развития и совершенствования существующих методик расследования преступлений. Очевидно, что с развитием информационных технологий возникает необходимость в преобразовании стандартных ме-

тодик и средств. Однако внимание также стоит уделять и предупреждению преступлениям данного вида. В связи с чем видятся актуальными рассмотрение вопросов, связанных с причинами и условиями совершения компьютерных преступлений, а также изучение характеристики личности преступника и потерпевшего.

В настоящее время наблюдается повсеместное внедрение компьютерных технологий во все сферы жизнедеятельности общества. Основное внимание уделяется внедрению в производственные, экономико-финансовые и общественные отношения. Рассматриваемый процесс компьютеризации способствует развитию и совершенствованию жизни общества, а также приводят к появлению новых категорий преступных деяний. Такие преступления совершаются с использованием компьютерной информации и посредством компьютерных технологий.

По общему правилу данные преступления делятся на три категории: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для электронно-вычислительных машин (ЭВМ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Данные противоправные деяния находят свое отражение в нормах Особенной части Уголовного кодекса Российской Федерации.

Рассматриваемые группы преступлений представляют особый интерес, который прежде всего обусловлен характеристикой субъекта совершения компьютерных преступлений. Данный аспект объясняется тем, что обычный гражданин вряд ли способен совершить неправомерный доступ к компьютерной информации или создать вредоносную программу, не обладая специальными знаниями в области информационно-телекоммуникационных систем.

В 2020 г. наиболее распространены мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70 % всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4 %, 237,1 тыс.).

В 2021 г. мошенничество в сфере информационно-телекоммуникационных технологий составило 73 % всех хищений (249,2 тыс.), совершенных путем обмана или злоупотребления доверием. При этом существенно замедлились темпы их прироста (с 73,4 % в 2020 г. до 5,1 % в текущем).

За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до 25 %. Большинство «киберпреступлений» совершается с использованием сети Интернет (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.).

Кроме того, по своей природе компьютерные преступления носят латентный характер. Немаловажным элементом выступает также и харак-

тер совершения данных преступлений. Все преступные деяния, которые совершаются с помощью использования информационно-телекоммуникационных систем, всегда скрыты от обычных людей и выявление таких преступлений представляет собой особый процесс. Прежде всего для выявления и последующего раскрытия компьютерного преступления необходимо обладать специальными знаниями в области компьютерных технологий, так как доказательственная база будет формироваться в большей степени путем нестандартных методов.

В связи с указанным ранее фактором следует сказать о том, что профилактика в таком случае должна базироваться на уяснении причин и условий совершения преступления данного вида. На этом вопросе, полагаем, нужно остановиться более подробно.

Анализируя разные источники по данному вопросу, был сделан вывод, что причины совершения преступлений в сфере компьютерной информации можно подразделить на две основные категории. Первая категория характеризуется общими причинами преступности с использованием возможностей информационно-телекоммуникационной системы. В данную категорию могут входить причины различного уровня, которые присущи как компьютерным преступлениям, так и иным видам преступности.

Что касается второй категории, то она характеризуется специфическими причинами компьютерных преступлений. В частности, причины данной группы выражаются в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений, связанных с появлением автоматизированных систем обработки информации. В рамках этой категории выделяют следующие причины компьютерной преступности:

уязвимость и зависимость компьютерных систем друг от друга;

несоответствие уровня развития юридических и политических структур уровню развития компьютерных и телекоммуникационных технологий;

динамичное развитие зависимости современных технологий от компьютерных систем;

отсутствие должного информирования граждан об уязвимости компьютерных систем;

существующие сегодня пробелы уголовного законодательства в части, касающейся регулирования общественных отношений в сфере компьютерной информации, а именно, отсутствие некоторых составов в уголовном законодательстве;

различия в законодательной базе с точки зрения соответствия отечественного и международного законодательства.

Однако, полагаем, необходимо отметить, что данные причины не могут рассматриваться в качестве непосредственных. В юридической

литературе отмечается, что основной причиной, подталкивающей лицо на совершение компьютерного преступления, будет являться детерминация преступного поведения.

Что касается условий совершения преступлений в сфере информационно-телекоммуникационных технологий, то стоит обратить внимание на следующие:

открытый доступ к автоматизированным информационным системам, с помощью которых могут совершаться финансовые операции различного характера;

отсутствие должного контроля за отдельными категориями сотрудников, что позволяет злоумышленникам использовать ЭВМ предприятий в качестве оружия преступления;

низкий уровень защиты компьютерных систем;

легкий доступ к данным ЭВМ, ввиду отсутствия надежной парольной системы;

отсутствие во многих организациях специально уполномоченного субъекта, отвечающего за сохранение конфиденциальности отдельных информационных данных;

отсутствие соглашений сотрудников о неразглашении данных, составляющих конфиденциальную информацию, в том числе пароли и иные ключи доступа к ЭВМ.

Необходимо отметить, что большинство условий создаются непосредственно потерпевшими лицами. Основной причиной является неосмотрительность лица. Помимо указанных условий могут отмечаться и иные. Нами были рассмотрены наиболее актуальные условия совершения информационных преступлений.

Рассмотрев причины и условия совершения преступлений в сфере компьютерной информации, вытекает вывод о том, что их круг достаточно обширен. На основании рассмотренных данных, считаем, стоит перейти к характеристике лиц, способных к совершению преступлений в сфере информационных технологий.

Анализируя практическую деятельность, можно сделать вывод о том, что субъектом совершения преступлений в сфере компьютерной информации в большинстве случаев выступает лицо мужского пола. Возрастная группа данных лиц, как правило, варьируется от 18 до 24 лет. Иными словами, совершают такое преступление лица студенческого возраста или же те, которые только завершили обучение в учреждении образования. Считаем, что именно в таком возрасте на человека можно оказывать некое воздействие, которое будет способствовать формированию у него устойчивого преступного поведения.

Полагаем, нужно акцентировать внимание на том, что огромная доля компьютерных преступлений носят латентный характер, соответст-

венно, не могут быть выявлены и проанализированы. В связи с этим возникает сложность в точном определении возрастных рамок субъекта совершения преступления, а также отдельных черт, характеризующих его.

Характеризуя личность компьютерного преступника, важно обратить внимание на психологические особенности данных лиц. В этом вопросе стоит рассмотреть отдельные качества личности, указывающие на поведение преступника.

Так, изучаемые лица, как правило, имеют замкнутый характер и не стремятся достичь высокого положения в обществе. В большинстве случаев они действуют индивидуально в связи с такой чертой характера, как скрытность. При общении отдельные лица этой категории конфликтны, не обладают особой эмоциональностью.

Указанные выше факторы свидетельствуют об одиночном характере осуществления деятельности данными субъектами. Однако специалистами в этой области отмечается, что они стремятся принадлежать к определенной социальной группе, откуда и вытекает создание хакерских сообществ.

Рассматривая категорию субъектов преступления в сфере компьютерной информации, можно сделать вывод о том, что указанные лица обладают высокой самооценкой. По нашему мнению, это связано с тем, что данная сфера деятельности, а именно информационно-телекоммуникационные технологии, требует высоких знаний для ее осуществления. В связи с чем лица, разбирающиеся в этой области, считают себя на ступень выше от обычных людей, так как обладают высокими знаниями в сфере компьютерных технологий. Указанные факторы позволяют говорить о спонтанном совершении преступлений без должной к тому подготовки.

Изучение поведения субъектов компьютерных преступлений свидетельствует о наличии таких признаков, как:

установление и поддержание социальных связей с иными лицами, совершающими преступления в сфере компьютерной информации;

обсуждение способов совершения преступлений в сфере информационно-телекоммуникационных технологий;

использование словесных оборотов, присущих лицам, разбирающимся в компьютерных технологиях.

В поведении рассматриваемой категории лиц могут выделяться и иные черты.

В рамках исследования данной темы была отмечена также проблематичность получения информации о типичных характеристиках личности компьютерного преступника. Это обстоятельство обусловлено высокой латентностью таких преступлений и отсутствием должного эмпирического материала, позволяющего изучать данную тему со всех сторон.

Таким образом, подводя итог настоящей статье, полагаем, следует отметить, что компьютерные преступления сегодня набирают особую популярность. В большинстве случаев преступления такого рода остаются незамеченными. Данное обстоятельство вытекает из-за отсутствия компетентных специалистов среди сотрудников органов внутренних дел, способных раскрывать и расследовать преступления в сфере информационно-телекоммуникационных технологий.

Одной из причин совершения этой категории преступлений выступает формирование преступного поведения у лиц. Такая причина рассматривается в качестве основной, поскольку именно преступное поведение может подталкивать лицо на совершение преступления.

При рассмотрении особенности личности субъекта преступлений в сфере компьютерных технологий главной характеристикой считается возраст лица, который был отмечен в диапазоне от 18 до 24 лет. Безусловно, данный диапазон не может рассматриваться в качестве основного и единственного, поскольку такие преступления совершаются лицами и в 16 лет, и в 35.

Специфические особенности личности преступника проявляются в его поведенческих чертах. Так, например, компьютерный преступник, как правило, обладает скрытным и замкнутым характером, малообщителен и обладает низким уровнем эмоциональности.

В заключение стоит отметить то, что криминологическая характеристика компьютерных преступлений будет оставаться актуальным вопросом, поскольку в настоящее время отсутствует достаточная эмпирическая база для изучения данной темы в полном объеме. Указанное обстоятельство вызвано тем, что большинство преступлений в сфере информационно-телекоммуникационных технологий носят латентный характер, ввиду чего не учитываются в общей статистике преступлений.

Список использованных источников

1. Аскольская, Н.Д. Специфика криминалистической характеристики киберпреступлений / Н.Д. Аскольская // Закон и право. – 2019. – № 8. – С. 89–92.

2. Ахмедханова, С.Т. Криминологическая характеристика преступлений в сфере информационных технологий / С.Т. Ахмедханова, Э.Х. Кахбулаева // Вестн. МГОУ. Серия «Юриспруденция». – 2018. – № 4. – С. 16–23.

3. Маслакова, Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика / Е.А. Маслакова // Среднерус. вестн. обществ. наук. – 2018. – № 1. – С. 31.

4. Поляков, В.В. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Изв. АлтГУ. – 2018. – № 6. – С. 104.

5. Ханов, Т.А. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений / Т.А. Ханов, А.Ж. Нуркеев // Изв. АлтГУ. – 2017. – № 6. – С. 98.

УДК 347.775

П.А. Тарасов

О ГРАЖДАНСКО-ПРАВОВОМ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационное пространство имеет особое значение в жизни современного человека. В Республике Беларусь идет активное развитие информационных технологий, информационная сфера становится системообразующим фактором жизни общества, оказывает активное влияние на состояние стабильности социальной, экономической и других сфер обеспечения национальной безопасности Республики Беларусь. Все большее значение приобретает информационная безопасность как составная часть общей системы обеспечения национальной безопасности Республики Беларусь.

В соответствии с Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» информацией являются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Данные сведения часто являются объектами необоснованного распространения, в связи с чем становится актуальным вопрос о защите информации с помощью комплекса организационных, технических и правовых мер, направленных на обеспечение ее конфиденциальности, сохранности, целостности, подлинности и доступности.

В настоящее время защита информации становится неотъемлемым атрибутом обеспечения безопасности граждан, общества и государства. В нашем государстве в целях консолидации усилий и повышения эффективности государственных органов, иных организаций и граждан по обеспечению национальной безопасности Республики Беларусь, защиты ее национальных интересов, а также обеспечения комплексного подхода к проблеме информационной безопасности приняты: Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» и постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». В Республике Беларусь также действуют законодательные акты, регулирующие общественные отношения в сфере

информации, информатизации и защиты информации, коммерческой тайны и персональных данных. Принятые нормативные правовые акты составляют комплексную систему мер, направленную на защиту информации правовыми способами, включая гражданско-правовые.

Гражданское законодательство также призвано защищать интересы субъектов информационных отношений. В Гражданском кодексе Республики Беларусь (ГК) определено, что одним из объектов гражданских прав является нераскрытая информация, к которой относятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, составляющих коммерческую или служебную тайну. Защита указанной информации осуществляется предусмотренными законодательством Республики Беларусь способами.

В ГК предусмотрена ответственность за нарушение договорных обязательств одной из сторон, связанных с незаконным ознакомлением или использованием информации, составляющей коммерческую или служебную тайну. В соответствии со ст. 19 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» лицо, по вине которого произошло незаконное разглашение, ознакомление или использование сведений, составляющих коммерческую тайну обязано возместить убытки (в том числе упущенную выгоду), которые были причинены владельцу этой информации.

ГК устанавливает также ответственность за нарушение обязательств вследствие причинения вреда одним лицом другому в связи с непредоставлением необходимой информации о товаре, работе или услуге. Статья 965 ГК определяет, что возмещение вреда, причиненного вследствие непредоставления полной и достоверной информации о данных объектах, подлежит возмещению по выбору потерпевшего продавцом или изготовителем товара, исполнителем. В данный момент гражданское законодательство Республики Беларусь не относит саму информацию о товарах, работах, услугах, частной жизни граждан, персональных данных, личной и семейной тайны к объектам гражданских прав.

Ряд белорусских и российских правоведов (Д.П. Александров, В.М. Богданов, Е.Н. Насонова) полагают, что, несмотря на отсутствие законодательного закрепления в целом информации в качестве объекта гражданских прав, ее следует считать таковым. Другие юристы (Л.Б. Ситдикова, В.А. Дозорцев) считают данный вопрос дискуссионным. В этом случае к объектам гражданских прав предлагают относить лишь ту информацию, которая определена законом, – охраняемую (нераскрытую) информацию.

При этом необходимо отметить, что принципами регулирования информационных отношений являются: защита информации о частной жизни физического лица и персональных данных, обеспечение безо-

пасности личности, общества и государства при пользовании информацией и применении информационных технологий (ст. 4 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»). С целью гражданско-правовой защиты граждан от неправомерного использования указанной информации правовое регулирование отношений в информационной сфере должно строиться на принципах, перечисленных в данном Законе.

Изложенное свидетельствует о необходимости совершенствования гражданского законодательства, регламентирующего способы защиты гражданских прав в сфере информационной безопасности. По нашему мнению, только определив, какую информацию следует считать объектом гражданских правоотношений, и закрепив это законодательно, можно обеспечить комплексную защиту прав граждан в информационной сфере.

УДК 343.985.2

А.Ю. Теслёнок

ПРОГРАММНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, ИСПОЛЬЗУЕМОЕ ПРИ СОВЕРШЕНИИ ОРГАНИЗАЦИИ НЕЗАКОННОЙ МИГРАЦИИ

Обеспечение противодействия преступности на современном этапе требует постоянного поиска новых механизмов раскрытия, анализа причин и условий совершения преступлений, выработке современных рекомендаций. Совершение противоправных деяний в данный период, как правило, носит латентный характер, следы преступления в частных случаях могут храниться лишь в цифровых носителях информации, а успешное закрепление следов преступлений зависит от профессионализма должностного лица органа предварительного расследования в применении действующего уголовно-процессуального законодательства. Например, согласно изменениям уголовно-процессуального законодательства, имевшим место в 2021 г., был выделен осмотр компьютерной информации в самостоятельное следственное действие наряду с другими следственными действиями, такими как осмотр места происшествия, предметов и документов, помещения, жилища и иного законного владения.

Согласно п. 5 ч. 1 ст. 37 Уголовно-процессуального кодекса (УПК) Республики Беларусь Государственный пограничный комитет, территориальные органы пограничной службы, орган пограничной

службы специального назначения является государственным органом, уполномоченным осуществлять дознание по уголовным делам о преступлениях, выявляемых при выполнении возложенных на органы пограничной службы задач, которыми являются: участие в проведении государственной пограничной политики, обеспечение пограничной безопасности, охрана Государственной границы Республики Беларусь, организация взаимодействия и координация деятельности государственных органов и иных организаций в области проведения государственной пограничной политики и обеспечения пограничной безопасности, предупреждение, выявление и пресечение преступлений и административных правонарушений, создающих угрозу пограничной безопасности, осуществление пропуска через Государственную границу граждан Республики Беларусь, иностранных граждан и лиц без гражданства, за исключением пунктов пропуска через государственную границу, в которых такой пропуск осуществляется таможенными органами, а также товаров в пунктах упрощенного пропуска через государственную границу.

В настоящее время органы пограничной службы выполняют задачи в условиях резкого осложнения миграционной обстановки на границе со странами Евросоюза. События, происходившие в течение 2021 г., показали, что Республика Беларусь в полном объеме выполняет работу по предотвращению нелегальной миграции. Ее причины кроются в поддержке отдельными странами цветных революций в регионах, где из-за них разрушен привычный уклад жизни или идет война.

Незаконные проявления в сфере миграции иностранных граждан и лиц без гражданства в Республике Беларусь также могут иметь разновекторную оценку при определении демографической ситуации в стране. С одной стороны, миграция позволяет сгладить последствия демографического кризиса, с другой – является крайне негативным фактором, ухудшающим криминогенную ситуацию в государстве. Данную ситуацию отметил Президент Республики Беларусь А.Г. Лукашенко в своем Послании белорусскому народу и Национальному собранию: «К сожалению, до сих пор определяющим фактором роста численности населения Беларуси является миграция».

Основными техническими средствами преступления, содержащими информацию со следами преступления, могут выступать компьютерные устройства, автоматизированные информационные системы и сети, в том числе интернет. В таких устройствах хранятся и обрабатываются самые разнообразные данные. Подобная информация может быть получена в ходе проведения процессуальных действий из компьютерных устройств, компьютерной системы или сети и в перспективе может являться доказательством по уголовным делам.

Предметами преступления по уголовным делам по ст. 371[1] Уголовного кодекса Республики Беларусь (организация незаконной миграции), в частности, могут выступать мобильные телефоны и планшеты операционных систем Android и iOS, ноутбуки, работающие под информационными системами Windows, MacOS и Linux, смарт-часы, которые позволяют дистанционно блокировать компьютерные устройства (режим пропажа), содержащие следы преступления.

Осмотр указанной компьютерной информации согласно ст. 204[1] УПК Республики Беларусь проводится с согласия обладателя информации и в его присутствии, по постановлению следователя, органа дознания с санкции прокурора или его заместителя, по постановлению следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном осмотре в случаях, не терпящих отлагательства.

Например, в ходе выполнения задач, возложенных на органы пограничной службы, было выявлено, что гражданин «Эн», действуя по предварительному сговору с неустановленными лицами, достоверно зная о том, что иностранные граждане вынашивают намерения незаконно мигрировать в Республику Польша в обход установленного пункта пропуска, за денежное вознаграждение в размере не менее 300 долл. США и 300 р. Национального банка Республики Беларусь оказал им содействие в незаконном выезде из Республики Беларусь в страны Евросоюза, которое выразилось в доставлении последних с 13.40 по 18.35 1 января 2022 г. из г. Минска в пограничную зону.

Осмотр компьютерной информации, содержащейся в мобильном телефоне гражданина «Эн», целесообразно будет проводить с согласия собственника (обладателя информации) и в его присутствии. Согласно ч. 2 ст. 173 УПК Республики Беларусь законодателем предоставлена возможность осмотра компьютерной информации в качестве неотложного следственного действия до возбуждения уголовного дела. После получения согласия, компьютерная информация, содержащаяся в памяти мобильного телефона, подвергается осмотру, в ходе производства которого особое внимание необходимо уделить на присутствие в осматриваемом телефоне программного обеспечения, позволяющего переводить текст и звуковые сообщения с иностранного языка на русский и в обратном порядке. В результате осмотра указанной информации в большинстве случаев можно получить информацию, которая станет одним из оснований для возбуждения уголовного дела. Однако в практической деятельности может возникнуть ситуация, когда после фиксации результатов осмотра компьютерной информации, собственник мобильного телефона в целях поставить под сомнение факт дачи разрешения на его осмотр, отказался от подписи в указанном протоколе. Согласно смыслу ст. 204[1] УПК Республики Беларусь указание по количественному ограничению производства осмотра компьютерной информации одного и того же мобильного телефона отсутствует, в связи с чем предлагается в случае получения согласия на производство осмотра компьютерной информации, содержащейся в памяти мобильного телефона, и дальнейшим отказом от подписи протокола следственного действия, фиксирующего результаты его проведения, необходимо получить санкцию на производство осмотра с последующим повторным его проведением с предъявлением постановления о производстве осмотра компьютерной информации, санкционированного прокурором либо его заместителем.

УДК 343.123.66

П.М. Титов

РАССМОТРЕНИЕ УГОЛОВНЫХ ДЕЛ ЧАСТНОГО ОБВИНЕНИЯ СУДАМИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Настоящее время характеризуется как время современных технологий, которые разрабатывают и активно внедряются во все сферы деятельности людей, управления и обороны. Под цифровыми технологиями можно понимать новейшие технические ноу-хау, которые имеют в основе своей направленность на представлении сигналов аналоговых уровней, что способствует повышению качества и переход на новый этап развития цифровой техники. Абстрагируясь от технического определения цифровых технологий, обратим внимание на внедрение цифровых технологий в уголовный процесс России. Обращаясь к словам Президента Российской Федерации В.В. Путина, который неоднократно в своих выступлениях подчеркивал, что «у нас есть и кадровый потенциал, и весомый научный задел в этой области. Уверен, что при эффективном и грамотном использовании этих возможностей страна может добиться серьезного прорыва в информационной сфере. Мы просто не должны упустить такой шанс, тем более что ряд государств достигли в этой сфере успеха, имея не такие сильные стартовые позиции». Эти слова подчеркивают потенциал в данной сфере и обозначают вектор движения дальнейшего развития. Переходя к законодательству и рассматривая его, а также работу по нему посредством контакта граждан и должностных лиц, Т.Н. Москалькова углубленно анализирует перспективы «цифрового законодательства» с внедрением электронного взаимодействия граждан и должностных лиц посредством мессенджеров, чатов или электронных приемных, подчеркивает актуальность

широкого применения цифровых технологий и в уголовно-процессуальной деятельности. В настоящей статье, полагаем, следует остановиться именно на реализации в жизни цифровых технологий, а именно, взяв узкое ее применение, а именно в рассмотрении уголовных дел частного обвинения судами.

Говоря о цифровых технологиях, применяемых в судах, в первую очередь стоит подразумевать видеоконференц-связь (ВКС), которая нашла свое широкое применение, так как ее применение упрощает работу суда с лицами, которые находятся на расстоянии и по тем или иным причинам не явились в зал судебного заседания. Так, А.В. Казакова в статье упоминает об удобстве использования ВКС, но при этом подчеркивает невозможность ее использования, если лицо находится за пределами нашего государства, Российской Федерации. С вышеизложенным можно согласиться, так как ВКС, используемая в государственных органах, в том числе и в суде, может применяться только в Российской Федерации, так как имеет определенную степень защиты из вне. Сегодня многие страны мира широко применяют цифровые технологии в уголовном судопроизводстве в целом и при рассмотрении дел в суде в частности. Это уже не новая практика применения ВКС. Однако мало случаев подтверждения того, что ВКС применяется при рассмотрении уголовных дел частного обвинения. В первую очередь, из-за того что по данной категории дел участвует в самом разбирательстве и поддерживает обвинение частный обвинитель, а не государственный. Во-вторых, лица, проходящие по таким делам с любой из сторон, в большинстве случаев не находятся, например, в местах лишения свободы и имеют возможность самостоятельно прибыть в суд. Актуальность ВКС, как нам видится, по делам частного обвинения будет тогда, когда лицо, подавшее заявление, находится в местах лишения свободы или в иных местах, где предстоит провести значительное время, примером может также служить больница, где человек проходит лечение.

Стоит обратить внимание на критерии допустимости использования цифровых технологий в уголовном судопроизводстве и выделить их: «законность, соблюдение прав и законных интересов личности, актуальность и открытость их применения». При использовании всех цифровых технологий необходимо помнить и о рисках, связанных с их использованием. ВКС технологично имеет свою степень защиты, но в век прогресса, как показывает практика, все бурно развивается, в том числе и средства противодействия. Поэтому, применяя цифровые технологии, в том числе и при рассмотрении уголовных дел частного обвинения по существу, необходимо обращать внимание на методы защиты применяемых цифровых технологий, которые должны не просто упростить работу суда, но и, главным образом, не навредить, особенно от разглашения сведений, охраняемых законодательством Российской Федерации.

С.В. Зуева и А.С. Титова раскрывают в статье слабые стороны цифровизации уголовного судопроизводства с позиции механизма правового регулирования. Однако на слабые стороны всегда найдутся сильные, которые покажут жизнеспособность и, что немаловажно, применяемость. Л.В. Головко с осторожностью относится к цифровизации уголовного судопроизводства в целом и обращает внимание на то, «что самый мощный научно-технологический прорыв в истории человечества 20–60-х гг. прошлого века не привел к созданию ”космического уголовного процесса“ или ”лунной подследственности“». Полагаем, с точкой зрения вышеуказанного автора можно согласиться, так как цифровизация в первую очередь должна быть безопасной.

Таким образом, используя цифровые технологии при рассмотрении уголовного дела частного обвинения, необходимо обращать внимание на защиту данных. При этом широкое использование данных технологий ускоряло бы рассмотрение уголовных дел, способствовало незатягиванию самого рассмотрения и в конечном итоге приводило бы к более оперативному и всестороннему рассмотрению уголовного дела.

УДК 343.985

А.Н. Тукало, С.В. Король

О НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Использование глобальной компьютерной сети Интернет (далее – Интернет) в повседневной жизни является нормой для каждого человека. Интернет и компьютерные технологии стремительно проникли во все сферы жизнедеятельности человека. Несмотря на неопровержимую полезность Интернета, он таит в себе множество опасностей. В настоящее время мир захлестнула проблема совершения преступлений в сфере информационных технологий. Это не только преступления, связанные с хищением денежных средств или личной информации. Посредством Интернета также совершаются вымогательства, мошенничества, распространение наркотиков и детской порнографии, преступления экстремистской направленности, груминг, кибербуллинг и т. д.

Опережающие темпы освоения Интернета в Республике Беларусь являются одним из стимулирующих факторов рассматриваемого вида преступлений. Беларусь вышла на среднеевропейские показатели по

плотности широкополосного доступа в Интернет, а если говорить о скорости передачи данных – на передовые в мире позиции.

На протяжении последних лет наблюдается волнообразный рост количества регистрируемых киберпреступлений. Изучение и анализ международного опыта показывает, что подобная тенденция к росту свойственна большинству стран мира. В связи с постоянным бурным развитием общественных отношений в сфере информационных технологий, тенденции к росту преступлений в данной сфере будут сохраняться.

Государством уделяется повышенное внимание обеспечению защищенности информационного пространства, информационной структуры, информационных систем и ресурсов. Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 утверждена Концепция информационной безопасности Республики Беларусь (далее – Концепция). В рамках реализации Концепции противодействие киберпреступности возложено на Министерство внутренних дел (МВД) Республики Беларусь. На основании Концепции разработан «Комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021–2022 годы» (далее – Комплексный план), в рамках которого в целях повышения эффективности борьбы с вышеуказанной проблемой одним из направлений деятельности обозначена «необходимость объединения усилий государственных органов, общественных объединений, гражданских инициатив, направленных на повышение уровня компьютерной грамотности и цифровой безопасности граждан».

Стоит отметить, что уровень киберграмотности населения не в полной мере соответствует скорости внедрения тех или иных информационных процессов в повседневную жизнь. Существует также формализм в отношении граждан к собственной информационной безопасности, который часто является последствием непонимания реальности угрозы рассматриваемого вида преступлений.

Согласно исследованию, проведенному GlobalWeblndex совместно с Snap Inc. в 2019 г. (соответственно, показатели, полученные в ходе исследования, с каждым годом, в связи с процессом информатизации общества, увеличиваются), у 97 % представителей так называемого поколения Z (молодые люди, родившиеся между 1997 и 2015 гг.) есть мобильный телефон. В данную категорию входят учащиеся школ, которые, в силу своего возраста, не всегда могут распознать обман, мошеннические действия или же иные истинные цели злоумышленника, находящегося по ту сторону Интернета.

С целью повышения компьютерной грамотности населения, считаем целесообразным ввести изучение форм и методов информационной безопасности в учреждениях дошкольного и среднего образования. Данное направление нашло свое частичное отражение в вышеприведенном Комплексном плане в разд. «Профилактические мероприятия» (п. 35, 36, 39, 40, 41, 42, 45, 51).

Анализ указанных пунктов позволяет сделать выводы о том, что профилактические мероприятия в учреждениях образования проводятся на классных (кураторских) часах, в том числе с представителями правоохранительных органов; профилактические мероприятия включают в себя проведение конкурсов, размещение листовок на стендах, распространение информации на интернет-ресурсах, освещение вопросов ответственности за правонарушения, распространение листовок среди учащихся по данной тематике; организация методических сборов на тему «Деятельность специалистов социально-психологической службы по обучению учащихся навыкам информационной безопасности».

Несмотря на целенаправленную профилактическую работу со стороны учреждений образования и подразделений криминальной милиции, рассматриваемый вид преступлений составляет существенное количество от общего числа совершаемых преступлений. Это связано с тем, что способы совершения таких преступлений постоянно совершенствуются.

На наш взгляд, профилактика киберпреступлений была бы более эффективной, если бы поток профилактической информации был приведен в единую систему и подавался поступательно и постоянно. Любая познавательная деятельность должна сопровождаться изучением основ в той или иной отрасли. В силу возраста учащиеся должны получать информацию, начиная с основ информационной безопасности и структуры киберпреступности и заканчивая мерами по ее предупреждению и профилактике. Исходя из изложенного, считаем целесообразным ввести в учебную программу учреждений образования учебную дисциплину «Кибергигиена».

Полагаем, что повышение эффективности профилактики киберпреступлений возможно посредством поступательного обучения основам информационной безопасности с раннего возраста специалистами учреждения образования во взаимодействии с сотрудниками подразделений криминальной милиции. К подготовке учебной программы необходимо привлечь все заинтересованные органы (в том числе профильные отделы Министерства образования, учреждения образования МВД Республики Беларусь, подразделения криминальной милиции и т. д.).

Кроме этого, целесообразно ввести отдельные занятия в старших группах детских дошкольных учреждений, где в игровой форме доводить детям основы кибербезопасности (в том числе приглашать кур-

сантов учреждений образования МВД Республики Беларусь, сотрудников подразделений криминальной милиции для проведения различных мероприятий по обучению навыкам информационной безопасности).

В целях выработки наиболее оптимальных путей повышения эффективности борьбы с киберпреступностью в Республике Беларусь посредством более тесного взаимодействия граждан и организаций с правоохранительными органами считаем необходимым продолжить изучение рассматриваемой проблематики в рамках комплексного исследования, в котором будут изучены ее правовые, социальные, психологические и иные аспекты.

УДК 343.9

Д.Д. Урстенова

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

В наше время наступила информационная эра, т. е. переход от традиционной индустрии промышленности к оцифрованной, компьютеризованной индустрии, направленный на моментальный обмен информации, что послужило началом цифровой революции во всех сферах жизни человечества. В своем послании Глава государства Президент Республики Казахстан Касым-Жомарт Токаев пояснил, что «Цифровизация – это не следование модной тенденции, а ключевой инструмент достижения национальной конкурентоспособности. Прежде всего предстоит устранить цифровое неравенство, обеспечить максимальный доступ к интернету и качественной связи для всех граждан. Сегодня это такая же базовая потребность, как дороги и электричество» [1]. В период всеобщей цифровизации правительства и экономических процессов преступность трансформируется под современные реалии.

Мошенничество в сети Интернет на данный момент имеет масштабный характер, о чем свидетельствуют статистические данные регистрации уголовных правонарушений. Преступники используют все более изощренные способы и методы совершения мошенничества в сети Интернет, что даже самые бдительные граждане попадаются на ловушку преступника.

В настоящее время в интернет-ресурсах Казахстана имеется огромное количество онлайн-сервисов объявлений (olx.kz, krisha.kz, kolesa.kz и т. д.), которые содержат различные виды услуг, купли-продажи и т. д.

Каждый пользователь сети Интернет может выставить любое объявление без указания достоверных личных данных и описание товара или услуги. Проверить достоверность данных пользователей не предоставляется возможным, так как затрагивает права человека, указанные в Законе Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите».

Во всем цивилизованном мире права человека стоят на первом месте и защищаются международными соглашениями, такими как Международный пакт о гражданских и политических правах (International Covenant on Civil and Political Rights – ICCPR) и Всеобщая декларация прав человека (Universal Declaration of Human Rights – UNDP). Анонимность – это невозможность идентифицировать субъект. Также это не допускает возможности несанкционированного использования персональной информации, которой могут воспользоваться в корыстных целях.

Однако у данного утверждения имеется обратная сторона, так как то, что нельзя контролировать, может быть опасным. Вопрос о защите персональных данных пользователей сети Интернет с правовой точки зрения был не до конца изучен. Республика Казахстан при форсированном развитии цифровизации и почти полном переходе документооборота в цифровой формат параллельно проводит законотворческую работу по изменению законодательства с целью наиболее качественной защиты персональных данных граждан.

Так, по мнению К.В. Кецко, для субъектов электронной коммерции анонимность в сети Интернет, с одной стороны, является преимуществом, с другой – вызывает опасения участников, несет определенные риски, в частности, доступность внешнего проникновения, спам-атаки, создание сайтов-дубликатов [2].

Другие авторы относят анонимность в сети Интернет к проблемам правового регулирования цифровых технологий, связанным с реализацией прав и свобод граждан. Они утверждают, что анонимность пользователя – это его конституционная гарантия, обеспечивающая охрану тайн его личной жизни. При этом авторы не исключают ограничение анонимности, когда она используется во вред охраняемым законом общественным отношениям [3].

Сегодня на просторах глобальной компьютерной сети Интернет имеются различные фишинговые сайты, с помощью которых интернет-мошенники осуществляют преступные деяния в сети Интернет.

Фактической профилактикой интернет-мошенничества занимаются как правоохранительные органы, так и государственные структуры, кроме того и IT-гиганты, такие как Google, Yandex и др. Кроме того, профилактикой занимаются и субъекты предпринимательской дея-

тельности – банки, крупные корпорации, операторы сотовой связи, организации, занимающиеся разработками IT-продуктов, другие организации и физические лица, так или иначе заинтересованные в информационной безопасности в сети Интернет.

Список использованных источников

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана [Электронный ресурс] // Президент Республики Казахстан : офиц. сайт. – URL: http://https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048 (дата обращения: 01.09.2022).

2. Кецко, К.В. Преступность в сфере электронной коммерции / К.В. Кецко // Рос. следователь. – 2021. – № 9. – С. 58–63.

3. Уваров, А.А. Проблемы использования цифровых технологий при реализации прав и свобод граждан / А.А. Уваров // Право и цифровая экономика. – 2020. – № 2. – С. 5–11.

УДК 343.918.2

И.А. Фомина

ТИПОЛОГИЯ ЛИЧНОСТИ КИБЕРПРЕСТУПНИКА ПО ПАРАМЕТРАМ НАПРАВЛЕННОСТИ

Киберпреступность как правовая, практическая и политическая проблема представляет собой прямую угрозу правам человека, общества и государства. Ее большая опасность в том, что современное развитие мира немыслимо без телекоммуникационных систем. Наш современный мир – цифровой мир, где есть место не только новым возможностям, но и рискам. Рост и прогресс цифровых технологий создали совершенно новую платформу для преступной деятельности. Соответственно, перемещение преступности в киберпространство вполне закономерно – это диктует необходимость перепрофилирования не только правоохранительных органов, но и изменения научных исследований в этом направлении, с учетом особенностей киберпространства. Из-за технологических достижений киберпреступность обычно относится к преступлениям, в которых компьютерная сеть используется в незаконных целях, таких как кража конфиденциальных данных, мошенничество, отмывание денег и детская порнография. С развитием технологий появляются и виды киберпреступлений, которые совершают преступники. При этом киберпреступность принимает различные формы, включая хакерство, распространение вредоносного программного обеспечения, программ-вымогателей, фишинг и др. Многие виды ки-

берпреступности являются продолжением существующей офлайн преступной деятельности, поскольку компьютеры и интернет отделили их от географического местоположения преступника, обеспечивая анонимность и защиту от судебного преследования.

Лица, активно использующие киберпространство в своих преступных целях, обладают специфическими, характерными для них характеристиками целей и мотивов, позволяющими классифицировать (объединить) их по параметрам направленности. Благодаря точной типизации потенциальных киберпреступников, сотрудники правоохранительных органов, занимающиеся предупреждением киберпреступлений, лучше понимают, кто такие киберпреступники, какие методы они используют и какие контрмеры могут быть приняты для защиты и предотвращения будущих киберпреступлений.

Следует иметь в виду, что киберпреступники – это, обычно, отдельные лица или небольшие группы. Однако существуют также крупные и высокоорганизованные группы, которые способны проводить массовые целенаправленные атаки. Они относятся к киберпреступности как к бизнесу, даже формируя глобальные сообщества, которые разделяют стратегии и инструменты. Они могут объединять силы для проведения скоординированных атак и обмена украденными личными данными и информацией на своем подпольном рынке.

Киберпреступники широко представлены в так называемой Dark Web, где они в основном предоставляют свои незаконные услуги или продукты. При этом, так как киберпреступность представлена в двух разновидностях: как преступная деятельность, нацеленная на компьютеры, использующие вирусы и другие типы вредоносных программ, и как преступная деятельность с использованием компьютеров для совершения других преступлений, то в рамках деления киберпреступников по параметрам направленности целесообразно выделять:

киберпреступников, нацеленных на компьютеры (могут например, заражать их вредоносными программами, чтобы повредить устройства или остановить их работу; могут использовать вредоносные программы для удаления или кражи данных; могут помешать пользователям использовать интернет или помешать бизнесу предоставлять программные услуги своим клиентам, т. е. атака по типу «отказ в обслуживании» (DoS));

киберпреступников, которые используют компьютер для совершения других преступлений, когда происходит использование компьютеров или сетей для распространения вредоносных программ, незаконной информации, предметов или незаконных изображений (например, наркопреступление, детская порнография, кибертерроризм и др.);

киберпреступников, которые совмещают в себе два типа: делают и то, и другое одновременно. Они могут сначала заражать компьютеры

вирусами, а затем использовать их для распространения вредоносных программ на другие компьютеры или по всей сети. Могут вносить вирусы, которые делают рассылки по пользователям, в которых будет содержаться, например, информация-реклама «дизайнерских наркотиков» или мошеннические сообщения.

Установление направленности личности преступника помогает в первую очередь в квалификации их действий, особенно если имеет место быть подготовка или покушение. Кроме того, деление по направленности позволяет разработать целенаправленные профилактические мероприятия.

УДК 343.98

Р.С. Хамидуллин, А.А. Староверов

ВЫЯВЛЕНИЕ НЕЗАКОННОГО ПРИОБРЕТЕНИЯ И СБЫТА ОГНЕСТРЕЛЬНОГО ОРУЖИЯ, СОВЕРШАЕМОГО ЧЕРЕЗ ТЕНЕВЫЕ РЕСУРСЫ СЕТИ ИНТЕРНЕТ

Стремительное развитие торговли в сети Интернет и социальных сетях приводит к росту количества преступлений в сфере незаконного оборота оружия, оборота наркотических средств, поддельных денежных средств и знаков. Актуальность данной работы связана с быстрым ростом преступлений, совершаемых в теневом секторе сети Интернет, а также с высокой сложностью раскрытия этих преступлений. Так, по данным Главного информационно-аналитического центра МВД России, с января по октябрь 2022 г. совершено 429 245 преступлений с использованием информационно-телекоммуникационной сети Интернет, преступлений, связанных с незаконным оборотом оружия, на территории Российской Федерации зарегистрировано 19 158.

В настоящее время интернет является основной площадкой для продажи наркотиков, оружия, сбыта похищенного имущества. Люди создают множество сайтов и веб-страниц, благодаря которым возможно осуществление покупок и продаж подобных вещей, находясь в любой точке планеты. В связи со сложившейся криминогенной обстановкой в мире отдельное внимание следует уделить преступлениям в сфере незаконного оборота оружия, совершаемым с помощью теневых браузеров (DuckDuckGo, Tor, Whonix). Так, на торговой площадке THIEF можно приобрести оружие любого калибра для любых целей – от простых пистолетов до противотанковых ракетных комплексов (например, ПТРК Javelin). К слову, через эту платформу совершено уже более 2 000 сделок.

Минимальная связь между преступными элементами (покупатель, продавец) доставляет значительные трудности по выявлению, раскрытию и расследованию преступлений, связанных с незаконным оборотом оружия. Это связано с тем, что ни покупатель, ни продавец не видят друг друга и даже не встречаются при осуществлении сделки, в данном случае используется способ демонстрации и бесконтактной оплаты – продавец размещает объявление и прикрепляет к нему фотографии или видео, чтобы покупатель смог увидеть товар, покупатель, в свою очередь, посредством перевода криптовалюты на счет продавца осуществляет покупку. Вследствие чего при задержании покупателя или продавца ни один из них не может дать какой-либо информации о другом.

Серьезную проблему составляет также тот факт, что продажа осуществляется через теневые сектора сети Интернет DarkNet. С помощью этой сети так называемые оружейные бароны осуществляют незаконную продажу огнестрельного оружия и патронов к нему. В сети размещаются специальные платформы, например THIEF, где и находятся объявления по продаже оружия и патронов. Эти площадки позволяют покупателю и продавцу действовать анонимно.

Специалисты в области киберпреступности сходятся во мнении, что в странах с большим количеством интернет-пользователей все чаще для незаконной покупки и продажи оружия используется DarkNet. Такая ситуация складывается вследствие того, что способ оплаты, как и где она производилась, отследить почти невозможно. Цифровизация процессов с помощью blockchain-технологий не в полном объеме дает сотрудникам правоохранительных органов осуществлять физический и юридический контроль по финансовым операциям.

Все расчеты в DarkNet осуществляются при помощи криптовалюты, которую покупатель приобретает на специальном обменнике. После этого покупатель выбирает необходимый ему товар и производит оплату, криптовалюта переводится на счет продавца, который подтверждает оплату. Сам продавец также при помощи обменника должен провести операцию по переводу криптовалюты в фиатную валюту (доллары, евро, рубли и т. д.).

Важной особенностью при покупке оружия через теневые сети является способ общения покупателя и продавца. Сегодня существует множество разных мессенджеров, однако наиболее часто используемым для таких целей является Telegram. Он представляет собой анонимную среду с огромным функционалом, одним из которых является возможность создавать ботов, выполняющих определенные функции. В сети Telegram применяется несколько протоколов шифрования (MTProto 2.0 и MTProxy), что обеспечивает шифрование сообщений при их передаче и получении, а также лиц, их отправляющих. Так, в 2019 г. гражданин за-

казал автомат Калашникова через теневую интернет-платформу DarkNet. Связь с продавцом осуществлялась посредством использования сети Telegram. После проведения оплаты товара продавец отправил покупателю сообщение с координатами тайника оружия, сам же автомат был закопан рядом с деревом, которое служило ориентиром. По прибытии на место покупатель выкопал тайник с автоматом и наглядно продемонстрировал его на видеокамеру.

Рис. 1. Гражданин П. получил координаты от продавца и направляется к месту нахождения тайника

Рис. 2. Гражданин П. прибыл к месту, где находится тайник

Рис. 3. Гражданин П. выкапывает автомат. Автомат завернут в тряпку

Рис. 4. Гражданин П. демонстрирует на видеокамеру автомат АК-47

Особенностью при проведении оперативно-розыскных мероприятий при пресечении незаконного оборота оружия через теневые браузеры является возможность их проведения на первоначальном этапе стадии возбуждения уголовного дела. Если в ходе проведения оперативно-розыскных мероприятий удается установить данные Telegram-аккаунта лица, то оперативные сотрудники могут установить все проводимые лицом операции (отправление и получение фиатных денежных средств, сообщения с покупателем или продавцом, данные о местонахождении тайников-закладок). Следовательно, проведение оперативно-розыскных мероприятий способствует полному, всестороннему и качественному получению информации и сбору доказательственной базы для расследования уголовного дела.

Для полного, своевременного и всестороннего раскрытия и расследования преступлений в области незаконного оборота оружия через теневые браузеры необходимо сочетание оперативно-розыскных и уголовно-процессуальных методов фиксации следов преступления и собирания доказательственной базы по делу. Необходимой мерой является также привлечение специалистов из соответствующих отраслей знаний при осуществлении документирования и последующего расследования рассматриваемых преступлений на всех стадиях оперативно-розыскной и процессуальной деятельности [1].

Итак, продуктивной мерой повышения эффективности работы правоохранительных органов в борьбе с незаконным оборотом оружия, совершаемым посредством теневых сетей, будет пересмотр организационно-тактических мер в отношении дел такой категории. Оперативно-розыскное обеспечение должно осуществляться безотрывно, как в рамках расследования уголовного дела, так и в рамках последующего судебного сопровождения.

Список использованных источников

1. Петухов, А.Ю. Современные тенденции использования средств теневого Интернета при совершении преступлений в сфере незаконного оборота наркотиков / А.Ю. Петухов, К.С. Куликов // Науч. компонент. – 2019. – № 1(1). – С. 22.

УДК 343.985

Д.Л. Харевич

О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ НЕКОТОРЫХ ДЕЙСТВИЙ ИНФОРМАЦИОННОГО ХАРАКТЕРА В ХОДЕ НЕГЛАСНОГО РАССЛЕДОВАНИЯ В ФЕДЕРАТИВНОЙ РЕСПУБЛИКЕ ГЕРМАНИЯ

Негласное расследование (verdeckte Ermittlung) в Федеративной Республике Германия (ФРГ) представляет собой собирательный термин, означающий негласные виды деятельности, осуществляемые в целях превенции (предотвращения опасности) либо в целях преследования и предупреждения уголовно наказуемых деяний (в репрессивных целях). Негласное расследование, проводимое в превентивных целях, регламентируется полицейским правом. Основу законодательной базы негласного расследования, осуществляемого в репрессивных целях, составляет уголовно-процессуальное законодательство. Содержание негласного расследования составляют негласные методы, направленные на получение информации. Нормативно регламентированы лишь те методы, которые затрагивают основные права граждан.

Длительное время действия, связанные с обработкой персональных данных, не рассматривались как вторжение в основные права гражданина и требующие законодательной регламентации. В настоящее время решениями высших судебных инстанций признано, что подобные действия затрагивают право граждан на информационное самоопределение. В толковании Федерального конституционного суда ФРГ оно включает в себя право каждого гражданина принимать решение о предоставлении и использовании сведений о своей личности и о том, как он желает быть представленным в глазах других людей. Совершение указанных действий без согласия лица является нарушением рассматриваемого конституционного права. Исключения из данного правила возможны лишь в случаях, оговоренных в законе, например, если гражданин нарушает права других или посягает на конституционный строй или нравственные нормы. В этой связи в законодательстве ФРГ существует достаточно детальная правовая регламентация действий, связанных с получением и обработкой персональных данных, неоднократно являвшаяся предметом научной дискуссии и рассмотрения в Федеральном конституционном суде и конституционных судах федеральных земель.

К действиям указанного рода относятся растровый поиск и полицейское наблюдение.

Под растровым поиском (Rasterfahndung) понимается сквозной поиск по базам данных и автоматизированное сопоставление машинным способом персональных данных о лицах, которые соответствуют проверочным признакам, предположительно указывающим на определенное лицо, с другими данными, хранящимися в иных организациях, осуществляемое с тем, чтобы исключить непричастных лиц или установить лиц, представляющих интерес для расследования.

Одним из примеров успешного проведения растрового поиска является установление местонахождения и задержание члена одной из опасных террористических организаций. Во время расследования было установлено, что террористы, снимавшие квартиры от имени несуществующих лиц, оплачивали счета за электричество наличными деньгами во избежание своей идентификации по номеру счета при безналичной оплате. В связи с этим полицией были истребованы адреса, по которым осуществлялась оплата за электроэнергию деньгами. Из полученных примерно 16 000 совпадений были исключены реально существующие лица: те, кто был зарегистрирован по адресу проживания, имел местную регистрацию автотранспорта или получал пособие либо пенсию. В результате было выделено лишь два лица, при проверке оказавшихся: первый – наркодилером, второй – искомым террористом.

С тех пор существенно расширились возможности получения информации, однако алгоритм действия при проведении мероприятия остался неизменным. На первоначальном этапе растрового поиска из признаков, ставших известными в ходе расследования, осуществляется составление профиля лица (растр). После этого по относящимся к нему признакам организуются запросы в различные банки данных, содержащие соответствующую информацию. По результатам ее обработки выделяются те наборы сведений, которые удовлетворяют всем признакам. Каждое лицо, попавшее таким образом в указанный растр, подлежит более тщательной проверке.

Выделяют две разновидности растрового поиска: «позитивный» и «негативный». Примером «позитивного» растрового поиска может являться сопоставление банка данных разыскиваемых лиц с реестром регистрации граждан. На основе совпадений возможно установление места проживания таких лиц. Данный вид поиска направлен на ограничение круга лиц, подлежащих проверке иными методами. «Негативный» растровый поиск представляет собою более уникальный способ, при котором

из большого массива данных постепенно исключаются лица, не удовлетворяющие поисковым признакам, как это сделано в вышеприведенном примере с розыском террориста. Как видно, основной целью негативного растрового поиска является исключение непричастных лиц.

Рассматриваемое мероприятие охватывает лишь автоматизированное сопоставление машинным способом; мероприятия по поиску, осуществляемые вручную, попадают под регламентацию иных норм. Например, не является растровым поиском обработка данных, которые ранее получены органом уголовного преследования в результате конфискации предметов, которые могут иметь значение доказательств; ознакомления с бумагами и электронными носителями информации и их изъятия; проведения полицией любого вида расследования (дознания) и принятия ею неотложных мер. Это позволяет разграничить растровый поиск и информационно-аналитическую деятельность.

Под термином «полицейское наблюдение» (polizeiliche Beobachtung) понимается планомерное, как правило, негласное наблюдение за лицом или объектом в целях установления его полного профиля перемещения. Полицейское наблюдение подразумевает ввод персональных данных обвиняемого или номерного знака (наружного обозначения) транспортного средства в контрольную систему, которая позволяет установить персональные данные, номерной знак или наружное обозначение. Если наблюдаемый объект проезжает мимо контрольного поста, то происходит регистрация данного события. При связывании полученных данных получают профиль перемещения, позволяющий отследить передвижение и действия лица. Рассматриваемое действие также служит установлению связей между наблюдаемым и иными лицами для выявления криминальных структур и борьбы с организованной преступностью.

В качестве объекта для осуществления полицейского наблюдения могут рассматриваться лицо, автомобиль, водное судно, летательный аппарат или контейнер и др. Для составления профиля перемещения могут использоваться различные данные, свидетельствующие о местоположении или действиях того или иного лица, например, о местоположении абонента сотового телефона или объекта, оснащенного системой глобального позиционирования, о местах совершения оплаты с использованием пластиковых магнитных карточек. В качестве контрольной системы используется, как правило, федеральная полицейская информационная система Inpol-neu.

Помимо установления личных данных могут фиксироваться такие сведения, как сопровождающее или контактирующее с фигурантом лицо, водитель, маршрут, транспортное средство и перевозимые предметы.

Проведенное рассмотрение позволяет выделить профиль лица (растр) и профиль его перемещения в качестве информационных моделей конкретного события, которые могут использоваться для розыска и установления лиц, представляющих интерес; ограничения круга лиц, подлежащих дальнейшей проверке; отслеживания передвижений и действий лица. При этом возможно выдвижение обоснованных версий о причастности фигуранта к ведению противоправной деятельности либо к определенному событию, установление его связей с иными лицами, получение другой значимой информации, выявление криминальных структур и решение иных частных задач негласного расследования.

С учетом принятия Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» представляется, что изложенные положения могут представлять интерес не только с точки зрения порядка осуществления действий, но и принципов правового регулирования общественных отношений, связанных с обработкой персональных данных лиц.

УДК 343.98

А.М. Хлус

ТЕНДЕНЦИИ РАЗВИТИЯ И ИННОВАЦИИ В МЕТОДИКЕ РАССЛЕДОВАНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» внесен в Уголовный кодекс Республики Беларусь (УК) ряд изменений и дополнений. Существенные изменения коснулись уголовных статей, содержащихся в гл. 31, которая в настоящее время именуется «Преступления против компьютерной безопасности». Это обстоятельство определяет потребность совершенствования частных методик расследования преступлений данной группы. На примере преступления, предусмотренного ст. 349 «Несанкционированный доступ к компьютерной информации» УК, рассмотрим возможности совершенствования частной методики его расследования, что представляется аналогичным в связи с иными деяниями, посягающими на компьютерную безопасность.

Современные методики расследования, основываясь на полувековой традиции, формируются с учетом положений криминалистических характеристик определенного вида или группы преступлений. Не являются исключением в этом аспекте деяния, родовым объектом посягательства которых ранее рассматривалась информационная безопасность.

В качестве общих и наиболее значимых элементов криминалистической характеристики группы преступлений, посягающих на информационную безопасность, рассматривались: 1) личность преступника; 2) способы совершения преступления; 3) обстановка их совершения; 4) особенности образования следов.

Не анализируя все указанные элементы, обратим внимание, что характеристика личности преступника представлена с позиции ее криминологического понимания. Выделены три группы преступников. Одну составляют лица, совершающие деяние с целью самореализации и апробации своих навыков в сфере информационных технологий (хакеры, крэкеры, вирмейкеры). Вторая группа лиц характеризуется ярко выраженной корыстной направленностью совершаемых преступлений. К ним относятся упомянутые хакеры и крэкеры, а также компьютерные пираты. Третью группу составляют специалисты субъектов хозяйствования, государственных органов и организаций (программисты и т. п.), умышленно нарушающие правила эксплуатации компьютерной системы или сети.

Знание приведенной выше классификации преступников значимо для раскрытия и расследования преступных деяний, но в основу разработки криминалистической характеристики любого криминального деяния указанной выше группы должны быть положены сведения о материальных составляющих преступной структуры. Это дает возможность познать преступление в процессе его расследования, основываясь на следовой картине, отражаемой материальными элементами преступной системы.

Данная идея базируется на криминалистическом учении о материальной структуре преступления (А.Е. Гучок). В его основе представление о системе преступления, состоящей из ряда материальных элементов, вступающих во взаимосвязь в момент его совершения.

Учитывая положения упомянутого учения, рассмотрим материальные составляющие анализируемого преступления. В его материальной структуре можно выделить следующие материальные элементы: субъект, совершающий преступное деяние, объект и предмет преступного посягательства, средства совершения преступления.

Субъектом совершения данного преступления является человек, реализующий преступный замысел единолично либо в составе группы. Особенность субъекта рассматриваемого преступления в наличии у него специальных знаний в области компьютерной техники и информационных технологий. В преступной системе субъект вступает во взаимодействие с иными структурными элементами, оставляя на них следы преступных действий, информация о которых подлежит отражению в криминалистической характеристике. Эти следы могут быть обнаружены на средствах, которые использовались для несанкционированного доступа к компьютерной информации. Следует иметь в виду, что средства воздействия на объект отражают следы-действия (например, использование компьютерной программы для преодоления системы защиты) и материальные следы использования средства.

Субъекты неправомерного доступа к компьютерной информации подразделяются на две группы: внешние по отношению к объекту посягательства и внутренние, на которых возложены обязанности по соблюдению правил обслуживания объекта. Разновидностью последних являются близкие лица, пострадавшего от преступления (примечание к гл. 31 УК).

Объектом преступного посягательства с позиции учения о материальной структуре преступления следует считать материальную систему, на которую направлены преступные действия субъекта.

Криминалистический анализ ст. 349 УК позволяет в качестве объектов посягательства выделить компьютерные системы, сети и т. п. Данные «системы» и «сети» представляют собой непосредственный объект преступного посягательства. Но в широком понимании объектом для рассматриваемых преступлений являются организации, которым по неосторожности причиняется существенный вред или иные тяжкие последствия. Объектами выступают различные материальные системы, в отношении которых преступные действия виновного повлекли крушение, аварию, катастрофу (ч. 2 ст. 349 УК). Жертвами этих последствий могут быть люди, которых также надо рассматривать объектом посягательства.

На указанные «системы» и «сети» оказывается неправомерное воздействие, в результате которого формируется следовая картина. Криминалистическое исследование информации, содержащейся в следах, отраженных на объекте посягательства, обеспечивает познание иных, как правило, неизвестных на первоначальном этапе расследования элементов материальной структуры.

В тесной связи с объектом находится предмет преступного посягательства, в качестве которого нами понимается материальный элемент преступной системы, определяющий целевую направленность деяния. На основе анализа ч. 1 и 2 ст. 349 УК можно сделать вывод, что таким предметом выступает информация.

Неправомерный доступ к информации предполагает использование средств совершения преступления, в качестве которых используются материальные системы, обеспечивающие воздействие на объект и достижение цели доступа к компьютерной информации. Доступ к компьютерной информации путем нарушения системы защиты осуществляется посредством средств компьютерной техники с возможным использованием специальных компьютерных программ.

Выделение элементов материальной структуры рассматриваемого преступления не является самоцелью и не противопоставляется уче-

нию о криминалистической характеристике. Для формирования теоретической основы построения частной методики расследования необходимо, по нашему мнению, первоначально рассмотреть типичные элементы материальной структуры преступления, которые затем подлежат описанию (характеристике) в аспекте криминалистически значимой для расследования информации. Такое сочетание двух различных по своей сути криминалистических научных категорий можно представить в виде «криминалистической характеристики материальной структуры преступлений».

На основе вышерассмотренного для обсуждения предлагаются следующие выводы.

Во-первых, разработка криминалистических характеристик отдельных видов преступлений против компьютерной безопасности не дает о них полного представления и не может служить надежной основой для построения частных методик их расследования.

Во-вторых, в основу криминалистической характеристики отдельных видов преступлений против компьютерной безопасности должны быть положены сведения о типичных элементах материальной структуры данных видов преступлений.

УДК 343.98

А.В. Ходасевич

КРИПТОВАЛЮТА КАК ПРЕДМЕТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА ПО ДЕЛАМ О ХИЩЕНИЯХ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В настоящее время операции, совершаемые с использованием криптовалюты, получили широкое распространение. Базовые принципы функционирования криптовалютной индустрии, а именно: анонимность при проведении операций, отсутствие надлежащего контроля со стороны какого-либо государства в момент покупки и продажи такой валюты, трансграничность позволили представителям преступного сегмента использовать криптовалюту при совершении противоправных действий. Активное распространение манипуляций злоумышленников с операциями с использованием криптовалюты не позволяют законодателю в таком же темпе менять существующие правовые нормы под возникающие реалии цифрового общества.

Непосредственно суть каждой криптовалюты состоит в том, что она является своеобразным «денежным эквивалентом» и состоит из электронной записи (числовых единиц), которая используется участниками расчетов для проведения операций. При этом курс криптовалюты относительно той или иной валюты формируется спросом и предложением на рынке, функционирование же такой системы происходит децентрализованно в распределенной компьютерной сети, где платежная единица – это некая электронная монета. Поэтому, исходя из сути механизма, заложенного в процедурах покупки и продажи криптовалюты, возникает вопрос, можно ли криптовалюту отнести к предмету преступления по делам о хищениях имущества путем модификации компьютерной информации и какова в целом ее природа?

Поскольку предметом преступления по делам о хищениях имущества путем модификации компьютерной информации выступает имущество, что следует как из названия ст. 212 Уголовного кодекса Республики Беларусь (УК), так и из диспозиции данной статьи, то первоначально следует ответить на вопрос: «Какое именно содержание законодатель вкладывает в понятие «имущество?».

В комментарии к УК для определения понятия «имущество» как предмета посягательства против собственности принято выделять три признака имущества: физический признак (включает в себя такую характеристику предмета, как материальность, т. е. вещи, деньги, ценные бумаги и иные предметы материального мира, не лишенные своей вещной субстанции), экономический признак (вещь должна иметь стоимостный эквивалент), юридический признак (имущество должно быть чужое – принадлежать иному лицу, которое, соответственно, приобрело его и является собственником). В комментарии к гл. 24 УК к предмету хищений относится и право на имущество – полномочия собственника по владению, пользованию и распоряжению имуществом.

Однако криптовалюта не является ни видом денежных средств, в том числе электронных, ни видом ценных бумаг. В Декрете Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» под криптовалютой понимается биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена.

Данного определения недостаточно для отнесения криптовалюты к понятию «имущество», так как указание на суть криптовалюты как на средство обмена не позволяет в полной мере понять ее природу. При этом, как мы отмечали выше, криптовалюта имеет определенный денежный эквивалент. Приобретая некоторое количество криптовалюты, пользователь уплачивает определенную сумму денежных средств и

получает «товар», владеть, пользоваться и распоряжаться которым может при наличии у него сведений об определенном наборе символов. Но криптовалюта лишена своей вещной составляющей, она существует только лишь виртуально (аппаратный криптокошелек не принимается во внимание в связи с тем, что в рассматриваемом контексте интерес представляет лишь количество криптовалюты, хранящейся на нем, а не непосредственно устройство).

Итак, вывод: криптовалюту можно приравнять к имуществу, а хищение криптовалюты путем модификации компьютерной информации следует квалифицировать по ст. 212 УК. Данный вывод сделан путем расширенного толкования, проведения аналогий, тогда как в действующем законодательстве он не нашел своего закрепления.

Существующий пробел в нормативно-правовом регулировании имущественного оборота криптовалюты создает почву для нарушения интересов пользователя в обладании данным электронным средством обмена.

Учитывая, что задача уголовного закона сводится к защите прав и свобод человека и гражданина, полагаем, что отсутствие законодательного закрепления статуса криптовалюты недопустимо. Очевидно, что расширение представлений о предмете преступного посягательства в преступлениях против собственности социально обусловлено и необходимо не только с позиций защиты законных интересов граждан от посягательств на принадлежащие им блага.

Можно отметить, что законодатель, исследователи при определении понятия «имущество» не могли предвидеть саму возможность существования имущества в каком-то нематериальном, отличном от предметов внешнего мира, виде. При этом все приведенные позиции, относительно сути определения понятия «имущество», актуальны до настоящего времени, устарело только лишь содержание физического признака. Для устранения существующих противоречий необходимо законодательно закрепить понятие «имущество». При этом под имуществом следует понимать любое благо, которое имеет экономическую ценность, признается объектом экономического оборота – принимает товарную форму, имеет стоимостное выражение, может выражаться в электронном цифровом виде.

УДК 343.985

А.А. Чехович

НЕКОТОРЫЕ АСПЕКТЫ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Развитие современного общества характеризуется повсеместным распространением информационно-коммуникационных технологий и активным развитием киберпространства. Ключевым явлением в развитии информационной сферы стало появление персональных компьютеров, а в последующем, в конце XX в., появление компьютерных сетей, в том числе сети Интернет. Благодаря компьютерным сетям финансовая, торговая, промышленная, правоохранительная и другие сферы деятельности вышли на качественно новый уровень. Сеть Интернет не только предоставила людям возможности мгновенной, непрерывной и недорогой связи по всему миру, но и стала всеобъемлющим информационным ресурсом, не имеющим аналогов и альтернативы. Указанная сеть динамична, она постоянно изменяется, обеспечивая своих пользователей новыми технологиями доступа и вариантами обмена информацией, при этом она никому не принадлежит, а также является трансграничной. Благодаря сети Интернет появился новый способ оборота информации, ее носителями стали персональные компьютеры, переносные электронные устройства хранения и передачи информации и компьютерные сети, а отдельные виды информации трансформировались в компьютерную информацию.

Вместе с тем развитие информационных технологий открыло и новые возможности для совершения преступлений с помощью персонального компьютера, как при совершении традиционных преступлений, например, мошенничества, фальшивомонетничества, незаконного оборота наркотиков, так и при совершении принципиально новых, ранее неизвестных обществу противоправных деяний – киберпреступлений.

К числу общественно опасных и латентных киберпреступлений, связанных с нарушением компьютерной безопасности, относится несанкционированный доступ к компьютерной информации, ответственность за который предусмотрена ст. 349 Уголовного кодекса Республики Беларусь. Его общественная опасность в значительной степени предопределяется использованием цифровых технологий для совершения многих других умышленных преступлений, в том числе тяжких и особо тяжких.

Необходимо отметить, что сложность раскрытия преступлений в сфере компьютерной безопасности, в частности несанкционированного доступа к компьютерной информации обусловлена рядом причин:

быстрое старение компьютерных знаний и навыков (новые образцы компьютерной техники и программного обеспечения появляются настолько быстро, а число фирм-производителей так велико, что даже специалисту трудно уследить за нововведениями);

информационные процессы протекают с очень высокими скоростями, что отрицательно сказывается на сборе доказательств;

преступления в сфере компьютерной безопасности могут совершаться специалистами в этой области знаний, что обусловливает наличие определенного уровня противодействия;

несовершенство законодательной базы, регулирующей отношения в сфере оборота информации.

В этой связи в настоящее время правоохранительная практика стала нуждаться в разработке научно обоснованных рекомендаций по совершенствованию деятельности по выявлению и пресечению несанкционированного доступа к компьютерной информации.

Высокотехнологичный характер совершения преступлений против компьютерной безопасности значительно осложняет не только их раскрытие, но и квалификацию. Как в теории, так и в практике применения ст. 349 Уголовного кодекса Республики Беларусь существуют проблемные аспекты. При применении термина «компьютерная информация» допускается неверное его толкование, не соответствующее действительности представление о значении правовых последствий. Присутствует неоднозначность при определении места совершения преступлений данного вида.

Существует необходимость анализа практики противодействия несанкционированному доступу к компьютерной информации как в Республике Беларусь, так и за рубежом, в том числе государствах, являющихся стратегическими партнерами Республики Беларусь в области противодействия киберпреступности и правоохранительной сферах. Имеется также потребность в теоретическом обосновании и определении содержания оперативно-розыскной характеристики несанкционированного доступа к компьютерной информации. Не менее востребованным представляется исследование вопросов, касающихся способов и обстоятельств совершения несанкционированного доступа к компьютерной информации.

Развитие теории оперативной-розыскной деятельности детерминирует потребность обращения к проблеме проведения отдельных видов оперативно-розыскных мероприятий, не характерных для получения информации о лицах, совершивших несанкционированный доступ к компьютерной информации. В целях наиболее полного и всестороннего установления обстоятельств несанкционированного доступа, целесообразна систематизация возможных оперативно-розыскных ситуаций, их определения на первоначальном и последующем этапах раскрытия преступления.

Решение обозначенных проблемных аспектов представляется в разработке научно-практических рекомендаций по документированию несанкционированного доступа к компьютерной информации, предложений о направлениях совершенствования оперативно-розыскной деятельности и законодательства в данной области, а также необходимостью научной разработки отдельных аспектов выявления и фиксации преступной деятельности при несанкционированном доступе к компьютерной информации.

Таким образом, вопросы оперативно-розыскного противодействия несанкционированному доступу к компьютерной информации требуют в настоящее время комплексной научной проработки, в связи с наличием ряда проблем теоретического и прикладного характера.

УДК 343.985

О.Б. Шалагинова, Н.П. Мазанов

ИННОВАЦИОННЫЕ ПОДХОДЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Целью исследования являются обоснование и разработка подхода к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность», актуального на сегодня и основанного на повышении качества усвоения учебного материала дисциплин, предусмотренных учебным планом. Эта проблема требует решения в ближайшее время, так как речь идет о завтрашнем дне России и ее национальной безопасности.

Для достижения поставленной цели предлагается использовать инновационные методы обучения, основанные на использовании современных интерактивных образовательных технологий.

Исследование основано на анализе и использовании материалов исследований в области применения педагогических технологий в современном образовательном процессе, требований законодательства, которые являются обязательными при реализации основных образовательных программ высшего профессионального образования. При подготовке статьи также были использованы материалы, полученные ав-

торами в ходе планирования, подготовки, проведения и анализа лабораторных исследований со студентами, обучающимися по направлению подготовки «Информационная безопасность».

Специфика подготовки специалистов по направлению подготовки «Информационная безопасность», обусловленная высокими требованиями, предъявляемыми к ним работодателями, а также сложностью и необходимостью решения задач, стоящих перед Российской Федерацией, в области обеспечения информационной безопасности, заключается в необходимости получения знаний, наряду с фундаментальными знаниями в области информационной безопасности, современных и перспективных технологий защиты информации. Важную роль в повышении качества подготовки высококвалифицированных специалистов, профессионально востребованных и способных к саморазвитию, в настоящее время играет применение новых подходов к их подготовке, основанных на использовании инновационных методов. Предлагаемый подход заключается в разработке студентами современных и перспективных технологий защиты информации с использованием инновационных методов обучения при организации, подготовке и проведении учебных занятий. Одной из основных, наиболее важных в практических, исследовательских аспектах, форм проведения занятий в процессе подготовки специалистов по информационной безопасности является лабораторный семинар.

Предложенный подход апробирован в учебном процессе при планировании, подготовке и проведении лабораторных работ по теме «Создание виртуальной частной сети в виртуальной среде» по дисциплине «Технологии информационной безопасности». К основным особенностям данного урока можно отнести актуальность, высокую технологичность и практическую направленность темы урока, а также его интерактивность.

Результатом применения предложенного подхода стало повышение степени усвоения, широты охвата изучаемого материала и, как следствие, повышение эффективности формирования компетенций студентов, предусмотренных учебным планом.

Предложенный подход, заключающийся в применении инновационных интерактивных методов обучения при организации, подготовке и проведении обучения по актуальным, высокотехнологичным темам прикладной важности, был реализован на практике при изучении студентами дисциплины «Технологии информационной безопасности», что позволило повысить качество усвоения учебного материала дисциплины и в конечном итоге повысить качество подготовки специалистов по направлению подготовки «Информационная безопасность».

А. Тумаков рассказал о специфике подготовки специалистов в сфере кибербезопасности. Противодействие преступлениям в сфере информационных технологий, информационной безопасности подразумевает решение сразу нескольких задач. Об этом в интервью рассказал А. Тумаков, начальник кафедры гражданского и трудового права, гражданского процесса, кандидат юридических наук, доцент Московского университета МВД России имени В.Я. Кикотя. «Во-первых, это, безусловно, техническая составляющая, которой, собственно, и занимается факультет, вами обозначенный, и юридическая, безусловно, которой занимаются факультеты юридические», – отметил он. Образовательная программа факультета подготовки специалистов в области информационной безопасности, по его словам, предусматривает изучение технических дисциплин по специальности «Информационная безопасность автоматизированных систем». Она включает, в первую очередь, те учебные дисциплины, которые связаны с инженерно-техническими компетенциями, программно-аппаратными компетенциями, безусловно, отчасти организационно-правовыми компетенциями.

А. Тумаков поведал также о проводимых на факультете уникальных киберучениях. «Это комплекс учений, задачей которых является выработка компетенции технического характера и, безусловно, юридического, потому как в рамках проведения киберучений наши обучающиеся получают компетенции по проведению следственных действий, по подготовке процессуальных документов. Все это именно в рамках выявления и расследования преступлений, связанных с информационными технологиями, то есть непосредственно это различного рода хищения – пластиковых карт и так далее. Одновременно мы наших будущих выпускников готовим и с точки зрения технической, и, безусловно, с точки зрения юридической», – пояснил он.

Ученый также отметил, что факультет реализует дорожную карту по взаимодействию со стратегическими партнерами университета, которые являются специалистами в области кибербезопасности. «В частности, достаточно тесно мы взаимодействуем с Лабораторией Касперского. Специалисты лаборатории достаточно часто присутствуют на учебных занятиях, делятся опытом, помогают решать какие-то практические кейсы и так далее. Также мы взаимодействуем с ПАО «Сбербанк», кроме того, специалист Департамента обеспечения кибербезопасности активно присутствует на учебных занятиях. Это актуально не только для наших курсантов, но и для действующих сотрудников. Наши преподаватели совместно с привлекаемыми специалистами проводят повышение квалификации действующих сотрудников, следователей, оперативников и так далее», – рассказал А. Тумаков. И все это, по его словам, происходит непосредственно на том объекте, на котором

находится факультет подготовки специалистов в области информационной безопасности. «Подводя такой промежуточный итог работы факультета, я бы хотел отметить, что все-таки это решение по выработке технических компетенций практико-ориентированных и, безусловно, юридических. Поэтому данный факультет у нас является передовым и, безусловно, будет регулярно развиваться, регулярно совершенствовать образовательный процесс в рамках учебных дисциплин», – резюмировал он.

Кроме того, по мнению А. Тумакова, со временем цифровое право сформируется как отдельная отрасль. «Полагаю, что в настоящее время законодательство должно быть трансформировано. Причем трансформация должна происходить не только в области частного права, но и, безусловно, публичного права. Буквально вчера была поставлена задача Центральному банку и Министерству финансов предложить правовое регулирование цифровых финансовых активов. Думаю, что это достаточно позитивный пример, когда новые объекты, которые появляются в гражданском обороте, будут иметь соответствующее правовое регулирование. И, в целом, без выстраивания определенного категориального аппарата, в том числе в частном праве, нашим правоприменителям, судьям в том числе, достаточно сложно заниматься правоприменительной практикой, – добавил он. – Поэтому, полагаю, что законодательство в области как частного права, так и публичного права, должно трансформироваться в современных условиях и отвечать новым вызовам».

В результате исследования обоснован и разработан подход к повышению качества подготовки специалистов в области подготовки «Информационная безопасность».

УДК 343.98

И.О. Щербаков

ОСМОТР КОМПЬЮТЕРНЫХ УСТРОЙСТВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Несмотря на понижение темпа роста киберпреступлений, нельзя не отметить, что в целом все киберпреступления постоянно видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть

следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов во многом сейчас направлена на выявление, раскрытие и расследование преступлений, совершенных с использованием интернет-технологий.

Производство любого следственного действия, а особенно осмотра компьютерной техники, требует тщательной подготовки, обусловленной особенностями компьютерных средств. Осмотр электронных носителей информации возможно проводить в ходе осмотра места происшествия, либо как отдельное следственное действие [1].

На подготовительном этапе данного следственного действия следует:

проанализировать и систематизировать все сведения, имеющиеся в материалах уголовного дела, для определения вектора поиска криминалистически значимой информации;

привлечь специалиста, у которого есть необходимые компьютерно-технические средства;

разрешить вопрос об участии понятых, либо о применении технических средств, фиксирующих ход производства осмотра компьютерного устройства. Учитывая длительность и специфику производства данного следственного действия, целесообразным будет применение технических средств, что не противоречит ч. 1.1 ст. 170 Уголовно-процессуального кодекса Российской Федерации.

Для рабочего этапа характер осмотра методом «от общего к частному», т. е. сначала осматриваются внешние признаки устройства (цвет, марка, модель), а потом производится осмотр информации, содержащейся на электронном носителе. Неизменность, подлинность и сохранность источника информации обеспечивается следующим алгоритмом действий:

применять средства и программные обеспечения блокировки записи цифровой информации, копирования данных, позволяющих создавать копию, соответствующую оригиналу по содержанию и технологическим свойствам, позволяющие извлечь и проанализировать данные из устройств и облачных сервисов, такие как контакты, сообщения, звонки, геолокация, восстанавливают удаленные данные и др. [2];

не производить отключения уже запущенных программ и приложений, «авиарежима»;

не позволять самостоятельно совершать манипуляции с компьютерным устройством, если неизвестно, к какому результату это приведет;

детальный осмотр данных как на электронном устройстве, так и в «облачных» хранилищах;

удостоверение факта производства определенных действий, производимых с устройством, путем их фиксации письменно в протоколе,

составления фототаблицы, прилагаемой к осмотру, а также используя встроенную функцию на устройстве «скриншот».

На заключительном этапе оформляется протокол осмотра предметов и решается вопрос о дальнейшем хранении электронных устройств. Сведения, подлежащие занесению в протокол данного следственного действия:

1) осматриваемое устройство, его модель, марка, производитель, размеры, цвет, наличие внешних разъемов;

2) состояние устройства в момент осмотра, включенное либо выключенное;

3) провода, через которые производится электропитание прибора, их размер и цвет;

4) общее состояние осматриваемых устройств, внешний вид и наличие повреждений;

5) порядок соединения устройств с другими техническими средствами;

6) наличие или отсутствие вредоносных программ, их название, а также наличие или отсутствие антивирусной программы;

7) содержание найденной информации, откуда была скопирована [3].

Далее устройство упаковывается с соблюдением условий, исключающих возможность доступа к содержимому и дистанционного считывания.

Своевременное обнаружение компьютерных средств и правильное их изъятие предопределяет эффективность последующей компьютерно-технической экспертизы, назначаемой с целью извлечения информации, хранящейся на магнитных носителях, и обнаружения таким образом указанных следов преступной деятельности.

Список использованных источников

1. Иванов, В.Ю. К вопросу совершенствования противодействия киберпреступлениям правоохранительными органами / В.Ю. Иванов // Соврем. наукоем. технологии. – 2019. – № 1. – С. 52–57.

2. Бахтеев, Д.В. Криминалистическое мышление и программирование расследования / Д.В. Бахтеев // Вестн. Балт. федер. ун-та им. И. Канта. Сер. «Гуманитар. и обществ. науки». – 2018. – № 3. – С. 13–20.

3. Виноградова, О.П. Современные направления использования информационных технологий в раскрытии и расследовании преступлений / О.П. Виноградова // Тенденции развития современного уголовно-процессуального законодательства Российской Федерации : сб. науч. тр. Всерос. науч.-практ. конф. – Екатеринбург, 2019. – С. 24–28.

УДК 343.9

Л.Ю. Югай

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ: ОПЫТ РЕСПУБЛИКИ УЗБЕКИСТАН

Цифровая трансформация общества и государства влечет за собой динамичный рост сфер жизнедеятельности человека, где используются биометрические технологии. В Республике Узбекистан биометрическая идентификация личности используется в нотариальной деятельности, при оказании государственных и банковских услуг в удаленном режиме, при проведении вступительных экзаменов в высшие учебные заведения, при оформлении административного протокола при нарушении правил дорожного движения и в других случаях.

Данная тенденция имеет место и в деятельности по раскрытию и расследованию преступлений, что обусловливает качественное изменение применяемых научно-технических средств и методов, а также переход от материальной формы вещественных доказательств в цифровую. Правоохранительными органами эффективно используются специализированные биометрические базы данных.

Анализ правоприменительной практики показывает, что с учетом внедрения аппаратно-программного комплекса «Безопасный город» с интеллектуальной системой видеонаблюдения значительно возросло количество проводимых портретных исследований: начиная с 2019 г. – на 2,3 %, в 2020 г. – на 172,9 %, в 2021 г. – на 258,3 %, включая идентификации по фотороботу, фотоизображениям лиц, идентификаций неизвестных лиц и видеоматериалам. Учитывая, что количество портретных экспертиз, проведенных с 2017 по 2021 г., увеличилось на 119,7 %, портретных исследований за указанный период достигло 311,3 %, следует отметить важность оснащения системами видеонаблюдения всех общественных мест в комплексе с технологией распознавания лиц.

С апреля 2022 г. осуществляет свою деятельность Центр единого оперативного управления ГУВД г. Ташкента (далее – Центр). В дежурной части данного Центра в круглосуточном режиме ведется мониторинг системы видеонаблюдения общественных пространств с использованием технологии распознавания лиц. При обнаружении человека, похожего на лицо, находящееся в розыске, искусственный

интеллект подает сигнал о его местонахождении и транслирует его видеоизображение в режиме онлайн. Дежурный связывается с ближайшим патрулем, который оперативно принимает меры к его задержанию. Сотрудник Центра физически не в состоянии проанализировать изображения нескольких сотен камер и сопоставить с базой разыскиваемых лиц. В данном аспекте искусственный интеллект показывает высокие результаты по установлению личности правонарушителей, розыску лиц и оказанию помощи в оперативном управлении ситуацией.

Следует подчеркнуть, что сегодня особую актуальность приобретает возможность удаленного доступа к специализированным базам данных для подтверждения и проверки личности неизвестных лиц без доставления в территориальные подразделения органов внутренних дел. Постановлением Кабинета Министров Республики Узбекистан от 22 июля 2022 г. № 399 «О мерах по внедрению современных информационных технологий в деятельность патрульно-постовой службы органов внутренних дел» предусмотрено использование системы «Электронный патруль». Данная система представляет собой централизованную электронную систему проверки изображения лица в режиме реального времени путем фотографирования, формирования, сбора, обобщения, хранения соответствующей информации, а также межведомственного обмена информацией между уполномоченными государственными органами с использованием специального сканера отпечатков пальцев на планшете.

В соответствии с названным выше постановлением в случае, если идентифицировать лицо по отпечаткам пальцев не представляется возможным, то сотрудник постовой службы может использовать бодикамеру для проверки по базам данных по чертам внешности. При помощи специального планшета и сотрудники УБДД, ППС могут осуществлять мобильную оперативную проверку на наличие судимости, розыска, профилактического, пробационного и административного надзора.

Данная система позволяет идентифицировать лицо без доставления его в территориальные подразделения органов внутренних дел, что, несомненно, положительным образом отражается на оперативной обстановке, позволяет экономить время, создает удобства и для проверяемых лиц, и для сотрудников органов внутренних дел.

Кроме того, на вооружение органов внутренних дел Республики Узбекистан поступили 12 передвижных криминалистических лабораторий, каждая из которых оснащена двумя беспилотными летательными аппаратами (БПЛА) и мобильными комплексами автоматизированной дактилоскопической идентификационной системы и автоматизи-

рованной системы идентификации личности. Такие мобильные комплексы позволяют осуществлять проверку следов папиллярных линий, отпечатков пальцев, изображений лиц по базам биометрических данных непосредственно с мест происшествия. Вышеуказанное способствует раскрытию преступлений по горячим следам.

При этом сегодня существенное значение приобретает использование БПЛА для решения задач, стоящих перед правоохранительными органами. Специалистами проводятся исследования, посвященные вопросам использования БПЛА, в целях осуществления и фиксации осмотров мест происшествий, ведения скрытого наблюдения за отдельным контингентом лиц, представляющих оперативный интерес, поиска пострадавших лиц, при чрезвычайных происшествиях фиксации массовых беспорядков, идентификации их зачинщиков и активных участников. Беспилотные летательные устройства для решения правоохранительных задач используются в США, Великобритании, Дубае, Китае, Франции, Японии, Республике Беларусь и других странах.

Указанные БПЛА позволяют документировать преступные события и идентифицировать правонарушителей, а также обеспечивают безопасность участников процессуальных действий при осмотре опасных для жизни и здоровья человека или труднодоступных мест происшествия.

Подводя итог, следует отметить, что в Республике Узбекистан проводится динамичная системная работа по повышению эффективности использования биометрической идентификации личности в раскрытии и расследовании преступлений. Реализуется в тестовом режиме проект «Электронное уголовное дело», которое в перспективе предусматривает использование биометрических идентификаторов. При реализации всех вышеуказанных высокотехнологичных проектов особое значение имеет решение комплекса правовых, организационных, методических и иных вопросов. Особую важность приобретает обеспечение безопасности биометрических персональных данных при их сборе, хранении, использовании, передаче и обработке от кражи, неправомерного использования, модификации, а также защита прав и законных интересов граждан на неприкосновенность частной жизни.

УДК 343.985

Д.С. Якжик

О РОЛИ СЕРВИСОВ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ В ПРОТИВОДЕЙСТВИИ КИБЕРМОШЕННИЧЕСТВУ

Наиболее распространенным видом кибермошенничества является фишинг, и Беларусь не является исключением. Задача фишинга – «получить» конфиденциальные данные и использовать их, в том числе для получения доступа к денежным средствам пользователя. Выделяют две категории фишинга: обычный и целевой. Обычный фишинг (безадресный) отличается широким охватом и обычно имеет вид спам-кампаний. Целевой фишинг более технологичен. Злоумышленники собирают информацию о своих жертвах и впоследствии используют эти данные для составления убедительного и правдоподобного письма. Для достижения цели злоумышленнику необходимо привлечь внимание жертвы заголовком письма и добиться от нее выполнения ряда действий: открыть письмо, перейти по ссылке, ввести конфиденциальные данные в поля фишингового окна либо страницы. На каждом из этапов успех злоумышленника зависит от используемых уловок и приемов психологического манипулирования и от бдительности жертвы. По мере распространения фишинга накапливается статистическая информация о вероятности успешной атаки с использованием различных схем, при этом наиболее простые и успешные схемы ставятся на поток. Для начала преступной деятельности достаточно оплатить вступительный взнос и получить доступ к телеграм-чату с инструкциями, заготовками фишинговых ссылок и страниц, сетью наставников, технической поддержкой. Количество участников подобных чатов исчисляется сотнями.

Наиболее распространенной в настоящее время схемой мошенничества является «Мамонт» или «Курьер» – предложение о покупке товара по объявлению на электронной торговой площадке. Мошенник выбирает объявления, в которых указан номер мобильного телефона продавца и направляет в мессенджере сообщение о заинтересованности в покупке товара, при этом сообщает, что находится в другом регионе, предлагает оплатить товар переводом с карточки на карточку и воспользоваться службой доставки. Жертва, движимая желанием продать товар, соглашается принять оплату на свою банковскую платежную карточку, после чего ей направляется поддельный запрос от банка на зачисление денежных средств, в котором требуется указать реквизиты карточки и CVV/CVC код (VISA использует обозначение CVV (Card Verification Value), MasterCard использует обозначение CVC (Card Validation Code)). Цель мошенников – использовать полученные реквизиты для покупки криптовалюты, но им не хватает сеансового ключа 3D Secure, поступающего по SMS на телефон держателя карточки. Поэтому продавцу направляется окно для ввода кода, якобы для зачисления платежа на карточку. В результате мошенники получают все необходимое для однократного использования карточки жертвы в своих целях, процесс может развиваться далее для получения новых сеансовых ключей и данных других банковских карточек.

Залогом успеха описанной схемы является наличие в объявлении на торговой площадке необходимой мошеннику на первоначальном этапе информации: номер мобильного телефона жертвы и психологический триггер – желание продать определенную вещь.

Социальная инженерия в подобных схемах базируется на двух факторах. Во-первых, осведомленность держателя карточки о конфиденциальной информации, необходимой для дистанционного списания средств со счета. Во-вторых, отсутствие у продавца опыта совершения сделок с получением платежа на банковскую платежную карточку, что создает неуверенность в себе и повышает восприимчивость к манипулированию со стороны «искушенного покупателя». Незнание того, что для зачисления средств достаточно сообщить отправителю только номер карточки (для некоторых банков эмитентов дополнительно потребуется либо срок действия карточки либо имя и фамилия владельца). В любом случае отправителю не требуются CVV/CVC код карточки получателя, а при зачислении средств на карточку не генерируется ключ 3D Secure.

Условием успешной защиты от уловок мошенников является исключение любого из указанных факторов. В целях снижения восприимчивости граждан к методам социальной инженерии в последние годы в Беларуси ведется широкомасштабная информационная кампания по разъяснению населению способов защиты от фишинга и вишинга. К сожалению, практика показывает, что осведомленность людей не гарантирует защиту от мошенников.

Вместе с тем первый фактор – осведомленность держателя карточки о конфиденциальных сведениях, открывает доступ к широкому спектру мер противодействия кибермошенничеству. Возможно ли пользоваться банковской платежной карточкой без данных о держателе, номере карточки, сроке действия, CVV/CVC коде? Да, и многие делают это ежедневно, когда прикладывают карточку к картридеру, оплачивая товары либо услуги.

Традиционная технология приложений на базе смарт-карт состоит в двухступенчатой аутентификации. Сначала владелец смарт-карты локально аутентифицируется относительно смарт-карты при помощи пин-кода через кардридер, а затем смарт-карта исполняет более слож-

ный криптографический протокол аутентификации, включающий, например, вычисление цифровой подписи. В процессе аутентификации используются протоколы с защитой данных.

В настоящее время в торговле набирает популярность мобильный SoftPOS-эквайринг. Он дает возможность принимать безналичные платежи с помощью смартфона с NFC-модулем (Near Field Communication). Для покупателя процесс оплаты выглядит аналогично покупке при помощи обычного платежного терминала. Он прикладывает свою бесконтактную карточку к смартфону продавца, на котором установлено приложение SoftPOS-эквайринга. После обработки платежа у продавца на экране телефона отображается информация об успешно проведенной операции, а покупатель получает оплаченный товар или услугу. Электронный чек приходит в виде SMS.

Адаптация функционала SoftPOS-эквайринга к переводам с карточки на карточку (P2P-переводам) позволит продавцу выставлять электронный счет, а покупателю акцептовать его, приложив свою карточку к смартфону.

Для дистанционных сделок возможным решением является интернет-эквайринг. В процессе оформления приобретаемого товара или услуги покупатель покидает сайт продавца и перенаправляется на специальный защищенный сайт банка-эквайера, что можно сразу заметить в адресной строке браузера. При оплате покупок в интернете вместо терминала используется специальный защищенный сервис банка.

Организация платежного сервиса на электронных торговых площадках имеет ряд положительных факторов и для торговой площадки, и для продавцов, и для покупателей. Средства покупателя депонируются на счете торговой площадки до получения от покупателя подтверждения о соответствии товара заявленному в объявлении о продаже, после чего перечисляются продавцу. На счетах торговой площадки формируется оборотный капитал, что создает источник средств для инвестирования и дополнительного дохода. Продавец сообщает сведения о своей банковской платежной карточке только торговой площадке, что защищает его от социальной инженерии мошенников на стороне покупателя. Покупатель приобретает дополнительную защиту своих прав. В случае получения товара ненадлежащего качества он имеет возможность расторгнуть сделку, вернуть товар продавцу и вернуть удерживаемую торговой площадкой уплаченную сумму.

Менее технологичным и менее защищенным вариантом является информационное взаимодействие электронной торговой площадки с банковскими сервисами переводов с карточки на карточку (P2P-переводы). Идея заключается в создании возможности сторонам сделки перейти с сайта торговой площадки на страницу банка эмитента

карточки покупателя с официальной информацией об условиях перевода с карточки на карточку.

Таким образом, дальнейшее развитие используемых и создание новых сервисов безналичной оплаты товаров и услуг для физических лиц позволит отказаться от использования CVV/CVC кодов и создать механизм противодействия кибермошенничеству с применением социальной инженерии.

УДК 340.1

К.В. Янчуревич

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КАК ВАЖНЫЙ ЭЛЕМЕНТ ПРОЦЕССА ФОРМИРОВАНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РЕСПУБЛИКЕ БЕЛАРУСЬ

В настоящее время в ряде стран наблюдается процесс активного формирования и развития информационного общества. В зависимости от множества различных факторов отдельные государства находятся на разных этапах вышеуказанного процесса.

Следует отметить, что информационное общество представляет собой сложную систему, которая включает в себя множество элементов. Большинство ученых, занимавшихся исследованиями в области информационного общества, сходятся во мнении, что именно информация, по сути, и является центральным звеном («ядром») информационного общества.

Необходимо подчеркнуть, что для того чтобы общество могло беспрепятственно пользоваться информацией, распространять ее, а также ощущать защищенность от преступных посягательств со стороны преступников, следует применять высокоэффективные действенные меры.

Безусловно, уже разработано и активно применяется на практике достаточно много способов борьбы с киберпреступлениями (правовые, организационно-технические и др.). Вместе с тем факт наличия значительного количества киберправонарушений свидетельствует о необходимости разработки и использовании на практике новых эффективных способов борьбы с данными правонарушениями.

Считаем целесообразным, наряду с уже используемыми методами обеспечения кибербезопасности, применение следующих:

1. Включение в образовательный процесс учащихся школ и средних специальных учебных заведений, а также учреждений высшего образо-

вания учебных дисциплин (спецкурсов), направленных на изучение основ кибербезопасности. Полагаем, что в данном случае возможно использовать элементы таких учебных дисциплин, как «Основы права» и «Информационное право» и на их базе создать предмет «Основы информационного права» либо «Основы кибербезопасности». Это позволит в значительной степени снизить подверженность потенциальных жертв преступлениям в киберсфере. Думаем, что такая работа должна быть направлена в первую очередь на перечисленные выше категории населения, поскольку именно они наиболее простые потенциальные цели для киберпреступников и менее всего обладают информацией о возможных путях противодействия последним. Считаем целесообразным также введение форм контроля (например, зачет) по указанным спецкурсам для контроля за уровнем усвоения указанного материала учащимися.

2. В качестве эффективного профилактического мероприятия, направленного на повышение уровня знаний в области информационной безопасности (иными словами, направленной на повышение цифровой грамотности), будут выступать курсы повышения квалификации и курсы повышения мастерства по дисциплинам, указанным выше. Данные курсы, полагаем, необходимо проводить для сотрудников различных предприятий и организаций, а также сотрудников государственных органов на постоянной систематической основе, не реже чем один раз в 1–2 года, поскольку информация в этой сфере обновляется с достаточно высокой скоростью. Период обучения на таких курсах считаем целесообразным делать от 1,5 до 3 недель с последующей сдачей квалифицированного зачета либо защитой выпускных работ.

3. Очевидным и необходимым нововведением для Республики Беларусь может стать также разработка и использование комплекса компьютерных программ, которые будут способны заменить зарубежные аналоги, а также, с другой стороны, позволят государственным органам осуществлять значительно проще контроль за сферой кибербезопасности в стране.

В качестве наиболее эффективного метода поддержания необходимого уровня кибербезопасности на территории Республики Беларусь может стать открытие учебной дисциплины «Информационное право» на юридических факультетах крупнейших учреждений высшего образования страны. Это позволит подготовить необходимое и вместе с тем достаточное количество обученных специалистов, владеющих навыками и знаниями на высоком профессиональном уровне, а в дальнейшем с их помощью обеспечивать кибербезопасность Республики Беларусь.

Сфера кибербезопасности, цифровой грамотности и иные сферы, тесно связанные с информацией и информационными услугами, постоянно сталкиваются с новыми проблемами и угрозами, соответственно,

для их решения необходимы формирование и применение в практической деятельности новых способов (методов).

Кроме того, для более эффективного урегулирования области отношений, связанных напрямую со сферой кибербезопасности, необходимы, с нашей точки зрения, разработка и принятие комплекса нормативных правовых актов. В качестве значимого и центрального звена может выступить единый кодифицированный акт в информационной сфере – Информационный кодекс. Его подготовка, по нашему мнению, позволит урегулировать значительное количество правоотношений.

На основании вышеизложенного можно сделать следующие выводы:

1. Информация в целом и обеспечение кибербезопасности является важными элементами информационного общества и для его формирования и развития необходим комплекс эффективных мер, способных обеспечивать регулирование и защиту с различных направлений (правового, организационно-технического и др.).

2. Для обеспечения кибербезопасности необходим комплексный системный подход, который сможет обеспечить нахождение требуемых решений актуальных вопросов в данной сфере. В качестве основы применения такого подхода может стать создание учебной дисциплины «Информационное право» в крупнейших учреждениях образования Республики Беларусь.

3. Для обеспечения высокого уровня защиты кибербезопасности необходимо разработать и принять ряд нормативных правовых актов, направленных на поддержание данного уровня. В качестве центрального звена требуемых правовых актов может выступить единый кодифицированный правовой акт – Информационный кодекс.

СВЕДЕНИЯ ОБ АВТОРАХ

БАЛИТКИН Александр Валерьевич – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

БЕЛЕВСКИЙ Роман Александрович – старший преподаватель кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России им. В.В. Лукьянова, кандидат юридических наук.

БЕСПАЛОВ Виталий Александрович – преподаватель кафедры информационного права Академии Министерства внутренних дел Республики Беларусь.

БОБОВИЧ Николай Михайлович – доцент кафедры информационного права Академии Министерства внутренних дел Республики Беларусь, кандидат технических наук, доцент.

БОРОВИК Петр Леонидович – доцент кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

ВЕНГЛОВСКИЙ Владислав Леонидович – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

ВИНОГРАДОВА Ольга Павловна – доцент кафедры криминалистики Уральского юридического института МВД России, кандидат юридических наук.

ГАЙНЕЛЬЗЯНОВА Венера Равилевна – доцент кафедры криминалистики Уфимского юридического института МВД России, кандидат юридических наук.

ГЕРАСИМОВА Евгения Валериевна – старший преподаватель кафедры административной деятельности ОВД Воронежского института МВД России.

ГИЗАТУЛЛИН Марат Галимянович – доцент кафедры информационного обеспечения ОВД Уральского юридического института МВД России (начальник отдела инфраструктурной поддержки АО «Уралтрансмаш»), кандидат технических наук, доцент.

ГОЛОВЕНЧИК Марина Геннадьевна – аспирант кафедры уголовного права юридического факультета Белорусского государственного университета.

ГУБИЧ Михаил Валерьевич – заместитель начальника кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

ГУНЬКО Виталий Борисович – доцент кафедры информационного обеспечения ОВД Ростовского юридического института МВД России, кандидат технических наук, доцент.

ЕГОРОВ Дмитрий Анатольевич – доцент кафедры административной деятельности ОВД факультета милиции общественной безопасности Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

ЖИЛХАЙДАРОВА Баян Аблаевна – магистрант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

ЖУКОВА Анжелика Павловна – инспектор отделения планирования и контроля качества учебного процесса и практики учебного отдела Воронежского института МВД России.

ЗУБАРЕВА Людмила Леонидовна – сотрудник МВД Республики Беларусь, кандидат юридических наук.

ЗЫК Даниил Денисович – курсант следственно-экспертного факультета Академии Министерства внутренних дел Республики Беларусь.

ИВАНОВСКИЙ Александр Владимирович – профессор кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, доктор технических наук, профессор.

ИВАНУХА Иван Сергеевич – преподаватель кафедры информационных технологий в деятельности ОВД Омской академии МВД России.

КАРАПЕТЯН Роберт Арменович – слушатель факультета подготовки специалистов по программам высшего образования Ростовского юридического института МВД России.

КОМЕРЦОВ Вячеслав Викторович – преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России.

КОРНЕЕВ Сергей Алексеевич – ассистент Белорусского государственного экономического университета.

КОРОЛЬ Сергей Владимирович – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

КРАВЕЦ Владислав Владимирович – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

КУАНЫШ Даурен Калижанович – старший преподаватель кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан им. М. Есбулатова.

КУЗЬМЕНКОВА Светлана Валерьевна – доцент кафедры информационного права факультета криминальной милиции Академии Мини-

стерства внутренних дел Республики Беларусь, кандидат юридических наук.

ЛАВРЕНОВ Виктор Вячеславович – старший преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

ЛАСТОВСКИЙ Александр Андреевич – старший преподаватель кафедры психологии и педагогики Академии Министерства внутренних дел Республики Беларусь.

ЛАХТИКОВ Дмитрий Николаевич – начальник кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

ЛЕМЕШЕВСКИЙ Олег Олегович – старший преподаватель кафедры юридических дисциплин факультета внутренних войск Военной академии Республики Беларусь, магистр военных наук.

ЛОПАТЬЕВСКАЯ Эсмиральда Андреевна – доцент Белорусского государственного экономического университета, кандидат юридических наук, доцент.

ЛОХНИЦКИЙ Максим Андреевич – курсант следственно-экспертного факультета Академии Министерства внутренних дел Республики Беларусь.

ЛУЗГИН Иван Иванович – старший преподаватель кафедры криминалистики юридического факультета Белорусского государственного университета.

ЛУТОВИЧ Павел Валерьевич – преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

МАЗАНОВ Николай Павлович – курсант факультета № 3 подготовки сотрудников для оперативных подразделений Санкт-Петербургского университета МВД России.

МЕЗЯК Вадим Юрьевич – преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

МЕЛЬНИК Андрей Андреевич – магистрант Академии управления при Президенте Республики Беларусь.

МИСУН Елена Николаевна – начальник кафедры психологии и педагогики Академии Министерства внутренних дел Республики Беларусь, кандидат социологических наук, доцент.

МИТРЯЕВ Иван Сергеевич – старший преподаватель кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России им. В.В. Лукьянова.

МОРОЗОВ Андрей Владимирович – начальник Шкловского районного отдела Следственного комитета Республики Беларусь.

НАСЫРОВ Ренат Рабисович – доцент кафедры оперативно-разыскной деятельности ОВД Уфимского юридического института МВД России, кандидат юридических наук.

НЕСТЕР Иван Сергеевич – старший преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук.

НОВАКОВА Ксения Александровна – доцент кафедры исследования документов учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России, кандидат юридических наук.

ПАШКЕВИЧ Даниил Дмитриевич – курсант факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

ПЕТЛИЦКИЙ Сергей Викторович – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь

ПЕТРОВИЧ Алексей Александрович – магистрант факультета повышения квалификации и переподготовки руководящих кадров Академии Министерства внутренних дел Республики Беларусь.

ПЕТРОВИЧ Дмитрий Анатольевич – курсант факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

ПИКТА Владислав Игоревич – старший преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

ПИЛЮШИН Святослав Викторович – старший преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук.

ПОЛКОВНИЧЕНКО Юрий Владимирович – следователь по особо важным делам следственного управления УСК Республики Беларусь по Гомельской области.

ПОЛТОРЖИЦКИЙ Павел Олегович – магистр экономики и управления, старший оперуполномоченный по ОВД ГУБОПиК МВД Республики Беларусь.

РЯБЕНКО Денис Сергеевич – начальник цикла Института пограничной службы Республики Беларусь, кандидат технических наук, доцент.

САМОЙЛО Владислав Алексеевич – курсант уголовно-исполнительного факультета Академии Министерства внутренних дел Республики Беларусь.

САНУКЕВИЧ Анастасия Александровна – магистрантка Гродненского государственного университета им. Я. Купалы.

СЕРЕДА Александр Евгеньевич – ведущий специалист учебной лаборатории кафедры криминалистики юридического факультета Белорусского государственного университета.

СЛАЩИНИН Олег Андреевич – следователь ГСУ Следственного комитета Республики Беларусь.

СОБОЛЕВСКИЙ Евгений Николаевич – преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

СОРОКИН Максим Николаевич – старший преподаватель Института пограничной службы Республики Беларусь.

СОРОКУН Николай Сергеевич – доцент кафедры уголовного права и криминологии Ростовского юридического института МВД России, кандидат юридических наук.

СТАРОВЕРОВ Алексей Александрович – курсант Уральского юридического института МВД России.

ТАРАСОВ Павел Анатольевич – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

ТЕСЛЁНОК Александр Юрьевич – преподаватель кафедры правового обеспечения Института пограничной службы Республики Беларусь.

ТИТОВ Павел Михайлович – старший преподаватель кафедры оперативно-разыскной деятельности ОВД Уральского юридического института МВД России, кандидат юридических наук.

ТУКАЛО Алексей Николаевич – начальник кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

УРСТЕНОВА Дарина Данияровна – сотрудник Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова.

ФОМИНА Инна Анатольевна – старший преподаватель кафедры уголовного права и криминологии Восточно-Сибирского института МВД России, кандидат юридических наук.

ХАМИДУЛЛИН Руслан Сибагатуллович – начальник кафедры оперативно-разыскной деятельности ОВД Уральского юридического института МВД России.

ХАРЕВИЧ Дмитрий Людвикович – доцент кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь, кандидат юридических наук, доцент.

ХЛУС Александр Михайлович – доцент кафедры криминалистики Белорусского государственного университета, кандидат юридических наук, доцент.

ХОДАСЕВИЧ Анна Вячеславовна – аспирант юридического факультета Белорусского государственного университета, старший следователь Фрунзенского (г. Минск) РОСК Республики Беларусь.

ЧЕХОВИЧ Александр Александрович – адъюнкт научно-педагогического факультета Академии Министерства внутренних дел Республики Беларусь.

ШАЛАГИНОВА Ольга Борисовна – доцент кафедры математики и информатики Санкт-Петербургского университета МВД России, кандидат физико-математических наук, доцент.

ШКУРКО Денис Анатольевич – магистрант Академии Министерства внутренних дел Республики Беларусь, заместитель начальника УНиПТЛ КМ УВД Витебского облисполкома.

ЩЕРБАКОВ Игорь Олегович – преподаватель кафедры криминалистики Уральского юридического института МВД России.

ЮГАЙ Людмила Юрьевна – доктор философии (PhD) по юридическим наукам, докторант Академии МВД Республики Узбекистан.

ЯКЖИК Дмитрий Сергеевич – старший преподаватель кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь.

ЯНЧУРЕВИЧ Константин Викторович – магистр юридических наук, старший преподаватель Гродненского государственного университета им. Я. Купалы.

СОДЕРЖАНИЕ

Научное издание

ТЕОРИЯ И ПРАКТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Материалы заочной
Международной научно-практической конференции
(Минск, 12 декабря 2022 г.)

Компьютерная верстка *И.В. Бачилы*
Корректор *М.С. Прушак*

Подписано в печать 00.00.2023. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Ризография. Усл. печ. л. 12,09. Уч.-изд. л. 11,80
Тираж экз. Заказ

Издатель и полиграфическое исполнение:
учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/102 от 02.12.2013.
Пр-т Машерова, 6А, 220005, Минск.

Т11 **Теория и практика противодействия киберпреступности** : материалы заоч. Междунар. науч.-практ. конф. (Минск, 12 дек. 2022 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: Д.Н. Лахтиков (отв. ред.) [и др.]. – Минск : Академия МВД, 2023. – 206, [2] с.
ISBN 978-985-576-400-8.

Рассматриваются правовые и методологические проблемы противодействия киберпреступности, актуальные вопросы использования информационных технологий в этом направлении, инновационные подходы при подготовке специалистов в сфере противодействия киберпреступности.

Издание предназначено для научных сотрудников, преподавателей, аспирантов, адъюнктов, лиц, обучающихся в высших учебных заведениях юридического профиля, практических работников правоохранительных органов.

УДК 343.985.7 + 004:34 + 343.534
ББК 67.52 + 67.408