МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт МВД Российской Федерации»

Кафедра уголовного процесса

ДИПЛОМНАЯ РАБОТА

на тему **«ПРОЦЕССУАЛЬНЫЕ ПРОБЛЕМЫ ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Облицов Павел Александрович, обучающийся по специальности 40.05.01 Правовое обеспечение национальной безопасности 2017 года набора, 7101 учебной группы

Руководитель
старший преподаватель кафедры уголовного процесса
Хаметова Алиса Расимовна

К защите_____
рекомендуется/не рекомендуется

Начальник кафедры_____ Е.А. Кулеш
подпись

Дата защиты: «___» _____ 2023 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность исследования связана с тем, что одной из основных задач современного государства является защита общества и государства в целом и каждого отдельного гражданина в частности, защита прав и законных интересов гражданина от противоправных преступных посягательств.

Из года в год количество преступлений, совершенных с использованием IT-технологий, стремительно растет. Это большая проблема, потому что она указывает не только на увеличение количества преступлений в нашей стране, но и на определенную неспособность правоохранительной системы ее контролировать. Возбуждение уголовных дел о преступлениях, совершенных с использованием IT-технологий, по своей природе представляет осуществление им такой деятельности, которая направлена на подтверждение виновности подозреваемого или обвиняемого в совершении преступления, и выражает саму суть уголовного преследования, которое осуществляется «в целях изобличения».

Целиком и полностью изменения в сфере информационных процессов наложили отпечаток на состояние преступности. В структуре общей преступности основная доля 33,4 (305 фактов) приходится на кражи чужого имущества, 14% (129 фактов) составляют мошенничества, 12% (103 факта) кражи с банковских карт. Из 129 мошенничества совершенных за 2021 год бесконтактным способом совершено: посредством телефона – 59 фактов, сети Интернет – 58 фактов, с использованием банковских карт-9 фактов, связанных с кредитом- 11 фактов, связанных с неисполнением договорных обязательств – 5. Предметом преступного посягательства во всех случаях явились денежные средства[1].

[1] Состояние преступности в Российской Федерации в 2021-2022 годах. Официальный сайт МВД РФ: Режим доступа: https://мвд.рф/reports/item/35396677 (Дата обращения: 12.04.2023 г.).

Специфика поводов и оснований возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий, обусловлена как механизмом преступления, так и криминалистической характеристикой участников уголовного судопроизводства. Расследование преступлений – это достаточно трудоемкий и сложный процесс, требующий решения вопросов организационного характера, а соответственно, и высокого уровня ответственности и вдумчивости со стороны сотрудника следственного подразделения, занимающегося расследованием конкретного вида преступления.

Объектом исследования выступают общественные отношения, возникающие в процессе возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий.

Предметом исследования стали нормы российского законодательства, регламентирующие процесс возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий.

Целью исследования является выявление процессуальных проблем возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий.

Задачи исследования:

- дать общую характеристику преступлений, совершенных с использованием IT-технологий;

- раскрыть процессуальный порядок возбуждения уголовного дела;

- рассмотреть доследственную (предварительную) проверку сообщения о преступлении как способ установления основания возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий;

- описать решения, принимаемые на стадии возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий.

В настоящее время тема возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий, мало разработана, содержит проблемные вопросы в данной сфере. Можно сказать, что большее внимание

исследователи проявляли к проблемы борьбы с подобными преступлениями, игнорируя процессуальные аспекты исследуемой темы.

Практическая значимость исследования связана с тем, что в настоящем исследовании выявлены проблемы возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий. Нами предлагаются некоторые изменения действующего законодательства, путем внесения рекомендаций, направленных на дальнейшее перспективное развитие сферы возбуждения уголовных дел о преступлениях, совершенных с использованием IT-технологий.

Дипломная работа состоит из введения, двух, включающих в себя четыре параграфа, заключения и списка использованной литературы.

ГЛАВА 1. УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ХАРАКТЕРИСТИКА СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

§ 1. Общая характеристика преступлений, совершенных с использованием IT-технологий

Цифровые платформы, информационно-коммуникационные технологии и процессы электронного взаимодействия являются обязательным элементом практики оказания государственных, муниципальных услуг и всей системы государственной и муниципальной службы. «Цифровая трансформация социальной сферы, системы органов власти и управления, совокупности важнейших отраслей экономики является инструментом повышения эффективности процессов, протекающих внутри указанных систем и в комплексе отношений с внешними субъектами. Ориентация на оптимизацию и ускорение процессов, сокращение издержек обращения и повышение уровня открытости субъектов социально-экономических отношений – целевые ориентиры процесса цифровизации»[1].

Совершенствование и проникновение цифровых технологий во все аспекты социально-экономического пространства, цифровая трансформация ключевых сфер – необратимый процесс современности. Изменения, которые претерпевают в этом процессе объекты и субъекты отношений, носят устойчивый характер и глубоко проявляют свое действие.

Информационные технологии за последние десятилетие внедряются в деятельность не только коммерческих организаций, но и в деятельность государственных органов нашей страны. Достижения научно-технического прогресса изменили сам процесс работы органов государственной власти с

[1] Разувакина И.И., Разувакин А.А. Особенности организации и проведения проверки заявлений и сообщений о преступлениях в сфере компьютерной информации // Право и управление. 2022. № 9. С. 156-159.

населением: расширился спектр предоставляемых услуг, увеличилось время работы государственных органов, стали более специализированными и узконаправленными услуги данных органов, стали появляться различные сайты, на которых не только можно было получить нужную информацию, но и получить обратную связь на интересующие вопросы без лишней траты времени на выстаивания очередей.

По своей сути преступления в сфере IT-технологий – это «преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства, с использованием передовых методов и высокой технической оснащенностью»[1].

А.П. Будников разделяет киберпреступность на две категории:

противоправная деятельность, целью которой являются компьютеры и компьютерные системы;

противоправная деятельность, в которой компьютеры и сети используются для совершения других преступлений, в том числе для распространения вредоносных программ»[2].

Л.А. Аликина отмечает, что в законодательство также внесены изменения, в значительной степени ужесточающие требования к порядку выдачи электронной цифровой подписи и ее использования при подписании документов различными субъектами. Принят закон, на основании которого запрещено принимать оплату товаров, работ и услуг цифровой валютой. У кредитно-финансовых организаций появились полномочия своевременно блокировать переводы денежных средств без согласия клиента[3].

Особенностью современного состояния развития информационного общества является достаточно широкое использование информационно-

---

[1] Шигуров А.В., Шигурова Е.И. Проблемы правовой регламентации использования электронных следов и электронных носителей информации при производстве по уголовному делу // Гуманитарные и политико-правовые исследования. 2020. № 1. С. 53-63.

[2] Будников А.П. Актуальные вопросы возбуждения уголовного дела // Вестник магистратуры. 2022. № 1. С. 39-40.

[3] Аликина Л.А. Актуальные проблемы стадии возбуждения уголовного дела / В сб.: Пермский период. Пермь, 2022. С. 10-12.

телекоммуникационной сети Интернет (далее – Интернет) во многих сферах жизни, в том числе и криминальной. Одним из элементов борьбы с преступлениями в сфере высоких технологий является их предотвращение.

В законодательство внесены изменения, «в значительной степени ужесточающие требования к порядку выдачи электронной цифровой подписи и ее использования при подписании документов различными субъектами»[1].

Принят закон, на основании которого запрещено принимать оплату товаров, работ и услуг цифровой валютой[2]. У кредитно-финансовых организаций появились полномочия своевременно блокировать переводы денежных средств без согласия клиента[3].

Например, приказом МВД России от 27 июня 2018 г. № 167-ФЗ «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений»[4] предписывается осуществлять принятие решения о возбуждении уголовного дела в органе внутренних дел, в который поступило сообщение об IT-преступлении, вне зависимости от места его совершения. Для информационно-аналитического обеспечения мероприятий по выявлению, раскрытию и расследованию IT-преступлений приказом МВД России от 22.04.2020 № 236 введена в эксплуатацию

---

[1] О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»: федеральный закон от 27 декабря 2019 г. № 476-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[3] О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств: Федеральный закон от 27 июня 2018 г. № 167-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[4] О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 3 апреля 2018 г. № 196 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

подсистема программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня «Дистанционное мошенничество»[1].

Приказом МВД России от 29.12.2020 № 925 закреплена временная инструкция по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф», в ней же описаны основные ее принципы[2]. Функциональные возможности указанного программного обеспечения позволяют территориальным органам МВД России проводить анализ информации в целях выявления региональных и межрегиональных совпадений, из них - номеров телефонов, банковских карт, банковских счетов, электронных кошельков. Н.Ф. Цейтлин отметает, что «информационная модель позволит следователю выдвигать следственные версии, относимые к категории типовых, назначение которых – в определении наиболее вероятностных вариантов развития криминалистической ситуации и преступного поведения злоумышленника»[3].

Современный мир таит в себе большое количество угроз и опасностей, каждый день в новостных лентах Интернета, по радио и телевидению сообщают о новых преступлениях, которые нередко совершаются самыми бесчеловечными способами. Следует отметить, что с середины 2000-х гг. социальные сети, технологии беспроводного доступа в Интернет стали частью повседневной жизни граждан. Компьютер превратился в необходимый атрибут повседневной жизни. Все большее количество персональной информации пользователи помещают в информационные системы.

---

[1] О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф»: приказ МВД России от 22.04.2020 № 236 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[2] Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф»: приказ МВД России от 29.12.2020 № 925 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[3] Цейтлин Н.Ф. Преступления, связанные с использованием IT-технологий: проблемы выявления и расследования / В сб.: Актуальные вопросы охраны общественного порядка и административной деятельности. М., 2022. С. 189-192.

Также в последние годы участились случаи распространения наркотических и психотропных средств через сеть Интернет. Участники наркобизнеса не прекращают использовать для совершения наркопреступлений возможности информационно-телекоммуникационных технологии, основным свойством которых является высокий уровень анонимности общения между участниками преступной среды. Значительное количество интернет-ресурсов позволяет пропагандировать потребление и предлагает работу, связанную с распространением наркотиков. В связи с этим необходимо качественно обновлять методы и средства борьбы с преступлениями в сфере незаконного оборота наркотиков на современном этапе.

Исходя из анализа практики, можно убедиться в том, что основным фактором, оказывающим негативное влияние на состояние и развитие криминальной ситуации в сфере незаконного оборота наркотиков, является агрессивное применение преступными группами с целью пропаганды и сбыта запрещенных веществ информационно-телекоммуникационных технологий и сети Интернет.

Данное обстоятельство позволяет наркоторговцам оставаться в тени, осуществляя бесконтактный сбыт наркотических средств, несмотря на принимаемые меры по блокировке интернет-ресурсов, содержащих информацию о запрещенных товарах. Помимо изменения форм сбыта наркотиков с контактного на бесконтактный, на результаты работы по выявлению и раскрытию наркопреступлений оказывает существенное влияние перестройка наркорынка, а именно появление большого количества синтетических наркотиков, поступающих из других стран и производимых в условиях подпольных лабораторий.

Как показывает оперативно-розыскная практика, лица, связанные с незаконным оборотом наркотических средств, объединяются в устойчивые организованные группы, преступные сообщества с большим количеством преступных звеньев, обладающих высоким уровнем специфических знаний о действенных мерах сокрытия следов своей преступной деятельности в сети

Интернет. У каждого из участников преступных групп имеются инструкции, обеспечивающие конспирацию производимых действий и описывающие способы противодействия правоохранительным органам. Кроме того, сведения о пользователях в сети Интернет заменяются на никнеймы (псевдонимы), количество которых у каждого может достигать нескольких десятков.

При этом задерживаются в основном рядовые участники схем продаж наркотиков - курьеры и закладчики, находящиеся в пределах одного или нескольких регионов страны, либо единичные создатели сетевых наркомагазинов, лично осуществляющие закладки. Вместе с тем организаторы, не имеющие контакта с наркотическими средствами и часто находящиеся за пределами Российской Федерации, продолжают их сбывать, вовлекая в преступную деятельность новых лиц.

Необходимо отметить работу по выявлению и пресечению преступлений, совершаемых с использованием сети Интернет. Современные реалии свидетельствуют о том, что наркодельцы все чаще используют для своих преступных целей сеть Интернет-ресурсы. Через «Интернет» идет пропаганда наркотических средств и психотропных веществ, размещаются частные объявления о продаже наркотиков, создаются форумы, где происходит обсуждение процессов изготовления наркотиков, распространение формул их синтеза и обмен ими, а также осуществляется непосредственный сбыт наркотиков, при этом широкое распространение получают системы электронных форм денежных расчетов за сбываемые наркотики.

В целях повышения эффективности противодействия сбыту, приобретению, склонению к потреблению, незаконной рекламе и пропаганде наркотических средств и психотропных веществ с использованием сети Интернет С.Н. Ушекиным были подготовлены рекомендации по поиску вредоносных сайтов в сети «Интернет» и механизм прекращения делегирования доменного имени, проведены практические занятия по применению указанной методики. В результате выявлены сайты, на которых имелись сведения о рецептах изготовления дезоморфина, установлены сайты,

на которых осуществляется продажа «курительных смесей»[1].

Возникающие проблемы «свидетельствуют о недостаточной готовности правоохранительных органов к противостоянию в сере IT-технологий. Сотрудники правоохранительных структур не всегда обладают необходимым уровнем познания компьютерных систем для выявления правонарушений и сбора доказательной базы. Несмотря на привлечение в расследование компьютерных преступлений экспертов, которые позволяют установить обстоятельства, входящие в предмет доказывания, рассчитывать исключительно на специалистов неверно, так как это может повлечь за собой выполнение процессуальных полномочий не в полном объеме или вовсе их потерю»[2].

Для пресечения и предупреждения преступлений, совершенных с использованием IT-технологий, необходимо тесное сотрудничество между отдельными подразделениями правоохранительных органов государства. С активным использованием общей базы возможно качественное осуществление оперативного контроля за лицами, занимающимися незаконными деяниями в области IT-технологий или причастными к этим преступлениям. Данная процедура позволила бы своевременно установить правонарушителей по IP-адресам.

Взаимодействие является неотъемлемой частью деятельности всех правоохранительных органов по выполнению возложенных на них законодательством Российской Федерации, так как помогает обеспечить наиболее эффективную работу по направлению деятельности связанной с обеспечением общественной безопасности на территории Российской Федерации. Очень часто взаимодействие применяется в целях использования специальных знаний. Особое значение имеет организация взаимодействия участкового уполномоченного полиции с гражданами. Важной проблемой

---

[1] Ушекин С.Н. Некоторые проблемные вопросы в борьбе с преступлениями в сфере IT-технологий // Право: ретроспектива и перспектива. 2022. № 2. С. 89-94.

[2] Шигуров А.В., Шигурова Е.И. Указ.соч. С. 53-63.

является политическая пассивность населения муниципальных образований. Хотя сама проблема не имеет в основе взаимодействия участкового уполномоченного полиции с общественностью, пассивная деятельность граждан муниципальных образований приводит к пассивности граждан в области охраны общественного порядка и обеспечения общественной безопасности, что приводит к проблемам взаимоотношений органов внутренних дел и населения.

В действительности, многие ученые, занимающиеся проблемами взаимодействия участкового уполномоченного полиции с общественностью считают, что население нашей страны не готово интегрироваться в такой институт, как правоохранительные органы, так как закрепление в законодательстве положений о работе органов внутренних дел и функционирования различных механизмов правоохранительной деятельности не то же самое, что развить в гражданах высокий уровень правосознания и понимания того, для чего нужна охрана общественного порядка и каким образом каждый конкретный гражданин сможет стать участником этого большого и сложного процесса.

Процесс управления подразделениями территориальных органов МВД России по обеспечению эффективного расследования преступлений в сфере IT-технологий представляет собой комплекс взаимосвязанных, последовательных действий, направленных на реализацию конкретной основной задачи – борьба с преступностью и правонарушениями, достижение которых реализуется путем формирования и реализации конкретных задачи подразделений полиции. Реализация задачи в свою очередь основана на принципах правоприменительного управления, которые вытекают из социальных и правовых принципов – интегрированного, территориального, отраслевого, линейно-зонального, принципа единоначалия и личной ответственности.

В области эффективного расследования преступлений в сфере IT-технологий принцип комплексного подхода к обеспечению защиты граждан

заключается в обеспечении ряда согласованных действий и действий различных подразделений полиции, занимающихся вопросами выявления, предупреждения и пресечения преступлений, а также по выявлению административных правонарушений в этой области, а также по выявлению причин и условий их совершения. Необходимость в этом принципе обусловлена, прежде всего, состоянием оперативной обстановки, которая влияет на безопасность граждан, что влечет за собой обязанность координировать деятельность различных подразделений органа внутренних дел, работающих в одном месте.

Территориальный принцип означает соответствующее объединение территориального органа внутренних дел для определенной территории, как правило, совпадающей с территорией соответствующей административно-территориальной муниципальной единицы. Этот принцип позволяет обеспечить защиту граждан с учетом местных социально-экономических условий, дает возможность повысить эффективность комплексного использования сил и средств.

Отраслевым принципом построения аппарата управления подразделениями является специализация структурных подразделений на определенных направлениях деятельности. Отраслевое построение позволяет сосредоточить силы и средства на управлении однородными подразделениями. Специализация позволяет сотрудникам в полной мере понять содержание поставленных задач, изучить и применить на практике формы и методы работы, разработать меры по повышению эффективности, что, в свою очередь, способствует принятию правильных управленческих решений и их реализации.

Одновременно с отраслевым принципом функционирования является основой для построения всех звеньев полицейских подразделений, что позволяет системе функционировать в целом. Таким образом, в состав территориального органа внутренних дел входят наряду с подразделениями, занимающимися вопросами охраны общественного порядка и обеспечения,

такие подразделения, как кадровые, материально-технические, финансово-экономические, информационно-аналитические, юридические единицы. Эти подразделения проводят анализ эксплуатационной ситуации, занимаются подбором и расстановкой кадров, а также материально-техническим обеспечением подразделений, которые выявляют и пресекают преступления в сфере IT-технологий.

Линейно-зональный принцип заключается в том, что отдельное подразделение или отдельный сотрудник руководит одним направлением работы, то есть специализируется на определенной деятельности. Например, участковый уполномоченный полиции может выявлять преступления в сфере IT-технологий на вверенном ему участке. Особое значение имеет организация взаимодействия участкового уполномоченного полиции с гражданами.

Принцип единоначалия и личной ответственности является обязательным условием деятельности подразделений полиции. Являясь продолжением отраслевого принципа, он обеспечивает единое централизованное руководство, единство технической и кадровой политики в системе МВД России. Этот принцип не исключает коллегиальность при принятии управленческого решения; однако руководитель принимает окончательное решение самостоятельно и несет личную ответственность за деятельность доверенного отдела.

Эти принципы присущи не только деятельности подразделений территориальных органов МВД России, но и другим общественным сферам, в основе которых лежит комплекс практических мер и методов воздействия на общественные отношения в целом для решение поставленных задач.

Важной проблемой эффективного расследования преступлений в сфере IT-технологий является острая нехватка квалифицированных специалистов соответствующей компетенции. Обращаясь к практическому аспекту расследования преступлений в рассматриваемой нами сфере, необходимо отметить, что от верного выбора четкой последовательности следственных и иных процессуальных действий, их квалифицированного и своевременного

выполнения во многом зависит быстрота и успех предварительного расследования, а также всего производства по уголовному делу. Роль алгоритмизации в рассматриваемом аспекте является неоспоримой, так как позволяет обеспечить системный подход в достижении задач первоначального этапа расследования преступлений посредством оперирования тактическими приемами, тактическими комбинациями и тактическими операциями[1].

В настоящее время как в теории, так и в практике государственного управления все чаще возникают вопросы о нуждаемости в каких-либо новых, эффективных способах решения проблем взаимодействия полиции с общественностью.

Особенно необходимо затронуть вопрос виктимологической профилактики, основной целью которой является воздействие на сознание населения, понимание опасностей и незаконности соответствующих действий в сфере высоких технологий. Так, групповой уровень предполагает осуществление компетентными специализированными органами, должностными лицами, общественными организациями и объединениями мероприятий, оказывающих воздействие не на всё население, а на отдельные социальные группы в целях предупреждения преступлений. Такие группы, как правило, характеризуются повышенной степенью виктимности. К ним, например, можно отнести людей старшего поколения, которые очень мало знают о информационных технологиях, а также молодежь, которая очень сильно привязана к всевозможным гаджетам и социальным сетям.

Основными мерами виктимологической профилактики преступлений в сфере IT-технологий являются:

- разработка и распространение профилактических памяток, мобильных и иных интернет-приложений о том, как уберечься от мошеннических действий лиц с использованием мобильных телефонов, с рассмотрением наиболее

[1] Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199-207.

распространенных типовых ситуаций мошеннических схем кражи денежных средств с банковских карт;

- информирование граждан через средства массовой информации о правовом обучении, способах и мерах борьбы с мошенничеством в IT-сфере;

- периодическое проведение групповых и индивидуальных разъяснительных бесед о недопущении виктимного поведения, особенно подростков и лиц старшей возрастной группы;

- обучение граждан приемам блокирования действий телефонных мошенников, оповещение о предстоящих криминогенных ситуациях, ориентирование на поддержание взаимодействия с органами внутренних дел, контроль за поведением потенциальной жертвы и др.

Особенно важна работа, направленная на борьбу с мошенническими действиями, так же, как и другие меры, направленные на предотвращение и борьбу с преступлениями в отношении пожилых людей.

Наиболее эффективным признается частный уровень виктимологической профилактики. Он включает в себя индивидуальные профилактические занятия с отдельными лицами. На данном уровне предполагается индивидуальная работа с гражданами, которые с большей вероятностью могут стать жертвами преступлений вследствие их индивидуальных качеств и характеристик. Так, несовершеннолетние в силу своих физических и психологических особенностей обладают повышенной виктимностью. В связи с этим проведение профилактических мероприятий в отношении данной группы является крайне важным. Однако работу необходимо проводить и с их окружением: сверстниками, с которыми ребёнок или подросток проводит время, родителями, учителями школы, в которой обучается ребёнок, а также с остальными учениками.

Таким образом, под преступлением, совершенным с использованием IT-технологий, понимаются предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо

распространения информации или информационных ресурсов. Преступления, совершенные с использованием IT-технологий, включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического содержания, материалов, возбуждающих межнациональную вражду и т.д.) через Интернет, вредоносное вмешательство через компьютерные сети в работу различных систем, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие необратимые последствия.

Можно выделить следующие причины существования отдельных проблемных вопросов, возникающих в ходе расследования преступлений в сфере IT-технологий. Во-первых, это причины объективного характера и, во-вторых, причины, связанные с профессионализмом сотрудников правоохранительных органов.

Проблемы субъективного характера, выражаются в непрофессиональных действиях сотрудников правоохранительных органов, а также и следователей, которые дают неправильную оценку представленным результатам ОРД, что соответственно нарушает требования действующего уголовно-правового законодательства.

§ 2. Процессуальный порядок возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий

А.А. Калашников отмечает, что в общем виде возбуждение уголовного дела «представляет собой самостоятельную стадию уголовного процесса, в ходе которой компетентное должностное лицо или орган при получении первичной информации о готовящемся или совершенном преступлении, принимает решение о начале производства уголовного дела. При этом стадия возбуждения уголовного дела имеет большое значение, поскольку все принимаемые решения о возбуждении уголовного дела должны быть основаны

на законе и обоснованы»[1].

Возбуждение уголовного дела о преступлениях, совершенных с использованием IT-технологий, происходит согласно розыскной модели, поэтому решение принимают прокурор, а также орган дознания, дознаватель, следователь и начальник следственного отдела с согласия прокурора. Порядок возбуждения дела складывается из трех основных этапов: 1) вынесение постановления, 2) получение согласия прокурора, 3) уведомление о принятом решении заявителя и подозреваемого. Пример постановления представлена в приложении.

Для возбуждения уголовного дела по преступлению в сфере IT-технологий важны повод и основание. Стадия возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий, представляет собой систему действий, которая направлена на оценку информации о совершенном преступлении в сфере IT-технологий и принятие решение о возбуждении либо об отказе в возбуждении производства по данным делам.

Поводом возбуждения уголовного дела служит заявление о преступлении, при этом оно должно быть подписано, то есть иметь конкретное имя заявителя. Согласно ч. 7 ст. 141 Уголовно-процессуального кодекса Российской Федерации[2] (далее - УПК РФ) «анонимное заявление не может служить поводом для возбуждения уголовного дела». Данное условие обусловлено тем, что в случае не анонимности подобного заявления сотрудники, их регистрирующие будут обязаны принимать все заявления о преступлении, в которых, например, могут отсутствовать признаки, указывающие на состав преступления, и даже содержать заведомо ложные обстоятельства. Для решения этой проблемы следует внести точное изменение в понятие анонимности заявления о преступлении. Анонимное заявление о

[1] Калашников А.А. Процессуальные акты стадии возбуждения уголовного дела // Общество. 2022. № 4. С. 102-104.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 дек. 2001 г. // Собр. законодательства Рос. Федерации. 2001. № 52 (ч. 1), ст. 4921.

преступлении может служить поводом для возбуждения уголовного дела только случае, если оно содержит данные, которые указывают на признаки состава преступления.

Определение уголовного преступления невозможно без обращения к такой категории как «состав преступления». Юридический состав любого преступления представляет его важнейшую характеристику, так как состоит из юридически значимых элементов, наличие которых свидетельствует о самом факте административного правонарушения. Отсутствие состава преступления является основанием для прекращения производства по делу в случае, если оно было возбуждено. Следовательно, состав преступления является важнейшей категорией в рассматриваемом институте.

Состав преступления – это совокупность признаков, которые включают в себя объект правонарушения, объективную сторону, субъект и субъективную сторону преступления, наличие которых в конкретном деянии делает последнее уголовно-наказуемым деянием. Данное определение раскрывает не только сущность состава преступления, но и указывает на его составные элементы.

Особенность юридического состава преступления состоит в том, что он раскрывает перечень необходимых признаков, при наличии которых деяние становится уголовным преступлением. Данные признаки носят обезличенный характер и не зависят от конкретных обстоятельств дела. Фактически же состав предполагает совокупность признаков конкретного деяния, то есть он раскрывает уголовно-правовую сущность совершенного деяния. Для правильной квалификации необходимо, чтобы юридический и фактический составы правонарушения совпали. Только в таком случае можно говорить о фактическом наличии уголовного преступления[1].

При определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе

[1] Болтенкова Ю.В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации / В сб.: Поколение будущего: взгляд молодых учены. Курск, 2022. С. 170-174.

сети «Интернет», и, соответственно, территориальной подсудности уголовного дела судам необходимо учитывать, что доступ к данной сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных). Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления (например, при публичных призывах к осуществлению экстремистской деятельности – территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого лица, или использовалось компьютерное устройство для размещения в сети «Интернет» информации, содержащей призывы к осуществлению экстремистской деятельности).

Полномочия прокурора по возбуждению уголовных дел вообще носят чересчур дискреционный характер: при наличии поводов для возбуждения дела, прокурор вправе, как самостоятельно возбудить дело и направить его для рассмотрения уполномоченному субъекту уголовной юрисдикции, так и направить имеющуюся у него информацию для возбуждения дела уполномоченному должностному лицу (под предлогом недопустимости подмены компетенции).

Важно отметить, что вполне исчерпывающие средства и механизмы предупреждения, выявления и пресечения нарушений норм закона и, соответственно, прав и свобод человека и гражданина, имеются и в компетенции отраслевых органов государственной власти, в том числе и обращение в суд в защиту неопределенного круга лиц и публичных интересов (в рамках уголовного судопроизводства). Даже при таком колоссальном объеме дискреции прокурора в действующем правовом регулировании в юридической науке имеются мнения о недостаточности полномочий прокурора по уголовному делу. Так, авторы статей высказываются за необходимость наделения прокурора дополнительными полномочиями самостоятельно прекращать уголовные дела, направленные ему на проверку следователем или

дознавателем, самостоятельно изменять квалификацию преступления по уголовному делу, находящемуся у него на проверке, и, наконец возбуждать уголовное дело[1]. Некоторыми правоведами предлагается приравнять полномочия прокурора по надзору за предварительным следствием к полномочиям по надзору за дознанием[2].

Отмечается, что надзорные процедуры (проверка, процессуального решения о возбуждении уголовного дела, проверка и утверждение обвинительного акта, обвинительного заключения или обвинительного постановления, рассмотрение ходатайств органов предварительного расследования о производстве отдельных следственных действий и избрании мер пресечения перед направлением их в суд и др.), осуществляемые органами прокуратуры на стадии досудебного производства, напротив, затягивают сроки дознания и предварительного следствия.

Каждый участник, чьи права затрагиваются уголовным судопроизводством, имеет свой процессуальный интерес. У потерпевшего (его законных представителей, защитника), а также у обвиняемого (подозреваемого) они очевидны. Первый нацелен на возмещение причиненного преступлением вреда, применение к виновному в совершении преступления справедливого наказания, посредством доказывания вины второго. Второй – на доказывание своей невиновности, исключение или минимизацию подлежащих применению к нему мер пресечения, наказания и совершаемых в его отношении процессуальных действий.

Органы предварительного расследования в данном случае выдвигают уголовно-правовую претензию к обвиняемому (подозреваемому) и принимают исчерпывающие меры по сбору доказательств, позволяющих суду ее удовлетворить.

---

[1] Ахметзянов А.Ф. Система и содержание поводов для возбуждения уголовного дела // Молодой ученый. 2022. № 16. С. 159-161.

[2] Соркин В.С, Козел В.М. Об электронных доказательствах в уголовном процессе (проблемы правоприменения) // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2021. Т. 11. № 2. С. 79-84.

В теории уголовного права и процесса на основе анализа соответствующих законодательных норм следственные действия определяются как часть процессуальных действий, идентифицируемые по субъекту их осуществления, а также по содержанию деятельности.

В узком смысле – это действия должностных лиц, осуществляющих предварительное следствие или дознания, направленные на собирание, исследование, проверку и оценку доказательств.

Следственные действия, в отличие от судебных и иных процессуальных действий направлены исключительно на собирание доказательств по делу (формирование доказательной базы) и осуществляются на стадии досудебного производства в рамках предварительного расследования[1].

Часть вопросов на уровне ведомств решают приказы. Например, приказ Следственного комитета России от 11.10.2012 № 72 «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации»[2]. Так, в п. 20 указано, что не подлежат регистрации и не требуют процессуальной проверки в порядке, предусмотренном ст. 144 и 145 УПК РФ, заявления и обращения, которые не содержат сведений об обстоятельствах, указывающих на признаки преступления. Таким образом, по мнению Ю.В. Болтенковой, в законе следует указать: «Сообщение о преступлении – это полученные из любого источника и облеченные в установленную законом форму сведения об обстоятельствах, прямо указывающих на признаки конкретного преступления»[3].

Следовательно, «в данном случае имеется необходимость реально закрепить в процессуальном законодательстве конкретный перечень поводов

---

[1] Аликина Л.А. Актуальные проблемы стадии возбуждения уголовного дела / В сб.: Пермский период. Пермь, 2022. С. 10.

[2] Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации: приказ Следственного комитета России от 11.10.2012 № 72. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[3] Болтенкова Ю.В. Указ.соч. С. 170-174.

для возбуждения уголовного дела, добавив в него имеющийся рапорт должностного лица органа предварительного расследования о получении сообщения о совершенном или готовящемся преступлении»[1].

Специфика стадии возбуждения уголовного дела и первоначального этапа расследования состоит в относительно небольшом объеме доказательственной информации, полученной следователем основных проблем принятия процессуальных решений на рассматриваемом этапе уголовного процесса является сложность в оценке доказательств. При этом любое используемое в производстве по уголовному делу следственное действие должно не только осуществляться с учетом обеспечения допустимости полученных в результате него доказательств, но и правильно зафиксировано в соответствующем протоколе. Для создания и укрепления гарантий соблюдения прав и свобод человека и гражданина на стадии возбуждения уголовного дела требуется улучшение правового регулирования деятельности должностных лиц по проверке сообщений и заявлений о преступлениях.

Так, в расследовании преступлений в сфере IT-технологий, по нашему мнению, важнейшую роль играет обыск, потому что является одним из правомерных средств собирания достоверных доказательств по расследуемому уголовному делу. Это специфическое следственное действие является эффективным способом и приемом расследования. В связи с чем строгое и неукоснительное следование всем нормам закона при проведении следователем обыска обеспечивает как эффективность этого особого следственного действия, так и соблюдение и уважение гарантированных основным законом России конституционных прав и свобод лиц, вовлеченных в уголовный процесс, а также влияет на допустимость и достоверность собираемых по расследуемому уголовному делу важных доказательств. Реализация всех этих требований, в конечном счете, и служит соответствие целям уголовного процесса и правомерного назначения уголовного судопроизводства. Сегодня научное исследование порядка проведения и тактических особенностей обыска можно

[1] Александров А.С., Андреева О.И., Зайцев О.А. Указ.соч. С. 199-207.

охарактеризовать наличием достаточно различных подходов к определению ситуаций данного следственного действия[1]. Так, одними учеными выделяется конфликтность при его производстве, другие выделяют наличие как конфликтного, так и бесконфликтного его характера. Такой широкий диапазон направленности ситуаций, возникающих при производстве процедуры обыска, на наш взгляд, будет соответственно определять избрание соответствующей тактики проведения этого следственного действия. Как правило, дифференцированный подход выбора тактики к различным возникающим ситуациям при производстве обыска будет способствовать выбору оптимального решения для использования следователем различных приемов.

Организационное обеспечение состоит в том, что для успешного раскрытия и расследования таких дел нередко требуется применение всего арсенала имеющихся в настоящее время технических средств. Технико-криминалистическое обеспечение (ТКО), по нашему мнению, должно строиться с учетом общепринятого в настоящее время в криминалистической науке ситуационного подхода. Практическое значение имеет выделение ситуаций, складывающихся на этапе проверки сообщений о преступлении в сфере IT-технологий до возбуждения уголовного дела, также в ходе предварительного и судебного следствия и выработка практических рекомендаций по наиболее оптимальному применению соответствующих технических средств для соответствующей складывающейся ситуации. Целесообразным, по мнению А.А. Калашникова, является разработка рекомендаций по применению технических средств применительно к отдельным следственным действиям[2].

Так, в ходе расследования ряда уголовных дел установлена причастность гр. С. гр. К. к организации устойчивой преступной группы,

---

[1] Климова М.И. Особенности раскрытия и расследования оперативно-розыскными средствами и методами преступлений, предусмотренных статьей 138 УК РФ, совершенных с использованием информационно-телекоммуникационных технологий / В сб.: Актуальные вопросы теории и практики в деятельности подразделений полиции. М., 2022. С. 30-33.

[2] Калашников А.А. Указ.соч. С. 102-104.

которая осуществляла незаконные приобретения, хранение и пересылку в целях сбыта сильнодействующих веществ - анаболических стероидов. При сбыте анаболических средств, организованная группа использовала почтовые отправления и информационно-телекоммуникационную сеть Интернет. Для этой группы было характерно: единый преступный умысел, направленный на сбыт сильнодействующих веществ; достижение единого преступного результата; стабильность функционирования; постоянный состав группы и распределение ролей между преступниками; планирование криминальных действий на долгий срок; единый источник дохода у каждого из участников группы; стабильные формы и методы сбыта предмета преступления; длительная подготовка к совершению этих преступлений[1].

Важной проблемой считается «некачественная проверка полученного материала, когда максимально сокращаются количество проводимых должностными лицами, осуществляющими предварительное расследование, проверочных действий. Это делается в целях сокращения времени, ресурсов и материальной базы. В большинстве случаях полученной информации оказывается недостаточно для принятия правильного решения и приходится проводить поверочные действия заново. Для решения данной проблемы необходимо максимально точно и качественно проводить каждую проверку всех обстоятельств произошедшего преступления, чтобы ничего не упустить из внимания»[2].

Деятельность по оценке следственной ситуации и выдвижению версий должна осуществляться следователем параллельно. Должно выдвигаться максимальное количество всевозможных версий на основании собранной информации по уголовному делу, в том числе и контрверсии, а также версии защиты. Контрверсия – разновидность криминалистической версии, которая выдвигается с помощью логической операции отрицания основной версии и

---

[1] Приговор Люблинского районного суда г. Москвы от 11 апреля 2016 по ст. 234 УК РФ № 01 - 00090 / 2016. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

[2] Шигуров А.В., Шигурова Е.И. Указ.соч. С. 53-63.

выполняет важную функцию предупреждения односторонности и необъективности расследования. Проверка каждой из выдвинутых версий должна осуществляться оперативно, эффективно и в соответствии с криминалистическими рекомендациями. В процессе проверки выдвинутых версий и по мере поступления новой информации о совершенном преступлении должны быть выдвинуты и подлежат проверке иные версии.

Подводя итог важно подчеркнуть, что стадия возбуждения уголовного дела представляет собой первую стадию уголовного процесса. Институт возбуждения уголовного дела в российском уголовном процессе играет роль своеобразного фильтра, позволяющего отсеивать деяния, которые в соответствии с уголовным законом не являются преступлениями. Одной из главных трудностей в расследовании преступлений, совершенных с использованием IT-технологий, безусловно, является непостоянство места совершения преступления. Современный мир предлагает широкий выбор технических устройств для подключению к глобальной сети, в основной массе переносных (нестационарных). На данной стадии в том числе необходимо проверять лицо, совершившее преступные действия, на соответствие требованиям уголовного закона, предъявляемым к признакам субъекта преступления.

ГЛАВА 2. ПРОБЛЕМНЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОЦЕССУАЛЬНОГО ПОРЯДКА ВОЗБУЖДЕНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

§ 1. Доследственная (предварительная) проверка сообщения о преступлении как способ установления основания возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий

Поводы и основания, необходимые для возбуждения уголовного дела, содержатся в ст. 140 УПК РФ, в которой в качестве поводов для возбуждения уголовного дела законодатель выделил (ч. 1 ст. 140 УПК РФ):

- Заявление о преступлении.

- Явку с повинной.

- Сообщение о совершенном или готовящемся преступлении, полученное из иных источников.

- Постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

Согласно ч. 2 ст. 140 УК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления.

Соответственно, стадия возбуждения уголовного дела по преступлениям, совершенных с использованием IT-технологий, подразумевает выявление обстоятельств, позволяющих судить о совершении преступления[1].

Для эффективного расследования преступления следователь должен знать механизм закономерностей о преступных действиях. Этот механизм является сложной динамической системой, в которую входит и лицо,

[1] Аликина Л.А. Указ.соч. С. 10-12.

совершившее преступление, его действия и отношения к преступлениям и их последствиям; предмет деятельности; способ совершения неправомерного действия и т.д.

Механизм преступных действия в сфере компьютерной информации (ст. 272-274.4 УК РФ) представляет собой комплекс действий лица по подготовке к совершению неправомерного доступа. Особенность значимых сведений об обстоятельствах преступления заключается в том, что сведения могут содержаться как в одном, так и в нескольких электронных носителях, если они объединены в одну информационную систему. Информационную систему же формирует база информации (данных). Совокупность электронных баз данных в судебной практике[1] часто определяют через понятие «виртуальное пространство». Возможность синхронизации и последовательной реализации столь разнообразной деятельности по созданию баз данных (виртуального пространства) формирует структуру электронной комплексной системы[2].

Требования к качественному досудебному производству складываются из необходимости обеспечения полноты, всесторонности расследования.

Несмотря на имеющийся в теории и практике пошаговый механизм выполнения определенного алгоритма действий, каждое уголовное дело уникально, а потому четкого плана действий предусмотреть невозможно. Определенные временные рамки на расследование уголовного дела диктуют максимально рациональное использование всего комплекса следственных мероприятий для обеспечения полноты, всесторонности и объективности расследования. Правила оценки доказательств фактически основаны на этической составляющей субъективного познания, поскольку базируются на принципах внутреннего убеждения, всесторонности, полноты, объективности и

---

[1] Постановление Суда по интеллектуальным правам от 20.06.2019 № С01 -390/2019 по делу № А40-169068/2018 (Дата обращения: 12.04.2023 г.); Постановление Арбитражного суда Московского округа от 29.11.2019 № Ф05-18806/2019 по делу № А40-217942/2018 // Консультант-Плюс: справочно-правовая система (Дата обращения: 12.04.2023 г.).

[2] Бердникова О.П. Порядок получения электронных доказательств при проведении отдельных следственных действий // Право и государство: теория и практика. 2022. № 1. С. 366-368.

непосредственности исследования. Именно поэтому четкость действий, правильно и грамотно спланированный график выполнения всех следственных действий является залогом не только эффективного рабочего графика следователя, но и общей организации его работы.

Основной формой процесса доказывания выступает комплекс проводимых дознавателем следственных действий. При этом важнейшим условием, обеспечивающим допустимость полученных доказательств, является тщательное соблюдение всех процедурных нюансов производства следственных действий и их процессуальное оформление[1].

Завершающим обстоятельством является подтверждение выводов заключения эксперта другими фактическими данными и доказательствами, уже установленными к этому моменту по делу, т.е. устанавливается относимость экспертного заключения

С учетом положений п. 33 ст. 5 УПК РФ можно выделить признаки уголовно-процессуальных решений:

- направлены на реализацию назначения уголовного судопроизводства;

- основаны на установленных обстоятельствах;

- принимаются уполномоченными субъектами (должностными лицами органов предварительного расследования, прокуратуры и суда);

- вытекают из требований закона и облечены в установленную законом форму;

- обеспечиваются государственным принуждением.

Анализ содержания положений УПК РФ (ч. 4 ст. 7, ст.ст. 91, 101, 181 и др. УПК РФ) подтверждает, что процессуальные решения должны быть обоснованными и мотивированными[2].

Сегодня «использование как компьютерной, так и информационно-

---

[1] Антонова Е.Ю. Новые формы преступной деятельности в условиях цифровизации // Ученые записки юридического факультета. 2022. № 1. С. 18-23.

[2] Александров А.С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 130-139.

телекоммуникационной техники существенно в несколько раз расширило возможности органов внутренних дел в решении злободневных задач по раскрытию и расследованию преступлений»[1].

В настоящее время в криминалистической науке актуализируются вопросы внедрения в оперативно-служебную деятельность органов внутренних дел разработок, способствующих совершенствованию имеющихся методов, средств, приемов, направленных на выявление, собирание, исследование и использование доказательств.

Установление обстоятельств, подлежащих доказыванию по уголовному делу (ст. 73 УПК РФ), во многом определяется «компонентным составом компьютерной сети и их взаимообусловленным функционированием. Базовый элемент компьютерной сети (такой как подсистема), структурные составляющие которого могут быть источниками доказательственной информации об обстоятельствах совершенного преступления, представляет собой объединенные в группы компьютеры и ряд других компьютерных устройств (специалисты называют их телекоммуникационными сетевыми узлами), связанных друг с другом каналом связи и реализующих соответствующую программу»[2].

Цифровая информация в компьютерной сети распространяется по заданным программами маршрутам «в виде последовательной и полной цепи отраженных сведений, замкнутых по смыслу»[3]. Существо содержания криминалистически значимого следа заключается (проявляется) в изменениях цифровой информации, в разнице между тем «как было» до преступного воздействия и «как стало» после завершения «атаки».

Чтобы получить сведения об обстоятельствах расследуемого

---

[1] Кравцов Д.А. Некоторые аспекты предупреждения киберпреступности // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22). С. 57-60.

[2] Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-25..

[3] Мухина Ю.Р., Бельский А.И. Проблемы уголовно-правовой квалификации преступлений, совершенных с использованием IT-технологий / В сб.: Современность в творчестве начинающего исследователя. Иркутск, 2022. С. 168-170.

преступления в сфере компьютерной информации, субъект расследования при проведении следственных действий должен обладать навыками специалиста в сфере обмена цифровой информацией:

- исследовать хранящуюся в компьютерной цепи цифровую информацию;

- обнаруживать среди этой информации сведения, подтверждающие совершенное преступление (найти электронный след);

- фиксировать результаты поисковой деятельности в процессуальных документах.

При выполнении действий по обнаружению и изъятию доказательственной информации в ряде случаев используют помощь специалиста уже на подготовительном этапе. Следователь «предусматривает и принимает меры к исключению возможности ее возникновения за счет использования фактора внезапности производства следственного действия, привлечения сил и средств блокирования доступа к сети, дистанционного на нее воздействия с целью размагничивания носителей и таким способом уничтожения цифровой следовой картины. Ч. 7 ст. 164 УПК РФ закрепляет право следователя использовать сотрудников оперативных подразделений при производстве следственного действия»[1].

Особое значение приобретают тактико-криминалистические алгоритмы первоначального этапа расследования преступлений. Так, благоприятная для расследования следственная ситуация складывается, как правило, в результате совершения преступления на почве внезапно возникших личных неприязненных отношений, конфликта между преступником и потерпевшим, ранее знавшими друг друга. Несмотря на то, что такая ситуация является благоприятной для расследования, однако нередко она становится неблагоприятной при некачественном сборе материалов на первоначальном этапе, особенно в случае, когда обе стороны пытаются противодействовать расследованию, так как являются знакомыми, родственниками и

[1] Разувакина И.И., Разувакин А.А. Указ.соч. С. 156-159.

примирились[1].

Таким образом, следует согласиться с научной общественностью, что определяющим эффективность производства по уголовному делу фактором являются глубокие познания субъекта расследования (следователя, дознавателя) в различных видах и сочетаниях компьютерных сетей, компьютерных устройств, компьютерных технологий.

§ 2. Решения, принимаемые на стадии возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий

Проверка сообщений о преступлениях рассматриваемой категории дел реализуется «путем обращения к оперативно-розыскным мероприятиям, помимо того анализ следственной практики демонстрирует, что главный повод для возбуждения уголовного дела с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, - это рапорт сотрудника следственного аппарата об обнаружении признаков, указывающих на совершения преступления»[2].

Планирование расследования зависит не только от сложившейся по уголовному делу следственной ситуации, но и от выдвинутых версий. Деятельность по оценке следственной ситуации и выдвижению версий должна осуществляться следователем параллельно. Должно выдвигаться максимальное количество всевозможных версий на основании собранной информации по уголовному делу, в том числе и контрверсии, а также версии защиты. Контрверсия – разновидность криминалистической версии, которая выдвигается с помощью логической операции отрицания основной версии и выполняет важную функцию предупреждения односторонности и необъективности расследования. Проверка каждой из выдвинутых версий должна осуществляться оперативно, эффективно и в соответствии с

[1] Соркин В.С, Козел В.М. Указ.соч. С. 79-84.
[2] Ушекин С.Н. Указ.соч. С. 89-94.

криминалистическими рекомендациями. В процессе проверки выдвинутых версий и по мере поступления новой информации о совершенном преступлении должны быть выдвинуты и подлежат проверке иные версии.

Одним из принципов построения комплексной методики раскрытия, расследования и предупреждения преступлений указывается разработка криминалистических рекомендаций по взаимодействию следователей, дознавателей и других участников раскрытия, расследования и предупреждения преступлений. Выделение категории «серьезных» преступлений встречается как в литературе, так и в практической деятельности, однако это не значит, что по одним преступлениям необходимо работать, а другие (простые) можно и отложить, так как за каждым уголовным делом стоит чья-то судьба. В данном случае различаться может объем следственных действий, но процесс организации расследования всегда должен исходить из принципов уголовного судопроизводства.

Уголовные дела по ч. 2 ст. 272 УК РФ в некоторых случаях, когда вред преступлением был небольшой, следователь может о ходатайствовать о прекращении уголовного дела с назначением судебного штрафа. Так, рассматривая уголовное дело № 1-256/2017 от 17 ноября 2017 года по ч. 2 ст. 272 УК РФ, отметим, что Устиновский районный суд г. Ижевска Удмуртской Республики удовлетворил ходатайство следователя в отношении П., поскольку данный гражданин вину свою признал полностью, согласился на назначение меры уголовно-правового характера в виде судебного штрафа. В данном конкретном случае органы предварительного следствия установили, что П., находясь в квартире потерпевшего, из корыстного умысла с целью последующей продажи информации о логине и пароле доступа к сети Интернет, смог подобрать логин и пароль и изменил их. Данные действия П. нарушили модификацию и блокировку компьютерной информации потерпевшей. Однако, поскольку преступление по ч. 2 ст. 272 УК РФ относится к преступлениям средней тяжести, а также наличии положительной характеристики П., к тому же П. полностью загладил причиненный

преступлением вред, суд постановил назначение П. меру уголовного-правового характера в виде судебного штрафа в размере 15 тысяч, с чем П. согласился, поэтому на основании ст. 25.1 УПК РФ уголовное дело в отношении П было прекращено[1].

К сожалению, многие лица, имеющие соответствующие знания в области IT-технологий, часто в корыстных целях совершают неправомерные деяния в отношении юридических лиц, нанося вред их коммерческой деятельности. Рассматривая уголовное дело № 1-613/2017, которое было рассмотрено Октябрьским районным судом г. Ростов-на-Дону 1 декабря 2017 года, отметим, что М. специально написал компьютерную программу с целью проверки учетных записей магазина и за деньги через сеть Интернет продавал полученную информацию заинтересованным лицам. Уголовное дело против М. было возбуждено по ч. 2 ст. 272 УК РФ, поскольку М. осуществлял неправомерный доступ к компьютерной информации без ведома и согласия ее владельца. Суд квалифицировал действия М. по ч. 2 ст. 273 УК РФ и ч. 2 ст. 272 УК РФ. Подсудимый М., являющийся несовершеннолетним, свою вину признал полностью, в содеянном чистосердечно раскаялся, подал ходатайство о постановлении приговора без судебного разбирательства. При определении меры наказания М. судом было учтен характер и степень опасности причиненного вреда преступлением, а также личность подсудимого, вследствие чего были учтены смягчающие обстоятельства. Учитывая возможность исправления и перевоспитания М. без изоляции от общества, но в условиях контроля за его поведением специализированным государственным органом, суд пришел к выводу, что для достижения целей уголовного наказания

[1] Приговор по делу № 1-256/2017 от 17 ноября 2017 года Устиновского районного суда г. Ижевска Удмуртской Республики [Электронный ресурс]: Режим доступа: https://sud-praktika.ru/precedent/546816.html (Дата обращения: 12.04.2023 г.).

возможно назначить М. наказание в виде лишения свободы с применением ст. 73 УК РФ условно с испытательным сроком 2 года[1].

Ненадлежащая организация работы по проведению процессуальной проверки по сообщениям о мошенничествах, совершенных в сети Интернет, приводит к преждевременному принятию органами предварительного расследования решений о возбуждении уголовных дел»[2].

Так, «9 июля 2020 года в отдел полиции № 7 УМВД России по г. Нижнему Новгороду обратился «Л» с заявлением о хищении денежных средств с банковской карты суммой 14.809,42 рублей. В своем заявлении «Л» указал, что неустановленное лицо путем предоставления подложных документов на его имя оформило кредитный договор, в результате чего с его банковского счета на основании судебного приказа были списаны денежные средства. В связи с тем, что доследственная проверка была проведена не в полном объеме, следователем было возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ, которое в дальнейшем было прекращено в связи с отсутствием состава преступления (установлено, что заявитель сам оформил кредитный договор путем подачи электронной заявки в сети Интернет)»[3].

Рассматривая возбуждение уголовного дела по преступлениям, совершенных с использованием IT-технологий, например, связанных с незаконным оборотом оружия с использованием сети Интернет, отметим, оперативные сотрудники преимущественно получают информацию о незаконном обороте оружия в сети Интернет от лиц, ранее осужденных за аналогичные преступления, которые на конфиденциальной основе

---

[1] Приговор по делу № 1-613/2017 Октябрьского районного суда г. Ростов-на-Дону от 1 декабря 2017 года [Электронный ресурс]: Режим доступа: html https://sud-praktika.ru/precedent/467627.html (Дата обращения: 12.04.2023 г.).

[2] Шигуров А.В., Шигурова Е.И. Указ.соч. С. 53-63.

[3] Обзор практики раскрытия и расследования уголовных дел о хищениях, совершенных с использованием информационно-телекоммуникационных технологий в Нижегородской области за 2020 год [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

сотрудничают с органами внутренних дел.

Торговля оружием стала практически бесконтрольной в общемировом масштабе, причиной тому является нестабильная политическая ситуация в ряде стран. Геополитическое положение нашего государства остается сложным и уязвимым и сегодня. Для предупреждения незаконного оборота оружия важно совершенствовать законодательную базу, касающуюся вопросов установки единых требований к обороту оружия, боеприпасов, взрывчатых веществ и взрывных устройств не только внутри страны, но и во взаимосвязи со странами СНГ, странами Прибалтики. Необходимо тесное сотрудничество между правоохранительными органами данных государств.

Как мы отмечали выше, «при возбуждении уголовных дел, совершенных с использованием IT-технологий, заявление о преступлении, поступившее анонимно, не может выступать как повод для возбуждения уголовного дела, что закреплено ч. 7 ст. 141 УПК РФ. При этом в Приказе МВД «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» от 29 августа 2014 г. № 736 определено, что данная инструкция не распространяет свое действие на анонимные сообщения, в которых содержатся данные либо о готовящихся, либо об уже свершившихся противоправных деяниях. Исключения составляют преступления террористической направленности»[1]. Однако возможность подачи анонимного заявления о незаконном обороте оружия в сети Интернет (по аналогии с притуплениями террористической направленности) позволила бы существенно расширить круг источников информирования правоохранителей о совершении рассматриваемого вида преступлений, что, в свою очередь, приведет к большей эффективности возбуждения уголовных дел по данному виду преступлений. Кроме того, специалисты отмечают тесную

[1] Александров А.С., Андреева О.И., Зайцев О.А. Указ.соч. С. 199-207.

взаимосвязь, существующую между терроризмом и незаконным оборотом оружия.

Уголовная политика в сфере незаконного оборота оружия – это борьба государства, которая направлена на предотвращение, пресечение и профилактику преступности. Основная цель юридической науки – оказывать поддержку правоохранительным структурам в пресечении, выявлении преступной деятельности.

В данном аспекте востребованным можно назвать мнение Ю.В. Болтенкова, считающего, что существуют категории преступлений, возбуждение которых не требует данных об анонимном заявителе[1]. По мнению исследователя, справедливым данное утверждение будет в отношении, например, анонимного заявления о раскладывании наркотических средств в придомовых территориях. Как и в случае с терроризмом, допустимость анонимного заявления о незаконном обороте оружия в сети Интернет способствовала бы увеличению динамики дел, возбужденных на основании выявления признаков данного вида преступлений. Одновременно с этим внедрение обозначенного шага в практическую деятельность правоохранительных органов позволило бы снизить латентность незаконного оборота оружия с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, что в полной мере соответствует принципу высокого уровня раскрываемости преступлений.

При выявлении места совершения преступного деяния, определения места расследования в некоторых ситуациях требуется дополнительно брать в расчет место регистрации IP-адреса[2], с которого был произведен выход в сеть Интернет, в процессе которого и было совершено преступление. По наблюдениям Л.В. Головко, «не будет редкостью несовпадение места

---

[1] Болтенкова Ю.В. Указ.соч. С. 170-174.

[2] IP-адрес – это уникальный адрес, идентифицирующий устройство в интернете или локальной сети. IP означает «Интернет-протокол» – набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть.

совершения преступления, совершенного в сети Интернет, с местом расследования»[1]. Подобное положение дел может формировать сложности для возбуждения уголовного дела, заключающиеся в проверке материалов, необходимых для такового.

Ситуационная природа расследования проявляется в оценке складывающейся на определенный момент времени обстановки, в которой протекает оперативно-розыскные мероприятия, и определения на этой основе оптимальных тактических решений, которые включают такие процессуальные действия как назначение судебной экспертизы, производстве осмотра места происшествия, документов, предметов и других. В данном случае необходимо обратить внимание, что сбор доказательственной информации и формирование структурных элементов происходит на этапе проверки сообщения о преступлении, но в литературе чаще встречается определение «планирование расследования», и если мы говорим о планировании как об интеллектуальном процессе, то правильным будет планирование раскрытия и расследования преступления. В отдельную группу выделяется работа следственно-оперативной группы, которая создается на суточное дежурство и осуществляется по многоэпизодным делам сложной категории.

На сложности, возникающие при возбуждении уголовных дел по преступлениям, совершенным при помощи сети Интернет, указала Е.Ю. Антонова. В частности, автор пишет, что «в преступлениях, где присутствуют телекоммуникационные технологии, местом преступления признается не один лишь физический, т. е. традиционный адрес, но и определенная часть информационного пространства (сайт, домен), где фактически активным пользователем совершалось преступление. Таким примером выступает сайт, зарегистрированный на определенном сервере, который имеет физическое местоположение, и его пользователь, т. е. лицо,

[1] Головко Л.В. Указ.соч. С. 15-25.

которое при совершении преступления находится на конкретном адресе»[1].

Задач в уголовной науке достаточно много и все подразделяются на классификации по разным принципам: общие, частные и конкретные задачи.

- общие задачи предусматривают цель науки и определяют ее основное направление развития;

- частные задачи осуществляют всеобщие задачи науки и определяют направленность развития ее разделов;

- конкретные задачи обуславливают развитие определенных теоретических взглядов и концепций данной науки.

Итак, при возбуждении уголовного дела по преступлениям, совершенным с использованием IT-технологий, может возникнуть следующий наиболее существенный комплекс проблем:

1. Отсутствие возможности подать анонимное заявление о совершении преступления, например, незаконного борота оружия в сети Интернет, что сужает круг информаторов о данном виде преступления. В свою очередь, это приводит к тому, что по ряду фактов незаконного оборота оружия возбуждение уголовного дела не происходит вовсе, т. к. гражданские лица, которым стало известно о преступлении такого рода, не желают сообщать о данных фактах от своего имени.

2. Затруднения, связанные с запретом на получение материалов, необходимых для возбуждения уголовного дела на стадии возбуждения уголовного дела (ряд действий допускается лишь на стадии предварительного расследования).

3. Зачастую на стадии возбуждения уголовного дела отсутствует конкретный подозреваемый, что приводит к увеличению объема и сроков расследования уголовного дела.

4. Несовпадение места преступления, совершенного с использованием сети Интернет, с местом его расследования.

---

[1] Антонова Е.Ю. Новые формы преступной деятельности в условиях цифровизации // Ученые записки юридического факультета. 2022. № 1. С. 22.

Таким образом, проблемы, возникающие при возбуждении уголовных дел по преступлениям, совершенных с использованием IT-технологий, во многих моментах исходят от специфики данного вида преступлений, в частности, информирования о нем. Необходимо отметить, что своевременная разработка специальных мер по противодействию преступлениям в сфере IT-технологий, будет способствовать существенному повышению уровня информационной безопасности нашей страны и эффективной борьбе с противоправными деяниями в киберпространстве.

Так, круг субъектов, позволяющих информировать правоохранительные органы, к примеру, о незаконном обороте оружия в сети Интернет, в настоящий момент не является полным, из-за чего латентность такого вида преступлений возрастает. Следовательно, сам факт возбуждения уголовного дела по рассматриваемой категории преступлений способен привести к дальнейшему падению динамики.

На стадии проверки сообщения о преступлении, совершенном в сети Интернет, основная часть мероприятий возложена на орган дознания. «От качества проведенной предварительной проверки зависит эффективность расследования и раскрытия возбужденного уголовного дела. После того, как материалы предварительной проверки будут детально проверены, в случае наличия достаточных на то оснований выносится решение о возбуждении уголовного дела, которое будет иметь некоторые достаточно существенные различия от возбуждения уголовных дел по преступлениям, совершенным более традиционным способом, т. е. без использования новых технологий и средств телекоммуникаций»[1].

В постановлении о возбуждении уголовного дела, совершенных с использованием IT-технологий, «очерчиваются пределы производства по кругу деяний (если дело возбуждается только по факту), а также по кругу лиц (если оно возбуждается в отношении конкретного лица). Это создает правовую

[1] Ушекин С.Н. Указ.соч. С. 89-94.

определенность и снижает риск злоупотреблений, в частности использования полномочий для сбора информации в отношении граждан и организаций за пределами производства»[1].

С учетом положений п. 33 ст. 5 УПК РФ можно выделить признаки уголовно-процессуальных решений:

- направлены на реализацию назначения уголовного судопроизводства;

- основаны на установленных обстоятельствах;

- принимаются уполномоченными субъектами (должностными лицами органов предварительного расследования, прокуратуры и суда);

- вытекают из требований закона и облечены в установленную законом форму;

- обеспечиваются государственным принуждением.

Уголовно-процессуальные решения могут быть приняты только уполномоченными субъектами в пределах своей компетенции, то есть только в рамках зарегистрированного и подлежащего проверке материала о совершенном, совершаемом или готовящемся преступлении или возбужденного уголовного дела; на досудебном производстве – следователем, органом дознания, дознавателем, принявшим уголовное дело (материал) к своему производству (возможно, руководителем следственного органа в случае, когда он самостоятельно проводит расследование), либо должностным лицом по поручению субъекта, ведущего производство.

В случае принятия решения лицом на основании поручения субъекта проверки сообщения (производства предварительного расследования) пределы прав исполнителя ограничены поручением. Так, при поручении о производстве следственного действия исполнитель самостоятельно может определить дату и время проведения действия (если это возможно по поручению), его участников, тактику и другие аспекты проведения следственного действия[2].

---

[1] Аликина Л.А. Указ.соч. С. 10-12.

[2] Калашников А.А. Указ.соч. С. 102-104.

Анализ содержания положений УПК РФ (ч. 4 ст. 7, ст.ст. 91, 101, 181 и др. УПК РФ) подтверждает, что процессуальные решения должны быть обоснованными и мотивированными. Специфика стадии возбуждения уголовного дела, совершенных с использованием IT-технологий, состоит в относительно небольшом объеме доказательственной информации, полученной следователем основных проблем принятия процессуальных решений на рассматриваемом этапе уголовного процесса является сложность в оценке доказательств[1].

В последние годы появились новые виды преступлений с использованием интернет-ресурсов. К таким преступлениям можно отнести склонение с совершению самоубийства. Стоит отметить, что общественная опасность в данном случае заключается в том, что задания и «смертельные игры» направлены на неопределенное число лиц, в частности на несовершеннолетних, а в основной своей массе - на лиц, не достигших возраста 12 лет. Поэтому было целесообразно каким-либо образом декриминализовать действия лиц, осуществляющих деятельность, направленную на побуждение к подобному антисоциальному явлению, и привлекать их к уголовной ответственности, что возможно лишь при внесении дополнений в ст. 110 УК РФ либо изменении УК РФ, как и поступил законодатель.

Одним из критикуемых нами положений является широкое толкование квалифицирующего признака «распространение информации о способах совершения самоубийства» в связи с тем, что отсутствует законодательное определение нормы, в частности, нет Пленума Верховного Суда Российской Федерации, разъясняющего положения, дающего определения основных понятий и т.д. В законодательстве отсутствует определение «информация о способах самоубийства». Соответственно, под заложенным законодателем понятием возможно «обыденное» расширительное толкование и, казалось бы, упоминание таких понятий, как «вскрытие вен», «повешение», «выбрасывание

[1] Мухина Ю.Р., Бельский А.И. Указ.соч. С. 168-170.

из окна», и других способов самоубийства (которые повсеместно встречаются на страницах классической, художественной литературы, в СМИ, а также в специальных медицинских изданиях) является «распространением информации о способах совершения самоубийства».

Все же под «распространением информации о способах совершения самоубийства» следует понимать такие рекомендации и советы, которые, во-первых, прямо направлены на побуждение желания совершить самоубийство, а во-вторых, достаточны и необходимы (рекомендации) для наступления указанных в диспозиции статьи последствий. Например, пользователь социальной сети «Одноклассники» на своей личной странице публикует порядок изготовления смертельной медикаментозной дозы снотворного, советует оставить предсмертную записку, рассказывает о преимуществах смерти и т.п.

В связи с этим предлагаемые законодателем изменения в УК РФ не всегда являются эффективными в отношении истинных организаторов действий, направленных на склонение или содействие совершению самоубийства. Ведь до сих пор существует проблема расшифровки IP-адреса, который можно легко скрыть, а также возможно указать иное местонахождение, и не стоит исключать другие различные технические средства, которые могут позволить избежать ответственности.

При более тщательном исследовании становится очевидно, что под признаки преступления будут подпадать и пользователи сети, страницы которых направлены на профилактику суицидов, в том числе путем объяснения истинных последствий таких действий. А также, учитывая «палочную систему», под уголовную ответственность могут попасть и продавцы веревок, ножей, родители, педагогические работники и многие другие лица.

В результате закрадывается мысль, что цели наказания, предусмотренные ст. 43 УК РФ, не достигаются. Кроме этого, казалось бы, деяния, предусмотренные ст. 110.1, ст. 110.2 УК РФ, в соответствии с действующим уголовным законодательством не являются и не могут являться преступлением,

поскольку лицо, в отношении которого совершаются указанные деяния, то есть потерпевший, исходя из содержания приведенных статей, выступает соучастником этих деяний. Но УК РФ не предусмотрена уголовная ответственность за самоубийство или покушение на самоубийство, и, соответственно, склонение к совершению указанных действий не может являться преступлением, как, например, не может являться преступлением склонение потерпевшего к совершению мошенничества в его же отношении и т.п., поскольку такая формулировка является абсурдной (в соучастии с потерпевшим нельзя совершить преступление).

И самое главное: «социальный эффект», казалось бы, ведет к росту преступности в отношении несовершеннолетних, т.к. основными участниками «групп смерти» и подобных интернет-коммуникаций, имеющих деструктивную направленность, являются подростки. Можно прийти к выводу о том, что, несмотря на то, что уголовное законодательство развивается параллельно социальной практике, предусматривая уголовную ответственность за новые общественно опасные социальные явления, на практике реализация новых положений уголовно закона вызывает множество вопросов. Так, в аспекте уголовно-правовой охраны здоровья и жизни человека, исследуемого с позиции уголовно-правовой регламентации новых противоправных деяний, остаются недостаточно понятными и юридически точными, в связи с чем требующими повышенного законодательного внимания и нормативного закрепления, как уже имеющиеся дефиниции (ст. 110 УК РФ), так и закрепленные в новых составах, в частности ст. 110.1, 110.2 УК РФ.

Таким образом, хотелось бы еще раз отметить, что самоубийство как важнейшая социальная проблема существует в нашем обществе очень давно. С массовым развитием телекоммуникационных технологий проблема доведения до самоубийства актуализировалась.

Решение о возбуждении уголовного дела принимается не только на основании материалов предварительных проверок заявлений потерпевших, организаций и должностных лиц, но и, как указывалось выше, по материалам

органов, осуществляющих оперативно-розыскную деятельность при реализации оперативных разработок, результатов оперативно-розыскных действий по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших.

Необходимо отметить, что методика расследования преступлений, совершенных с использованием IT-технологий, имеет ряд существенных отличий от расследования иных преступлений. Некоторые методы и средства являются общими, в том числе и для данного вида преступлений. Значительную роль в расследовании таких преступлений играет программное обеспечение, которое должно быть развито на соответствующем современному миру уровне. Следует постоянно обновлять информационную базу касательно различных приемов и ухищрений, используемых преступниками в таких преступлениях. Особое значение для расследования оказывают специалисты в отдельных областях знаний, осуществляющие содействие следствию, как на этапе предварительного расследования, так и на этапе до возбуждения уголовного дела, при проведении проверки сообщения о преступлении.

Процесс выявления и последующее возбуждение уголовного дела по IT-преступлениям представляет особую сложность в деятельности органов внутренних дел, в частности в профессиональной деятельности следователей, поскольку сложность заключается в правильности квалификации того или иного преступления. Характер электронных доказательств (то есть данных, хранящихся в компьютерной системе и цифровой форме) предопределяет необходимость применения подхода, отличного от традиционных процедур проведения обыска и изъятия. В ходе проведения следственных действий, сотрудникам следственных подразделений необходимо заранее подготовиться к изъятию цифрового носителя информации, на котором хранилась преступная информация. Для правильной квалификации преступного деяния в сфере IT-технологий, следователям следует повышать свою квалификацию, обладать специальными познаниями в области информационно-электронных технологий.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать следующие выводы.

1. Под преступлением, совершенным с использованием IT-технологий, понимаются предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. Преступления, совершенные с использованием IT-технологий, включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического содержания, материалов, возбуждающих межнациональную вражду и т.д.) через Интернет, вредоносное вмешательство через компьютерные сети в работу различных систем, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие необратимые последствия. Преступления в сфере компьютерной информации с использованием IT-технологий иначе именуются киберпреступностью.

2. К сожалению, многие лица, имеющие соответствующие знания в области IT-технологий, часто в корыстных целях совершают неправомерные деяния в отношении юридических лиц, нанося вред их коммерческой деятельности. Также в последние годы появились новые виды преступлений с использованием интернет-ресурсов. К таким преступлениям можно отнести склонение с совершению самоубийства. Стоит отметить, что общественная опасность в данном случае заключается в том, что задания и «смертельные игры» направлены на неопределенное число лиц, в частности на несовершеннолетних, а в основной своей массе - на лиц, не достигших возраста 12 лет. Поэтому было целесообразно каким-либо образом декриминализовать действия лиц, осуществляющих деятельность, направленную на побуждение к подобному антисоциальному явлению, и привлекать их к уголовной ответственности.

3. Выделены следующие причины существования отдельных проблемных вопросов, возникающих в ходе расследования преступлений в сфере IT-технологий. Во-первых, это причины объективного характера и, во-вторых, причины, связанные с профессионализмом сотрудников правоохранительных органов. Проблемы субъективного характера, выражаются в непрофессиональных действиях сотрудников правоохранительных органов, а также и следователей, которые дают неправильную оценку представленным результатам ОРД, что соответственно нарушает требования действующего уголовно-правового законодательства.

4. Стадия возбуждения уголовного дела представляет собой первую стадию уголовного процесса. Институт возбуждения уголовного дела в российском уголовном процессе играет роль своеобразного фильтра, позволяющего отсеивать деяния, которые в соответствии с уголовным законом не являются преступлениями. Стадия возбуждения производства представляет собой систему действий, которая направлена на оценку информации о совершенном преступлении в сфере IT-технологий. Специфика стадии возбуждения уголовного дела, совершенных с использованием IT-технологий, состоит в относительно небольшом объеме доказательственной информации, полученной следователем основных проблем принятия процессуальных решений на рассматриваемом этапе уголовного процесса является сложность в оценке доказательств. Одной из главных трудностей в расследовании преступлений, совершенных с использованием IT-технологий, безусловно, является непостоянство места совершения преступления. Современный мир предлагает широкий выбор технических устройств для подключению к глобальной сети, в основной массе переносных (нестационарных). На данной стадии в том числе необходимо проверять лицо, совершившее преступные действия, на соответствие требованиям уголовного закона, предъявляемым к признакам субъекта преступления.

5. Порядок возбуждения уголовного дела о преступлениях, совершенных с использованием IT-технологий, складывается из трех основных этапов: 1)

вынесение постановления, 2) получение согласия прокурора, 3) уведомление о принятом решении заявителя и подозреваемого. Главный повод для возбуждения уголовного дела с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, - это рапорт сотрудника следственного аппарата об обнаружении признаков, указывающих на совершения преступления

Для получения сведений об обстоятельствах расследуемого преступления, совершенного с использованием IT-технологий, субъект расследования при проведении следственных действий должен обладать навыками специалиста в сфере обмена цифровой информацией:

- исследовать хранящуюся в компьютерной цепи цифровую информацию;

- обнаруживать среди этой информации сведения, подтверждающие совершенное преступление (найти электронный след);

- фиксировать результаты поисковой деятельности в процессуальных документах.

6. Определяющим эффективность производства по уголовному делу фактором являются глубокие познания субъекта расследования (следователя, дознавателя) в различных видах и сочетаниях компьютерных сетей, компьютерных устройств, компьютерных технологий. При выполнении действий по обнаружению и изъятию доказательственной информации в ряде случаев используют помощь специалиста уже на подготовительном этапе.

7. При возбуждении уголовного дела по преступлениям, совершенным с использованием IT-технологий, может возникнуть следующий наиболее существенный комплекс проблем:

- отсутствие возможности подать анонимное заявление о совершении преступления, например, незаконного борота оружия в сети Интернет, что сужает круг информаторов о данном виде преступления. В свою очередь, это приводит к тому, что по ряду фактов незаконного оборота оружия возбуждение уголовного дела не происходит вовсе, т. к. гражданские лица, которым стало известно о преступлении такого рода, не желают сообщать о данных фактах от

своего имени;

- затруднения, связанные с запретом на получение материалов, необходимых для возбуждения уголовного дела на стадии возбуждения уголовного дела (ряд действий допускается лишь на стадии предварительного расследования);

- отсутствие на стадии возбуждения уголовного дела конкретного подозреваемого, что приводит к увеличению объема и сроков расследования уголовного дела.

- несовпадение места преступления, совершенного с использованием сети Интернет, с местом его расследования.

Важной проблемой эффективного расследования преступлений в сфере IT-технологий является острая нехватка квалифицированных специалистов соответствующей компетенции.

8 Необходимо отметить, что методика расследования преступлений, совершенных с использованием IT-технологий, имеет ряд существенных отличий от расследования иных преступлений. Некоторые методы и средства являются общими, в том числе и для данного вида преступлений. Значительную роль в расследовании таких преступлений играет программное обеспечение, которое должно быть развито на соответствующем современному миру уровне. Следует постоянно обновлять информационную базу касательно различных приемов и ухищрений, используемых преступниками в таких преступлениях. Особое значение для расследования оказывают специалисты в отдельных областях знаний, осуществляющие содействие следствию, как на этапе предварительного расследования, так и на этапе до возбуждения уголовного дела, при проведении проверки сообщения о преступлении.

9. Организационное обеспечение состоит в том, что для успешного раскрытия и расследования таких дел нередко требуется применение всего арсенала имеющихся в настоящее время технических средств. Технико-криминалистическое обеспечение, по нашему мнению, должно строиться с учетом общепринятого в настоящее время в криминалистической науке

ситуационного подхода. Практическое значение имеет выделение ситуаций, складывающихся на этапе проверки сообщений о преступлении в сфере IT-технологий до возбуждения уголовного дела, также в ходе предварительного и судебного следствия и выработка практических рекомендаций по наиболее оптимальному применению соответствующих технических средств для соответствующей складывающейся ситуации. Целесообразным является разработка рекомендаций по применению технических средств применительно к отдельным следственным действиям.

10. Деятельность по оценке следственной ситуации и выдвижению версий должна осуществляться следователем параллельно. Должно выдвигаться максимальное количество всевозможных версий на основании собранной информации по уголовному делу, в том числе и контрверсии, а также версии защиты. Контрверсия – разновидность криминалистической версии, которая выдвигается с помощью логической операции отрицания основной версии и выполняет важную функцию предупреждения односторонности и необъективности расследования. Проверка каждой из выдвинутых версий должна осуществляться оперативно, эффективно и в соответствии с криминалистическими рекомендациями. В процессе проверки выдвинутых версий и по мере поступления новой информации о совершенном преступлении должны быть выдвинуты и подлежат проверке иные версии.

11. Несмотря на имеющийся в теории и практике пошаговый механизм выполнения определенного алгоритма действий, каждое уголовное дело уникально, а потому четкого плана действий предусмотреть невозможно. Определенные временные рамки на расследование уголовного дела диктуют максимально рациональное использование всего комплекса следственных мероприятий для обеспечения полноты, всесторонности и объективности расследования. Правила оценки доказательств фактически основаны на этической составляющей субъективного познания, поскольку базируются на принципах внутреннего убеждения, всесторонности, полноты, объективности и непосредственности исследования. Именно поэтому четкость действий,

правильно и грамотно спланированный график выполнения всех следственных действий является залогом не только эффективного рабочего графика следователя, но и общей организации его работы. Завершающим обстоятельством является подтверждение выводов заключения эксперта другими фактическими данными и доказательствами, уже установленными к этому моменту по делу, т.е. устанавливается относимость экспертного заключения.

Обращаясь к практическому аспекту расследования преступлений в рассматриваемой нами сфере, необходимо отметить, что от верного выбора четкой последовательности следственных и иных процессуальных действий, их квалифицированного и своевременного выполнения во многом зависит быстрота и успех предварительного расследования, а также всего производства по уголовному делу. Роль алгоритмизации в рассматриваемом аспекте является неоспоримой, так как позволяет обеспечить системный подход в достижении задач первоначального этапа расследования преступлений посредством оперирования тактическими приемами, тактическими комбинациями и тактическими операциями. Для правильной квалификации преступного деяния в сфере IT-технологий, следователям следует повышать свою квалификацию, обладать специальными познаниями в области информационно-электронных технологий.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 20 дек. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Собр. законодательства Рос. Федерации. 2002. № 1 (ч. 1), ст. 1.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. 1996. № 25, ст. 2954.

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 дек. 2001 г. // Собр. законодательства Рос. Федерации. 2001. № 52 (ч. 1), ст. 4921.

5. О полиции: Федеральный закон Рос. Федерации от 07.02.2011 № 3-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 28 янв. 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 2 фев. 2011 г. // Собр. законодательства Рос. Федерации. 2011. № 7, ст. 900.

6. О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»: федеральный закон от 27 декабря 2019 г. № 476-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31 июля 2020 г. № 259-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 1 2.04.2023 г.).

8. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств: федеральный закон от 27 июня 2018 г. № 167-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

9. О едином учете преступлений: приказ Генеральной прокуратуры РФ № 39 от 29 декабря 2005 г. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

10. Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации: приказ Следственного комитета России от 11.10.2012 № 72 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

11. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 3 апреля 2018 г. № 196 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

12. О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф»: приказ МВД России от 22.04.2020 № 236 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

13. Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф»: приказ МВД России от 29.12.2020 № 925 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

II. Учебная, научная литература и иные материалы

1. Александров А.С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 130-139.

2. Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199-207.

3. Аликина Л.А. Актуальные проблемы стадии возбуждения уголовного дела / В сб.: Пермский период. Пермь, 2022. С. 10-12.

4. Антонова Е.Ю. Новые формы преступной деятельности в условиях цифровизации // Ученые записки юридического факультета. 2022. № 1. С. 18-23.

5. Ахметзянов А.Ф, Система и содержание поводов для возбуждения уголовного дела // Молодой ученый. 2022. № 16. С. 159-161.

6. Бердникова О.П. Порядок получения электронных доказательств при проведении отдельных следственных действий // Право и государство: теория и практика. 2022. № 1. С. 366-368.

7. Болтенкова Ю.В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации / В сб.: Поколение будущего: взгляд молодых учены. Курск, 2022. С. 170-174.

8. Будников А.П. Актуальные вопросы возбуждения уголовного дела // Вестник магистратуры. 2022. № 1. С. 39-40.

9. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-25.

10. Калашников А.А. Процессуальные акты стадии возбуждения уголовного дела // Общество. 2022. № 4. С. 102-104.

11. Климова М.И. Особенности раскрытия и расследования оперативно-

розыскными средствами и методами преступлений, предусмотренных статьей 138 УК РФ, совершенных с использованием информационно-телекоммуникационных технологий / В сб.: Актуальные вопросы теории и практики в деятельности подразделений полиции. М., 2022. С. 30-33.

12. Кравцов Д.А. Некоторые аспекты предупреждения киберпреступности // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22). С. 57-60.

13. Мухина Ю.Р., Бельский А.И. Проблемы уголовно-правовой квалификации преступлений, совершенных с использованием IT-технологий / В сб.: Современность в творчестве начинающего исследователя. Иркутск, 2022. С. 168-170.

14. Разувакина И.И., Разувакин А.А. Особенности организации и проведения проверки заявлений и сообщений о преступлениях в сфере компьютерной информации // Право и управление. 2022. № 9. С. 156-159.

15. Соркин В.С, Козел В.М. Об электронных доказательствах в уголовном процессе (проблемы правоприменения) // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2021. Т. 11. № 2. С. 79-84.

16. Состояние преступности в Российской Федерации в 2021-2022 годах. Официальный сайт МВД РФ: Режим доступа: https://мвд.рф/reports/item/35396677 (Дата обращения: 12.04.2023 г.).

17. Ушекин С.Н. Некоторые проблемные вопросы в борьбе с преступлениями в сфере IT-технологий // Право: ретроспектива и перспектива. 2022. № 2. С. 89-94.

18. Цейтлин Н.Ф, Преступления, связанные с использованием IT-технологий: проблемы выявления и расследования / В сб.: Актуальные вопросы охраны общественного порядка и административной деятельности. М., 2022. С. 189-192.

19. Шигуров А.В., Шигурова Е.И. Проблемы правовой регламентации использования электронных следов и электронных носителей информации при

производстве по уголовному делу // Гуманитарные и политико-правовые исследования. 2020. № 1. С. 53-63.

III. Материалы судебной практики

1. Обзор практики раскрытия и расследования уголовных дел о хищениях, совершенных с использованием информационно-телекоммуникационных технологий в Нижегородской области за 2020 год: [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

2. Постановление Суда по интеллектуальным правам от 20.06.2019 № С01 -390/2019 по делу № А40-169068/2018: [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

3. Постановление Арбитражного суда Московского округа от 29.11.2019 № Ф05-18806/2019 по делу № А40-217942/2018: [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

4. Приговор по делу № 1-613/2017 Октябрьского районного суда г. Ростов-на-Дону от 1 декабря 2017 года [Электронный ресурс]: Режим доступа: https://sud-praktika.ru/precedent/467627.html (Дата обращения: 12.04.2023 г.).

5. Приговор по делу № 1-256/2017 от 17 ноября 2017 года Устиновского районного суда г. Ижевска Удмуртской Республики [Электронный ресурс]: Режим доступа: https://sud-praktika.ru/precedent/546816.html (Дата обращения: 12.04.2023 г.).

6. Приговор Люблинского районного суда г. Москвы от 11 апреля 2016 по ст. 234 УК РФ № 01 - 00090 / 2016. Доступ из справ.-правовой системы «КонсультантПлюс» (Дата обращения: 12.04.2023 г.).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну Облицов П.А.

ПРИЛОЖЕНИЕ

12301530055000000

ПОСТАНОВЛЕНИЕ
о возбуждении уголовного дела и принятии его к производству

г. Оренбург «20» января 20 23 г.
(место составления)

14 час 05 мин

Следователь 6отдела (по расследованию преступлений на территории Оренбургского
(должность следователя (дознавателя),
района г. Оренбурга ,
классный чин или звание, фамилия, инициалы)
рассмотрев сообщение о преступлении хищение имущества Фамилия И.О.
(каком)
поступившее в ОП №6 МУ МВД России «Оренбургское» (КУСП №333555 от 20.01.2023 г.)
(когда, куда, от кого)
и материалы проверки, по данному сообщению,

У С Т А Н О В И Л :

20.01.2023 года в 17 часов 18 минут неустановленное лицо, находясь в неустановленном месте, неустановленным путем, незаконно, умышленно, из корыстных побуждений с целью хищения чужого имущества, получило доступ к банковскому счету № 0000 1111 2222 3333 4444 банка ПАО «Сбербанк», откуда тайно похитило 5 700 рублей, принадлежащие Фамилия И.О., причинив тем самым последней ущерб на указанную сумму.

Принимая во внимание, что имеются достаточные данные, указывающие на признаки преступления, предусмотренного
п. «г» ч. 3 ст. 158 УК РФ
руководствуясь ст. 140, 145, 146 (147) и частью первой ст. 156 УПК РФ,

П О С Т А Н О В И Л :

1. Возбудить уголовное дело в отношении неустановленного лица по факту преступления, предусмотренного
п. «г» ч. 3 ст. 158 УК РФ
(пункт, часть, статья УК РФ)

2. Уголовное дело принять к своему производству и приступить к расследованию.

3. Копию настоящего постановления направить прокурору Оренбургского района
(наименование
г. Оренбурга
органа прокуратуры)

Следователь _____
(подпись)

Копия настоящего постановления направлена прокурору Оренбургского района
(наименование
г. Оренбурга «20» января 2023 г. в 14 ч. 10 мин.

О принятом решении сообщено заявителю гр-ке. Фамилия И.О.

Следователь _____
(подпись)