Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра оперативно-розыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «Организационные основы оперативно-розыскной деятельности по раскрытию преступлений, совершаемых с использованием высоких технологий»

Выполнил: Скрябин Никита Алексеевич
специальность 40.05.02
Правоохранительная деятельность, 2015 года набора, 051 уч. гр.,
младший лейтенант полиции

Руководитель:
кандидат юридических наук, доцент,
доцент кафедры оперативно-розыскной деятельности,
полковник полиции
Усманов ИльгизМиншакирович

Рецензент:
Начальник ОП № 6 «Савиново»
УМВД России по г. Казани,
подполковник полиции
Каримов Айрат Геннадьевич

Дата защиты: «___» _____2020 г. Оценка_____

Казань 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена практической и теоретической значимостью вопросов, связанных со становлением и развитием механизмов обеспечения информационной безопасности в России. Открытия в различных областях науки, развитие информационно-коммуникационных технологий, технологическое перевооружение промышленности привели к кардинальным переменам во всем мире, обусловили переход к новому типу общества – информационному. Основное содержание преобразований, происходящих и в настоящее время, обусловлено процессами создания, обработки, хранения и использования информации в различных сферах деятельности человека.

Компьютеризация ознаменовала современную эпоху научно-технического прогресса. Но, наряду, с бесспорными положительными сторонами компьютеризации, она имеет и негативные стороны, в частности, появление нового вида противоправных деяний, таких как преступления в сфере компьютерной информации. По своему механизму, способам совершения и сокрытия следов, эти преступления имеют свои особенности и характеризуются большой латентностью и низкой раскрываемостью.

Несмотря на многочисленные исследования, проведенные в данной области, многие вопросы на сегодняшний день остаются спорными, либо вовсе нерешенными. Кроме этого, вслед за постоянным внедрением новых технологии идет изменение способов и механизмов совершения преступлений в сфере компьютерной информации. Внедряются новые методы маскировки как самих противоправных деяний, так и следов, указывающих на лиц, их подготовивших и совершивших. Данные обстоятельства требуют постоянного научного внимания к проблеме

выявления и расследования преступлений в сфере компьютерной информации, а также глубоких знаний в области информационных технологий у лиц, связанных с этой деятельностью.

Недостаточная изученность криминологической характеристикb неправомерного доступа к компьютерной информации, необходимость совершенствования уголовного законодательства, комплексный анализ правовых и организационно-технических мер предупреждения и противодействия рассматриваемому виду противоправных деяний, предопределили выбор темы дипломной работы.

Объектом исследования данной работы являются общественные отношения, в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Предмет исследования включает в себя: преступность в сфере компьютерной информации, как объект уголовно-правового регулирования, ее состояние, структуру и динамику; методы, особенности расследования преступлений в сфере компьютерной информации; совокупность мер по предупреждению компьютерных преступлений.

Цель работы заключается в комплексном уголовно-правовом и криминологическом научном исследовании состояния, тенденций, характерных черт преступлений в сфере компьютерной информации в Российской Федерации.

Задачи исследования:

- проанализировать нормы права, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации;
- исследовать проблемы квалификации преступления, проблемы привлечения к уголовной ответственности;
- раскрыть основные причины и условия, способствующие совершению преступления в сфере компьютерной информации;
- изучить особенности и проблемы в раскрытии и расследовании преступлений в сфере компьютерной информации;

Методологической основой исследования послужили: общенаучные методы познания; частно-научные методы; историко-правовой - применительно к изучению истории компьютерных преступлений, уголовной ответственности за их совершение; формально-логический, заключающийся в детальном анализе уголовно- правовых и организационно-технических мер противостояния неправомерному доступу к компьютерной информации; статистический, включающий сбор и анализ статистических данных о неправомерном доступе к компьютерной информации.

Структура работы включает в себя введение, 2 главы, заключение, список использованной литературы и приложения.

ГЛАВА 1 ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

§1.История возникновения и развития преступлений в сфере высоких технологий.

Уже с начала становления общества людей, мы испытываем потребность общения друг с другом. Сначала это были простые мимика, жесты и знаки. Далее появились более сложные средства передачи информации: речь, письменность, книги. Общество шло по пути развития и средства общения тоже развивались, появились: телеграф, телефон, радио, компьютеры и телекоммуникационная сеть «Интернет».

Интернет создает для нас большую площадку для общения, обмена жизненно важной информацией, управление различными органами и службами. Автоматизация различных производственных процессов и повышение производительности труда – все это благодаря внедрению компьютеров в нашу жизнь.

Персональный компьютер потерял свою актуальность, в XXI веке,с появлением смартфонов и планшетов, из-за своих больших габаритов. Из дорогостоящего и громоздкого стационарного устройства превратился в доступный всем «гаджет», умещающийся в кармане и имеющий обширный функционал.

Вместе с положительными аспектами открылись и отрицательные, а именно развитие совершенно нового вида преступлений – компьютерных.

Одно из первых компьютерных преступлений было совершено в США в конце семидесятых годов прошлого столетия. Консультант по компьютерной безопасности SecurityPacificNationalBank Стэнли Рифкин расшифровал код, управляющий системой банка в Лос-Анджелесе, и дал

команду ЭВМ на перевод 10 млн. долларов на его текущий счет. По другой версии первое компьютерное преступление в 1969 г. совершил Альфонсе Конфессоре (США). Незаконно получив доступ к информации в электронно-вычислительной сети, он совершил налоговое преступление, ущерб от которого составил 620 тыс. долларов США.

В нашей стране первое преступление, связанное с несанкционированным доступом к компьютерной информации, было зарегистрировано в 1979 году на территории бывшего СССР (в Вильнюсе). Ущерб государству на тот момент составил 78 584 рубля. Используя недостатки программного обеспечения автоматизированного комплекса «Онега», женщина в течение двух лет совершала хищения денежных средств, направляемых гражданам в качестве пенсий и пособий по старости.

В 1983 году в Париже группой экспертов Организации экономического сотрудничества и развития (ОЭСР) было дано криминологическое определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных.

Чем дальше развивались технологии, тем более сложными и изощренными становились компьютерные преступления.

2 ноября 1988 года зафиксирован первый случай появления и «победоносного» шествия сетевого червя, парализовавшего работу шести тысяч интернет-узлов в США. Позднее в СМИ этот червь был наречён червём Морриса по имени его автора (аспиранта факультета вычислительной техники Корнеллского университета Роберта Т. Морриса). Хакеры же прозвали его «великим червём».Это был первый вирус, получивший значительное внимание в средствах массовой информации. Он также привёл к первой судимости в США по ComputerFraudandAbuseAct 1986 год

Первые преступления с использованием компьютерной техники в России появились в 1991 г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. Весь мир облетело уголовное дело по обвинению Левина и других соучастниках, совершивших хищение денег с банковских счетов на большом расстоянии с использованием ЭВМ.

С появлением новой угрозы, на законодательном уровне неоднократно предпринимались попытки регламентации ответственности за совершение компьютерных преступлений. Так, 06 декабря 1991 года был представлен проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предусматривал введение в действующий Уголовный кодекс РСФСР норм, устанавливающих ответственность за совершение компьютерных преступлений. Постановлением Верховного Совета РФ от23.09.92 № 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» предполагалось внесение изменений и дополнений в Гражданский, Уголовный кодекс РСФСР и другие законодательные акты, связанные с вопросами правовой охраны программ для электронных вычислительных машин и баз данных. В 1994 году был разработан проект закона о внесении дополнений в УК РСФСР, которым устанавливалась ответственность за ряд противоправных действий в сфере компьютерной информации. В 1995 году был опубликован проект Уголовного кодекса Российской Федерации, в котором предусматривалась Глава 29«Компьютерные Преступления», включавшая в себя следующие составы: самовольное проникновение в автоматизированную компьютерную систему (ст. 271); неправомерное завладение программами для ЭВМ, файлами или базами данных (ст. 272); самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273); внесение или распространение вирусных программ для ЭВМ (ст. 274); нарушение правил, обеспечивающих

безопасность информационной системы (ст. 275)[1].

Дальнейшее развитие информационных технологий, появление и активное внедрение сети Интернет, массовая компьютеризация привели к бурному развитию компьютерной преступности, как на уровне отдельных государств, в том числе, России, так и на международномуровне[2].

Разработка таких механизмов невозможна без изучения зарубежного опыта борьбы с киберпреступностью, поэтому рассмотрим опыт законодательной регламентации уголовной ответственности за подобные деяния на примере США, Германии иФранции.

Так как первые преступления совершенные с использованием ПК были совершенны в Америке, именно в США была установлена уголовная ответственность за совершение таких преступлений.

Так, в 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за такие деяния, как введение заведомо ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации. На основе данного законопроекта в октябре 1984 г. был принят «Закон о мошенничестве и злоупотреблении с использованием компьютеров» основной нормативно–правовой акт,устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) изменялся и дополнялся, а в

[1] Уголовный кодекс РСФСР (утв. ВС РСФСР 27.10.1960; ред. от 30.07.1996) // Ведомости ВС РСФСР. 1960. № 40. Ст. 591 (утратил силу).
[2] Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. Сычев.Изд. центр ЕАОИ, 2017. С. 300.

настоящее время он включен в виде §1030 в Титул 18 Свода законов США.

В Германии уголовная ответственность за компьютерные преступления была установлена в 1986 году, когда были внесены соответствующие изменения в УК ФРГ. К преступлениям в сфере компьютерной информации согласно УК Германии,отнесены:

- действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a);

- умышленные деяния лиц с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных или данных, неправомочного использования данных или иного воздействия на результат обработки данных (§263a);

- подделка или использование поддельных технических записей, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§268);

- аналогичная подделка данных, имеющих доказательственное значение (§ 269);

- уничтожение, изменение или утаивание технических записей (§274);

- противоправное аннулирование, уничтожение, приведение в негодность или изменение данных (§303a);

- нарушение обработки данных путем разрушения, повреждения, приведения в негодность либо приведения в негодность установки для обработки данных или носителей информации (§303b).

Уголовный кодекс Франции 1994 г., также предусматривает уголовную ответственность за ряд компьютерных преступлений. В сфере компьютерной информации УК Франции устанавливает ответственность

за совершение следующих преступлений:

- перехват, хищение, использование или предание огласке сообщений, передаваемых средствами дальней связи (ст.226-15);

- незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст.323-1);

- воспрепятствование работе или нарушение работы компьютерной системы (ст.323-2);

- ввод обманным путем в систему информации, а также изменение или уничтожение, содержащихся в автоматизированной системе данных (ст.323-3);

- ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19).

К преступлениям в информационном компьютерном пространстве, в соответствии с УК Франции, могут быть также отнесены:

- осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст.226-16);

- осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст.226-17);

- сбор и обработка данных незаконным способом (ст.226-18);

- хранение определенных данных сверх установленного законом срока (ст.226-20);

- идругие.

За рассматриваемые выше деяния УК Франции предусматривает уголовную ответственность, как для физических, так и для юридических лиц.

Не может обратить на себя внимание тот факт, что законодатели США, ГДР и, особенно, Франции изложили более четкие диспозиции и

квалификацию компьютерных преступлений, что, несомненно, благоприятно отразилось на эффективности их выявления и расследования.

Безусловно, на момент принятия Уголовного кодекса 1997 года Россия существенно отставала от стран Европы по количеству средств вычислительной техники, используемых как организациями различных форм собственности, так и непосредственно гражданами. Но, по моему мнению, ограниченная трактовка противоправных деяний, изложенных в Главе 28 УК РФ, зачастую не способствует их исчерпывающей и правильной квалификации.

С развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называли веком энергетики, то XXI - веком информатики.

Высказывание Натана Ротшильда: «Кто владеет информацией, тот владеет миром» в наши дни приобретает все большуюактуальность.

Информация обрела реальную цену и с развитием информационных технологий становится всеболее ценным товаром. Это подтверждает и возникновение виртуальных средств платежей, так называемых «криптовалют», которых по данным различных Интернетресурсов в мире насчитывается от 1,5 до 1,8 тысяч наименований! И все они имеют свою котировку по отношению к мировым валютам.

Но, новые технологии стимулируют развитие и новых форм преступности. В последние годы отмечается тенденция стремительного роста компьютерных преступлений, совершенных посредством глобальной сети передачи данных «Интернет». Кроме этого, акцент смещается в сторону атак на различные мобильные устройства, так как они получили колоссальное распространение среди жителей планеты, а большая часть их пользователей в силу разных причин пренебрегает элементарными мерами безопасности. Сети же крупных организаций имеют, как правило, несколько степеней защиты, обеспечиваемых как

аппаратными устройствами, так и специализированными программнымипродуктами.

На основании изложенного, можно сделать вывод о том, что компьютерная преступность является одной из самых специфических, сложно устроенных и динамично развивающихся видов преступности. Она является серьезной угрозой, как для отдельных государств, так и для всего мирового сообщества. Ущерб от действий киберпреступников огромен и исчисляется миллиардами долларов. Для эффективной борьбы с данным явлением необходимо совершенствование законодательства, регламентирующего уголовную ответственность за совершение компьютерных преступлений, в том числе и с использованием положительного опыта зарубежных стран.

§2. Криминалистическая характеристика преступлений.

Под криминалистической характеристикой компьютерных преступлений понимается наиболее характерная и значимая информация о конкретном виде преступлений, состоящая из признаков и свойств. Позволяющая говорить о событии преступления, личности преступника, оценке сложившийся ситуации, а также направлениях расследования преступления.[1]

Ключевым из них можно назвать способы совершения мошенничества

[1] Климов Д. В. Расследование хищений, связанных с использованием сети «Интернет»: учеб. пособие / Д. В. Климов. – Н. Новгород.: Нижегородская академия МВД России, 2017. – 24 с.

в сфере компьютерной информации. А.А. Комаров отмечает: «Определяющим признаком любой формы мошенничества является способ совершения преступления: обман или злоупотребление доверием, являющиеся единственным, исключительным способом совершения данного вида преступлений».[1]

Рассматриваемые преступления имеют полноструктурное строение, то есть состоит из подготовки к преступлению, реализации самой преступной деятельности и принятие мер к сокрытию следов преступления.[2]

Специфика рассматриваемых преступлений заключается в том, что еще на этапе уже на этапе преступник предпринимает меры к сокрытию следов будущего преступления. Это можно увидеть, например в покупке сим-карт зарегистрированных на других лиц, покупка номеров в интернете на время, установление программного обеспечения на мобильный телефон позволяющего скрывать номер абонента и др.

Так же, в зависимости от способа, преступник может разработать специальныйсайт, на которых потенциальная жертва ознакамливается с информацией и переходит по вредоносной ссылке. После чего производится рассылка спама либо заманивание жертвы в обманные схемы. Часто такие сайты создаются очень похожими на официальные сайты органов или организаций и неотличимы для впервые зашедшего на такой сайт пользователя.

По той же схеме, в зависимости от способы совершения мошенничества подбираются средства и орудия (специальные технические средства, сеть, условия и функции провайдера), а также лица, которые играют заранее распределенные роли. Чаще всего это специально подготовленные люди, хорошо знакомые с психологией людей, умеющие

---

[1] Комарова А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. М.: Юрлитинформ, 2013. С. 9.

[2] Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2015. № 11. С. 45-47.

убеждать и внушать необходимые злоумышленникам действия.

Анализ следственно-судебной практики, а также научной и нормативно-правовой литературы, позволяет констатировать, что единого подхода к классификации способов совершения мошенничества в сфере компьютерной информации не сегодняшний день нет.

Обусловлено это тем, что в случае использования того или иного способа деяние может быть квалифицировано по другой, нежели мошенничество, статье Уголовного кодекса или их совокупности. Так, например, М.И. Третьяк отмечает, что компьютерное мошенничество является специальным составом к компьютерным преступлениям (ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ), и рассмотренные в законе, теории и практике определения модификации компьютерной информации следует использовать и при характеристике компьютерного мошенничества, однако с учетом того, что в диспозиции ст. 159.6 УК РФ, в отличие от статей гл. 28 УК РФ, термины «удаление (уничтожение)», «блокирование» и «модификация» характеризуют способ компьютерного мошенничества.[1]

Именно такой позиции придерживается Верховный Суд, который в п.12 Постановления Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» определил, что в случаях,когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статьей 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или

[1] Третьяк М.И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. – 2016. – № 2. С. 95- 101; Третьяк М.И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий // Законность. – 2016. – № 7. С. 41-46.

273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.[1]

Именно такой подход положен в основу классификации основных способов совершения компьютерного мошенничества в Конвенции ООН «О преступности в сфере компьютерной информации»[2] , в ст. 8 которой определено, что для того чтобы квалифицировать в качестве уголовных преступлений, согласно ее внутригосударственному праву, в случае совершения преднамеренно и без права на это лишения другого лица его собственности путем: a) любого ввода, изменения, удаления или блокирования компьютерных данных; b) любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

Уже ранее совершались попытки классификации способов совершения компьютерных преступлений.«Так, например, кодификатор рабочей группы Интерпола в обобщенном виде компьютерные мошенничества предлагает определять и классифицировать следующим образом:

- компьютерные мошенничества, связанные с хищением наличных денег из банкоматов;
- компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств;
- мошенничества и хищения, связанные с игровыми автоматами;
- манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из

[1] Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате». «Бюллетень Верховного Суда РФ», № 2, февраль, 2008 (в ред. Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». «Собрание законодательства РФ», 03.12.2012, № 49, ст. 6752).

[2]"Конвенция о преступности в сфере компьютерной информации" (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003)

них путем манипуляции программами;

- компьютерные мошенничества и хищения, связанные с платежными средствами;
- телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.»[1]

С каждым днем появляются все новые и новые виды мошенничества, это делает их классификацию затруднительной. Поэтому в отношении наиболее распространенных в Интернете мошеннических схем можно говорить лишь о типологии. Согласно основным направлениям мошеннической деятельности А.А. Комарова выделяет следующие их типы:

- Виртуальный товарообмен.
- Легкие деньги.
- Лжеблаготворительность.
- Мошенничество в сфере интернет-знакомств.
- Телеработа, удаленный заработок.
- Мошенничество в сфере услуг.
- Инвестиционное мошенничество.
- Компьютерное мошенничество. [2]

В первую очередь, классифицировать мошенничество в сфере высоких технологий следует на основании способов, которым оно совершается.

Анализ следственной и судебной практики, а также репрезентативный опрос пользователей ПК и сотрудников правоохранительных органов говорит том, чтосегодня наиболее распространёнными преступлениями в сфере высоких технологий являются:

– незаконное завладение регистрационными данными различных учетных

[1] См.: Вопросы международного сотрудничества в борьбе с компьютерными преступлениями [Электронный ресурс]. URL: .crime-research.ru/news/ (дата обращения: 17.04.2020).

[2] Комаров А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. – М.: Юрлитинформ, 2013. С. 31-32.

записей (Appstore, googlemarket и т. п.) с последующей их реализацией либо дальнейшим использованием в мошеннических схемах;

– использование платежных сервисов различных Интернет-ресурсов (как в российском сегменте сети интернет, так и за его пределами) при осуществлении необходимых платежных операций с последующим обналичиванием денежных средств, либо с приобретением различных товаров с использованием денежных средств со счета жертвы (для совершения транзакции мошенники располагают необходимыми данными карты жертвы);

– размещение ложной информации с целью ввести в заблуждение потенциальную жертву (будущего инвестора) на специально созданном сайте (в том числе размещение сообщений на форумах) о возможности получения сверхкрупных прибылей от краткосрочных инвестиций с последующим заключением виртуальных сделок и переводом денежных средств на счет в банке за границей;

–взлом электронных кошельков (в том числе посредством рассылки вредоносного программного обеспечения либо ссылок на него) с последующим хищением денежных средств (их обналичиванием), переводом на другие счета, оплата услуг либо товаров, через электронные платежные системы («YandexMoney», «Webmoney», «PayPal», «Qiwi» и др.);

– рассылка писем-оферт об инвестировании бизнеса посредством пополнения счетов денежными средствами. В случае акцепта следует просьба предоставить персональные данные (для юридического лица банковские реквизиты, образцы подписей, оттиски печати). Возможны также просьбы о погашении «операционных расходов» за перевод средств;

– рассылка спам-писем на электронную почту, которые содержат вредоносные программы. Рекламные объявления могут содержать предложения разного характера (о переводе различных сумм денежных

средств лицам, указанным в списке, с последующей заменой на любого из списка на себя и дальнейшей рассылкой знакомым по электронной почте; о приобретении медикаментов и БАДов и способах различных диет; бесплатного приобретения товаров и услуг; быстрого обогащения; выгодного инвестирования; целевого кредитования на выгодных условиях; о надомной работе при покупке оборудования, комплектующих и прочих принадлежностей за счет жертвы и т.д.) ;[1]

– получение денег через виртуальные Интернет-магазины, а также создание мошенниками сайтов-двойников известных интернет-магазинов;

– проведение электронных торгов (выставляются несуществующие лоты) или «интернет-аукционы» (с целью завышения цены аукционного товара продавцы-мошенники делают на него ставки);

– организация благотворительных акций через Интернет, где предлагается на счета для конкретных лиц (инвалидов, нуждающихся в срочных операциях и т. п.) перечислять денежные суммы. С этой целью также могут создаваться сайты-клоны реальных благотворительных организаций;

– хищение посредством вредоносного программного обеспечения либо сайтов-двойников номеров пластиковых платежных карт жертв.

Следующим элементом криминалистической характеристики являются следы преступной деятельности. При расследовании любого преступления, основной целью является собирание более полной и подробной информации о событии.Однако в рассматриваемом виде преступлений, информация представляет собой специфическую категорию.

Особенности определения относимости компьютерной информации к доказательствам заключается в том, что это возможно только при воспроизведении информации с помощью технических средств, а так же анализесодержания информации и ее свойств. Оценка относимости

[1] Шурухнов В.А. Свойства компьютерной информации и их учет в расследовании преступлений // Актуальные вопросы применения уголовно- процессуального и уголовного законодательства в процессе расследования преступлений (к 90-летию со дня рождения профессора И.М. Гуткина): Сб. матер. межвуз. научн.-прак. конф.: В 2-х ч. М.: Академия управления МВД России, 2009. С. 84-88.

предполагает не только вывод о том, что компьютерная информации по тем или иным признакам соотносится с предметом доказывания, но и раскрытие того, как именно она связана, какие обстоятельства устанавливает, какой версии соответствует и какой противоречит.[1]

Участники судопроизводства имеют дело с объектами, являющимися либо носителями следов, либо средствами получения значимой для дела информации. Некоторые ученые такого рода следы именуют знаковыми[2]. Понятие «знак» в науке и практике применяется для указания на материальный объект, для получателя информации, являющейся условным обозначением какого-либо предмета, процесса или явления.

Знаковые системы состоят из однообразно интерпретируемых сигналов, которыми можно обмениваться как по естественным, так и по техническим каналам связи. Примерами могут служитьконтакт глазами при личном общении и использование языка программирования для передачи сообщений по электронной почте.

Со знаковыми следами криминалисты чаще всего сталкиваются при изучении устной и письменной речи, любого рода звуков, а также компьютерной информации.

Не вдаваясь в дискуссию, согласно примечанию к ч. 1 ст. 273 УК РФ, под компьютерной информацией следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Актуальность исследования и использования в доказывании по уголовным делам компьютерной информации поставила перед учеными-криминалистами вопрос о месте такого рода следов преступления в общей классификации. Изначально предпринимались попытки определить природу указанных следов с опорой на положения трасологии. Акцентируя внимание на

---

[1] Зигура Н.А., Кудрявцев А.В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М., 2011. С. 125.

[2] *КолдинА.В.,КрестовниковО.А.*Источникикриминалистическойинформации/подред. В. Я. Колдина. М. : Юрлитинформ, 2017. С.65—72.

методологической функции трасологии по отношению ко многим родам и видам судебных экспертиз, Н. П. Майлис полагает возможным рассматривать эти следы с позиций микро- трасологии в качестве «ультрамикрообъектов»[1].

Такой подход представляется некорректным. При цифровой записи:

1) вместо реального объекта с многообразием индивидуализирующих призна- ков фиксируется его абстрактная математическая модель, вид и параметры которой могут варьироваться;

2) на материальном носителе записывается последовательность чисел, харак- теризующая параметры математической модели;

3) для правильного воспроизведения и восприятия зафиксированной таким образом информации необходимо обеспечить точное соответствие абстрактных моделей, используемых при записи и воспроизведении[2].

Взаимодействующие в электронно-цифровой среде информационные объекты не имеют формы и могут состоять из нескольких частей, размещенных в разных точках пространства6. С учетом изложенного некоторые ученые называют такого рода следы «виртуальными», справедливо отмечая, что они (как и другие знаковые следы) занимают промежуточную позицию между материальными и идеальными следами.

Таким образом, типичными следами по делам о мошенничестве в сфере компьютерной информации, являются:

– традиционные следы: следы человека в местах нахождения конкретного лица в момент совершения преступления (следы пальцев рук на клавиатуре и других компьютерно-технических средствах, внешний облик при встрече с жертвой преступления или при совершении преступниками подготовительных действий, например,

---

[1] Майлис Н. П.Нетрадиционные виды следов, используемые в раскрытии и расследовании преступлений // Эксперт-криминалист. 2018. № 3. С. 36.

[2] Мещеряков В. А.Цифровые (виртуальные) следы в криминалистике и уголовном про- цессе // Воронежские криминалистические чтения : сб. науч. трудов. Вып. 9. Воронеж : Изд-во Воронеж. гос. ун-та, 2008. С. 221—232.

при заключении договора об услугах провайдера и т.п.); используемых транспортных средствах, средствах связи и т.п.

- компьютерные следы, которые при любых действиях с компьютерными или иными программируемыми устройствами (мобильными телефонами, смартфонами, планшетами и т.д.) получают свое отображение в электронной памяти:

1) в журналах администрирования, журналах безопасности отображаются такие действия, как включение, выключение, различные операции с содержимым памятикомпьютера;

2) в реестре компьютера (reg-файлах) отражаются действия с программами (установка, удаление, изменение ит.д.);

3) в log-файлах отображаются сведения о работе в сети Интернет, локальных и иныхсетях;

4) в свойствах файлов отображаются последние операции с ними (например, даты создания, последнихизменений).[1]

Так же необходимо сказать о том, что закономерности образования и специфика компьютерных следов тесно связана местом совершения такого рода преступления.

Под местом совершения преступления, традиционно в криминалистике, понимается определенная территория реализации преступного деяния. Одной из особенностей является то, что место совершения преступления оказывает влияние на весь процесс формирования следовой картины и, соответственно, является носителем и материальных, и идеальных следов, а значит, обладает существенной информативностью.

Изучая особенности работы сети персонального компьютера, можно утверждать, что: 1)местом совершения преступления в сфере высоких технологий является сама информационно-телекоммуникационная сеть,

[1] Протасевич А.А., ЗверянскаяЛ.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. – 2013. – №11. С.45-47.

через которую происходит основное управление (ввод, удаление, блокирование, модификация, загрузка, копирование, информации и другое не санкционируемое вмешательство с последующим управлением личными данными жертвы);2) местом совершения рассматриваемого мошенничества является месторасположение конкретного ПК, с которого производится неправомерный доступ.

Так же необходимо сказать еще одну особенность преступлений в сфере высоких технологий. Такое мошенничество может предусматривать наличие, как минимум, еще одного или нескольких устройств, которые будут участвовать в процессе обмена информацией для получения конфиденциальной информации лиц. Расстояние между такими устройствами может быть достаточно внушительным, что негативно сказывается на раскрытии и расследовании такого рода преступлений, особенно когда такие устройства разбросаны по всему миру.

Таким образом, в рассматриваемом преступном деянии местом совершения преступления является местонахождение лица управляющего компьютерно-техническим средством, с которого отправляются команды.

Указывая на трудности определения места происшествия, может быть несколько мест происшествия:

- рабочее место, рабочая станция – место обработки информации, ставшей предметом преступногопосягательства;
- место постоянного хранения или резервирования информации – сервер или стример;
- место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в другом месте, при этом место использования может совпадать с рабочим местом, но находиться вне организации (например, при стороннем взломе путем внешнего удаленного сетевого доступа);
- место подготовки преступления (разработки вирусов, программ

взлома, подбора паролей) или место непосредственного использования информации (копирование, распространение, искажение), полученной в результате неправомерного доступа к данным, содержащимся наПК.

«Преступное деяние, – отмечает в этой связи Н.А. Колоколов, – считается законченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом). Сам по себе факт ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей в зависимости от обстоятельств дела может содержать признаки приготовления к мошенничеству в сфере компьютерной информации или покушения на совершение такогопреступления.

Помимо вышесказанного, к местусовершения преступления относят пункт обналичивания денежных средств, добытых преступным путем. Исходя из выбранного злоумышленником приема и способа совершения мошенничества таковыми могут быть банкоматы, интернет-магазины, онлайн казино, букмекерские конторы, онлайн конвертеры валюты и т.д. Процесс «отмывания» денежных средств очень влияет на характер следообразования имеющий ключевое значение для разработки научных и практических рекомендаций по раскрытию и расследованию мошенничества в сфере компьютерной информации.

Специфика разработки криминалистической характеристики мошенничества в сфере высоких технологий обусловлены тем, что немаловажной является информация о местонахождении средства связи с глобальным миром, принадлежащего жертве и подвергшегося проникновению со стороны злоумышленника. Обусловлено это

особенностями самой преступной деятельности и характером функционирования системы, в которой она реализуется.

Компьютерные средства, как следообразующие объекты могут быть значимыми в двух аспектах: как носители данных об объективной стороне преступления, а также как носители информации о самом субъекте преступления. Особенность этого заключается в том, что компьютерные средства сами не всегда выступают следами преступной деятельности, так как не обладают характерными специфическими особенностями, но при этом они несут на себе следовую картину преступного деяния. Об этом говорит анализ материалов следственной и судебной практики, когда, например, при производстве следственных действий, из компьютера для удобства изымается только его «жесткий диск» – запоминающее устройство для хранения информации. Необходимо отметить следующее, что технические характеристики компьютерно-технических средств, их наличие или отсутствие, вообще должны свидетельствовать о возможности реализации преступного умысла (например, наличие или отсутствие подключения компьютера к телекоммуникационной сети).

В отечественном законодательстве, а также в литературе отсутствует единое определение компьютерно-технических средств. Необходимо отметить, большинство ученых солидарны во мнении друг с другом, что главными свойствами являются хранение и обработка информации, с последующей возможность обмена на расстоянии.

Так, например, В.А. Мещеряков относит к компьютерно-техническим средствам компьютер (ЭВМ), предлагая понимать под ним комплекс технических средств, включающий:

- процессор (или другое электронное устройство), выполняющий функции преобразования информации, представленной в машинном виде, и реализующий одно или несколько действий (программу) по обработке информации;

- устройство хранения управляющих программ и (или) данных, необходимых для реализации процессором его целевых функций;
- оборудование (приспособление), позволяющее каким-либо образом изменять или перезаписывать управляющие программы и (или) данные, необходимые для реализации процессором его целевых функций».

Однако выводя данное определение, автор смешивает это понятие с понятием ЭВМ, ставя между ними знак равенства, что не совсем верно.

По мнению П.В. Костина: «накопители на гибких и жестких магнитных дисках, флэш-карты различного типа, микросхемы памяти, оптические диски и другие объекты, предназначенные для хранения информации, записываемой и считываемой при помощи технических устройств, должны также рассматриваться в качестве машинного носителя криминалистически значимой компьютерной информации. Исходя из логики определения, машинный носитель информации – устройство, предназначенное для ее отображения и хранения, также относится к компьютерно-техническим средствам.»[1]

Вместе с тем следует заметить, что большинство ученых все же сходятся во мнении, что основной характерной особенностью компьютерно-технических средств, с проекцией на потребности расследования, является их свойство сохранять информацию. Именно в этом аспекте компьютерно-технические средства, выступая орудиями и средствами совершения компьютерных преступлений, в том числе мошенничества в сфере компьютерной информации, содержат наибольшее количество следов совершаемого или совершенного преступления.

Именно это обстоятельство позволяет говорить, что к источникам компьютерной информации относятся системы, компоненты которых обеспечивают размещение, доступность, а также целостность сведений,

[1] Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады ТУСУРа. – 2015. – №2 (32). С. 162-166.

составляющих информацию. Это:

- постоянное запоминающее устройство компьютера (ПЗУ) – его внутренняя память, включающая несколько микросхем, постоянно хранящих определенную информацию;
- оперативное запоминающее устройство (ОЗУ) – оперативная память,
- сверхоперативная память (кэш) – сверхбыстродействующие микросхемы памяти – кэш-память для повышения производительности компьютера (сейчас в характеристиках процессоров существует размер кэша нескольких уровней, все это хранится внутри кристалла процессора).

Таким образом, по определенным основаниям нельзя назвать компьютерной сетью систему, которая не включает в себя помимо рабочих станций (технически сложных устройств, например, компьютера, смартфона, компактного персонального компьютера (КПК), планшетного персонального компьютера и т.п.) посредством которого пользователь (абонент) получает доступ к ресурсам компьютерной сети) каких-либо промежуточных накопителей информации.

Следовательно, особенностью компьютерных сетей является то, что их существует несколько видов, в зависимости от территориальной распространенности и возможности изъятия следов делятся на:

- *локальные* компьютерные сети (ЛВС, LAN-LocalAreaNetwork) (создаются и используются юридическими лицами, как правило, в пределах своего размещения, либо физическими лицами в обособленной административно- территориальной единице);
- *региональные* компьютерные сети (РВС, MAN – MetropolitanAreaNetwork), связывающие абонентов района, города, области;
- *глобальные* компьютерные сети (ГВС, WAN – WideAreaNetwork), соединяющие абонентов, удаленных друг от друга на любое расстояние.

В процессе расследования исследуемых преступлений следует учитывать,

что подготовка, написание, тестирование специальных компьютерных программ для взлома, внедрение вредоносных «троянских» программ, программ-шпионов, поиск паролей или определение способов беспарольного входа будет оставлять информационные следы в памяти компьютера или иного технически сложного устройства, используемого мошенником. При этом примененные способы воздействия на компьютер «жертвы» будут аналогичным образом оставлять следы в памяти ее компьютера или смартфона

Криминалистическая характеристика мошенничества в сфере компьютерной информации представляет собой обобщенное описание системы криминалистически значимой информации о признаках и свойствах преступления, предусмотренного ст. 159. 6 УК РФ, состоящее из определенного множества элементов, таких как: непосредственный предмет преступного посягательства; способ совершения преступления, орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые в свою очередь,характеризуются корреляционной зависимостью между собой, и специфичностью проявлений во внешней среде (киберпространстве), что и отличает данный вид преступной деятельности от схожих видов преступлений, и позволяет служить основанием для выдвижения типичных версий о событии преступления и личности преступника, определения направления поиска и познания лица, ведущего расследование.

§3. Правовая основа и современное состояние преступности в данной сфере.

Имеющаяся в современных реалиях нормативно-правовая база (правоохранительных органов и иных государственных учреждений, общественных организаций, коммерческих структур, и т. п.) отличается своей разнородностью, следовательно, в вопросах расследования преступлений в сфере высоких технологий неизбежны проблемы взаимодействия в процессе правоприменения, «размытость» правовой базы не позволяет эффективно противодействовать преступности, поэтому совершенствование научного знания, методического обеспечения этого вида деятельности – одна из основных задач правоохранительных органов, государственных и других взаимодействующих структур. Основными источниками являются:

1. Против транснациональной организованной преступности: конвенция ООН, принятая Резолюцией 55/25 Генеральной Ассамблеи от 15.11.2000
2. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001)
3. О Концепции сотрудничества государств - участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий: решение Совета глав государств СНГ от 25.10.2013
4. Конституция РоссийскойФедерации
5. Уголовный кодекс Российской Федерации
6. Уголовно-процессуальный кодекс Российской Федерации
7. «О связи»: федер. закон от 07.07.2003 № 126-ФЗ
8. «Об информации, информационных технологиях и о защите информации»: федер. закон от 27.07.2006 № 149-ФЗ
9. «О ратификации Конвенции Организации Объединенных Наций против

транснациональной организованной преступности и дополняющих ее Протокола против незаконного ввоза мигрантов по суше, морю и воздуху и Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее»: федер. закон от 26.04.2004 г. № 26

10. Конвенция о преступности в сфере компьютерной информации (ETS №85) [рус., англ.] (Заключена в г. Будапеште 23.11.2001
11. 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: [приказ МВД России от 29.08. 2014 №736
12. Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»

В современных условиях жизнедеятельности общества сети Интернет являются основополагающим фактором сферы коммуникаций: с их помощью осуществляются различные операции с денежными средствами (с использованием компьютеров, банкоматов, иных платежных систем), осуществляется поиск различных товаров и услуг, информации. Эти действия напрямую зависят от различных информационных технологий, в результате чего ряд пользователей ежедневно подвергаются атакам со стороны киберпреступников.

Современные достижения в области телекоммуникаций, сопровождающиеся повсеместным и массовым внедрением цифровых технологий во все сферы жизни современного человека, в последнее десятилетие повлекли за собой периодически возникающие новые вызовы, угрозы и риски, которые потрясают сферу общественных отношений[1].

[1] Хохлова О.М. Общественное согласие в социально-политической сфере современного общества: монография. – Красноярск: Сиб. федер. ун-т, 2016. – 176с.

Интернет позволяет эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, порождать новые, неизвестные мировому сообществу виды общественно опасных преступлений.

Преступному сообществу в условиях современной действительности предоставляется обширный технический потенциал и всеобъемлющие возможности Интернета, которые киберпреступники используют в своих преступных целях. Глава 28 Уголовного кодекса Российской Федерации (далее УК РФ) предусматривает ответственность за преступления в сфере компьютерной информации, но в ней отсутствуют нормы, предусматривающие ответственность, например, за незаконные действия в сфере телекоммуникаций и компьютерной информации, не имеет современное российское уголовное законодательство и понятий, определяющих и регламентирующих преступления, совершаемые с использованием высоких технологий, что, разумеется, ставит перед научным сообществом ряд сложных задач.

Статистика преступлений демонстрирует печальную динамику: количество зарегистрированных преступлений в сфере компьютерной информации с 1995 по 2005 г. в России выросло более чем в 300 раз, что составило более 10 тыс. преступлений в год.

За прошедший 2019 г. широкое распространение получили мошеннические действия, совершаемые с использованием электронных средств платежа (ст. 159.3 УК РФ), их количество выросло за первое полугодие 2018 г. в семь раз, за второе – в 6 раз. Определены и регионы-лидеры РФ по количеству подобных преступлений: Ставропольский край (66), Мурманская область (52), республика Татарстан (37), Москва (34) и Саратовская область (31).

По данным Генеральной прокуратуры РФ в 2017 г., в новостных порталах Интернет зарегистрировано 1883 таких преступлений, общий рост

составляет 7,7 %, а за первое полугодие 2018 г. – 233, отмечен рост на 3,4 %. Наибольшее количество таких преступлений зарегистрировано в 2017 г. в Удмуртии (194),Республике Коми (132), в Омской (75), Владимирской (66), Кировской (64), Волгоградской областях (60), в Москве (60) и в Краснодарском крае (51).

Отрицательной тенденцией является уменьшение количества расследованных преступлений на 19,6 % (с 903 до 726), положительной – рост нераскрытых преступлений на 30,5 % (с 790 до 1031). Общий процент раскрываемости данных преступлений составил 41,3 %.

Процессы глобальной компьютеризации и цифровизации, происходящие в современном мировом сообществе, имеют как положительные, так и отрицательные последствия, порой приводят к модификации преступности, которая стремительно видоизменяется, приобретая новые характеристики.

Статистика МВД России только за 9 месяцев 2017 г. фиксирует стремительный рост (количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, увеличилось на 94 % по сравнению с 2016 г.). Имеются прогнозы специалистов, что рост преступлений в сфере высоких технологий в ближайшее время будет нарастать.

Современные информационные технологии сегодня используются практически во всех сферах жизни общества: в банковской, промышленной, торговой, научной, культурной, духовной, образовательной и других сферах, демонстрируя наглядно динамический рост и качественное обновление компьютерной преступности в нашей стране, это, несомненно, создает новые угрозы и вызовы для развития общества и государства в целом. Интернет в современной жизни по многим показателям более привлекательное средство для экстремистско-

террористической деятельности [1].

В январе - декабре 2019 года зарегистрировано 294,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 68,5% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8% в январе - декабре 2018 года до 14,5%.(рис. 1.1 и рис.1.2)

Практически все такие преступления (98,4%) выявляются органами внутренних дел.

Почти половина таких преступлений (48,5%) относится к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0%); половина (53,3%) совершается с использованием сети «Интернет»: 157,0 тыс. (+45,4%), более трети (39,5%) – средств мобильной связи: 116,2 тыс. (+89,5%).

Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества: 235,5 тыс. (+83,2%), каждое двенадцатое (8,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 24,7 тыс. (+31,2%).На основании изложенного, можно сделать вывод о том, что компьютерная преступность представляет собой очень серьезную угрозу, как для отдельных государств, так и для всего мирового сообщества, в связи, с чем необходимо разработать и реализовать на практике действенные механизмы противодействия подобным явлениям.[2]

---

[1] Лапунова Ю.А, Голяндин Н.П. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. – 2017. – № 3 (43). – С.100–104.

[2] «Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2019 года» МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ФКУ «ГЛАВНЫЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР» Официальный сайт Министерства внутренних дел Российской Федерации https:// мвд.рф (эл.ресурс) (дата посещения 20.02.2020)

ГЛАВА 2 ОРГАНИЗАЦИЯ И ТАКТИКА, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

§1. Организационно-тактические приемы раскрытия преступлений в сфере высоких технологий

Информационные и коммуникационные технологии все более активно используются в целях совершения противоправных действий. При этом значительное число «традиционных» преступлений, таких как кража, мошенничество, присвоение и растрата, вымогательство, причинение имущественного путем обмана или злоупотребления доверием и другие, совершаются в совокупности с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных компьютерных программ, нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей1.

В соответствии с ч. 2 ст. 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления. Процессуальными средствами их установления являются действия, предусмотренные ч. 4 ст. 21, ч. 1, 3 ст. 144 УПК РФ. Перечень конкретных обстоятельств, подлежащих установлению в стадии возбуждения уголовного дела, зависит от содержания диспозиции уголовно-правовой нормы, по признакам которой возбуждается уголовное дело.

Так, при решении вопроса о возбуждении уголовного дела по факту хищения денежных средств, принадлежавших потерпевшему и находившихся на его счете в кредитной организации, должны быть установлены факты:

– списания денежных средств со счета их собственника без согласия последнего;

– зачисления указанных денежных средств на счета иных лиц, не состоящих в договорных отношениях с пострадавшим;

– характеристики несанкционированной транзакции: дата и время ее совершения, номер счета списания / зачисления, сумма, идентификационные данные отправителя / получателя платежа.

В стадии возбуждения уголовного дела в зависимости от источника исходной информации возможны две типичные проверочные ситуации:

1) информация о преступлении поступила от лица, которому причинен вред вследствие совершения преступления;

2) признаки преступления выявил орган дознания в процессе реализации им оперативно-розыскной деятельности.

В первой следственной ситуации процессуальными средствами установления перечисленных фактов являются:

1. Получение письменного объяснения заявителя с указанием характера и размера вреда, обстоятельства его причинения, вероятного круга подозреваемых лиц.

Так, при поступлении заявления о хищении денежных средств с электронного средства платежа, принадлежащего потерпевшему, устанавливаются: наименование банковского учреждения и реквизиты счета, с которого произошло неправомерное списание денежных средств, дата, время и обстоятельства обнаружения такого списания, сумма материального ущерба (с учетом возможного неоднократного списания), используемый заявителем сервис дистанционного банковского обслуживания, поступавшие от него уведомления, дата и время их получения, способ входа в систему ДБО, используемое при этом оборудование (персональный компьютер, смартфон, планшетный компьютер,банкомт, банковский терминал самообслуживания и пр.), местонахождение данных устройств, производил ли пользователь спорные транзакции, подключена ли услуга SMS-информирования, а также отправлял ли пользователь SMS-сообщение с кодом подтверждения транзакции,

известны ли пользователю получатели списанных с его счетаденежных средств и в каких отношениях он с ними состоит (ответ на данный вопрос возможен при условии получения заявителем в банке расширенной выписки по своему счету, содержащей номера банковских счетов, лицевые счета мобильных телефонов, ФИО получателей).

2. Осмотр места происшествия, в рамках которого осматривается непосредственно микропроцессорное устройство (стационарный компьютер, ноутбук, планшетный компьютер, смартфон), с использованием которого заявитель установил факт совершения преступления, например, факт списания с банковского счета денежных средств. В последнем случае фиксируются наличие на устройстве программного обеспечения системы ДБО, а также сообщения, поступившие на устройство в связи со спорной транзакцией (уведомления и запросы системы ДБО). По результатам осмотра устройство подлежит изъятию для последующего назначения и производства судебно-компьютерной экспертизы. Телефон и компьютер должны быть изъяты с участием специалиста. Телефон необходимо перевести вавиарежим, компьютер – в режим гибернации.

3. Направление поручения в орган дознания на получение в кредитной организации справки по счету заявителя. В соответствии со ст. 26 Закона РФ от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве. Соответственно, на данной стадии орган дознания может получить названные сведения исключительно на основании судебного решения. Указанное обстоятельство, наряду с нормативно незакрепленным сроком на подготовку кредитной организацией ответа на запрос, порождает значительные сложности в оперативном получении информации о движении денежных средств по лицевым счетам абонентских номеров (банковских карт), сведений о владельцах абонентских номеров (банковских карт) и иных

сведений, имеющих значение для решения вопроса о возбуждении уголовного дела.

4. Назначение судебной компьютерной экспертизы в отношении изъятых в ходе осмотра предметов.

Во второй проверочной ситуации, с учетом требований Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно- розыскной деятельности», Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания,следователю или в суд[1]оперативные подразделения органов дознания по результатам оперативно-розыскных мероприятий предоставляют должностным лицам органов предварительного расследования следующие материалы и сведения:

1. Рапорт об обнаружении признаков преступления с отражением информации о времени, месте и обстоятельствах его совершения, содержании проведенных оперативно-розыскных мероприятий, документов и иных объектов, полученных в ходе их проведения (аудио-, видеозаписи, фотоснимки, электронные носители информации и т. п.).

2. Постановление о предоставлении материалов оперативно- розыскной деятельности органу предварительного следствия, подписанное руководителем органа (подразделения), осуществляющего оперативно-разыскную деятельность с указанием перечня предоставляемых документов (например, справки о результатах проведения оперативно-розыскных мероприятий, копии рассекреченных документов).

3. Копия судебного решения о проведении оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища.

---

[1]Об утверждении Инструкции о порядке представления результатов оперативно- розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/ 535/398/68

4. Постановление о проведении оперативно-розыскных мероприятий руководителя органа, осуществляющего оперативно-разыскную деятельность (начальника или его заместителя), в случае проведения оперативного эксперимента или оперативного внедрения.

5. Постановление о рассекречивании сведений, составляющих государственную тайну, их носителей, к которым относятся в том числе сведения об организации и тактике проведения оперативно- поисковых и оперативно-технических мероприятий, используемых при их проведении технических средствах, о штатных негласных сотрудниках, с указанием конкретного перечня документов, подлежащих рассекречиванию.

6. Документы, фиксирующие содержание и результаты проведения оперативно-розыскных мероприятий, в том числе протоколыизъятия электронных носителей, оперативного наблюдения, перехвата компьютерной информации и т. п.

7. Справки кредитных организаций, документы и видеозаписи, включая записи камер видеонаблюдения, банкоматов и пр.

8. Заключение специалиста о результатах исследования электронных носителей информации, а также иных объектов, изъятых в ходе оперативно-розыскных мероприятий.

9. Копии запроса, направляемого в НЦБ Интерпола, по форме, определенной в приложении 9 к Инструкции по линии Интерпола.

Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола[1] установлено, что в ходе проведения оперативно-розыскных мероприятий, дознания или предварительного следствия по преступлениям экономической направленности через НЦБ.

Интерпола может быть получена следующая информация:

а) официальные наименования юридических лиц, зарегистрированных за рубежом;

[1]Об утверждении Инструкции по организации информационного обеспе- чения сотрудничества по линии Интерпола: приказ МВД России, Минюста Рос- сии, ФСБ России, ФСО России, ФСКН России, ФТС России от 6 октября 2006 г.№ 786/310/470/454/333/971

б) их юридический адрес, номер, дата регистрации;

в) фамилии и имена физических лиц – руководителей (в отдельных случаях – учредителей, акционеров);

г) направление деятельности; д) размеры уставного капитала;

е) сведения криминального характера о деятельности юридических и физических лиц.

В отдельных случаях через НЦБ Интерпола возможно получение сведений о наличии недвижимости и иной собственности за рубежом у лиц, являющихся фигурантами дел оперативного учета, а также подозреваемых или обвиняемых в совершении тяжкого преступления, при условии, если известно предполагаемое местонахождение (регистрация) объектов собственности (страна, штат, регион, город, компания), а также получение ограниченной информации по некоторым вопросам финансово-хозяйственной деятельности юридических лиц (выполнение контрактов, финансовое положение), если запрашиваемая информация не относится к коммерческой тай- не. Получение указанных сведений и истребование копий финансово-хозяйственных и других коммерческих документов по каналамИнтерпола зависит от добровольного согласия проверяемых лиц на предоставление документов и дачу объяснений.

Сведения, составляющие банковскую тайну, в том числе об открытии физическими и юридическими лицами счетов в банках и о движении денежных средств по ним, могут быть получены от правоохранительных органов иностранных государств – членов Интерпола только после рассмотрения соответствующим органом юстиции, прокуратуры или судом иностранного государства официального обращения (международного следственного поручения по уголовному делу) Генеральной прокуратуры Российской Федерации, копия которого может быть передана по каналам Интерпола.

10. Иные материалы, в том числе объяснения лиц, располагающих информацией, имеющей значение для дела, а также иные объекты, полученные в ходе оперативно-розыскных мероприятий.

Органом, осуществляющим оперативно-разыскную деятельность, при подготовке и оформлении для передачи уполномоченным должностным лицам (органам) материалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, должны быть приняты необходимые меры по их сохранности и целостности (защита от деформации, размагничивания, обесцвечивания, стирания и др.). При представлении фонограммы к ней прилагается бумажный носитель записи переговоров. Допускается представление материалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно указывается в сообщении (рапорте), на бумажном носителе записи переговоров. В этом случае оригиналы мате- риалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, если они не были в дальнейшем истребованы уполномоченным должностным лицом (органом), хранятся в органе, осуществившем оперативно-розыскные мероприятия, до завершения судебного разбирательства и вступления приговора в законную силу либо до прекращения уголовного дела
(уголовного преследования).

Результаты оперативно-розыскной деятельности, представляемые для решения вопроса о возбуждении уголовного дела, должны содержать достаточные данные, указывающие на признаки преступления, а именно сведения: о том, где, когда, какие признаки и какого именно преступления обнаружены; при каких обстоятельствах имело место их обнаружение; о лице (лицах), его совершившем (если они известны), и очевидцах преступления (если они известны); о местонахождении предметов и документов, которые могут быть признаны вещественными доказательствами по уголовному делу;

о любых других фактах и обстоятельствах, имеющих значение для решения вопроса о возбуждении уголовного дела.

Так, например, результатом такого оперативно-розыскного мероприятия, как прослушивание телефонных переговоров является соответствующая аудиозапись телефонных переговоров, общий объем которых в оцифрованном виде может превышать десятки гигабайт. При этом, наряду со сведениями, имеющими значение для дела, такие аудиозаписи содержат в большом количестве нейтральные сведения. В этом случае в орган предварительного расследования предоставляются аудиозаписи и распечатки наиболее значимых переговоров, содержащих информацию, имеющую отношение к рас- следуемому событию, в том числе информацию об осознании членами преступной группы преступного характера совершаемых ими действий.

Также большой объем информации может содержаться по результатам снятия информации с технических каналов связи. В этом случае в орган предварительного расследования представляется справка, включающая распечатку наиболее значимых электронных писем, сведения об онлайн-платежах и пр.

С учетом данных, полученных в результате предварительной проверки сообщения о преступлении, совершенном с использованием информационно-коммуникационных технологий, принимается решение о возбуждении уголовного дела, об отказе в возбуждении уголовного дела или передаче сообщения о преступлении по подследственности в соответствии с положениями ст. 151 УПК РФ.

В следственной практике зачастую возникает неопределенность, связанная с установлением места совершения преступления и, соответственно, местом производства предварительного расследования. Это обстоятельство обусловлено тем, что в механизме преступлений, совершенных с использованием информационно- коммуникационных технологий, присутствует несколько мест локализации следов: место жительства субъекта

преступления, место его подключения к сети Интернет, местонахождение потерпевшего, адреса открытия и обслуживания его банковских счетов, адреса открытия и обслуживания банковских счетов, на которые переведены похищенные денежные средства, и т. д.

Следственным департаментом МВД России в органы предварительного следствия направлены директивные указания от 20 июня 2014 г. № 17/3-16230 об исключении фактов необоснованного пере- направления в порядке ст. 152 УПК РФ материалов доследственнойпроверки о преступлениях рассматриваемой категории, влекущих увеличение сроков ее проведения и утрату следов преступления, необходимости при наличии достаточных оснований принимать процессуальное решение о возбуждении уголовного дела по месту поступления заявления о совершенном преступлении.

Кроме того, заместитель Генерального прокурора Российской Федерации В. Я. Гринь в информационном письме от 3 ноября 2015 г. № 36-11-2015 предлагает при осуществлении прокурорского надзора при передаче материалов проверок и уголовных дел учитывать следующую позицию: «…правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно опасных последствий …».

Следует подчеркнуть, что независимо от источника исходной информации о преступлении его эффективное расследование возможно при условии оперативного сопровождения со стороны органа дознания. При этом в соответствии с п. 6.7 Решения совещания у заместителя Министра внутренних дел Российской Федерации – начальника Следственного департамента МВД России от 29 июля 2016 г. № 3 в целях устранения недостатков работы, повышения эффективности деятельности органов предварительного следствия введено в практику принятие процессуальных решений по сообщениям о преступлениях, предусмотренных ст. 159–159.6,

160, 165, 171,172, 174, 174.1, 193, 193.1, 195–197, 200.1, 200.2, 200.3, 201, 272–274,285, 286 УК РФ, если они совершены в кредитно-финансовой сфере, оборонно-промышленном, жилищно-коммунальном, топливно-энергетическом, агропромышленном комплексах, в сфере государственного оборонного заказа, информационных технологий (за исключением мошенничеств с использованием мобильных телефонных средств связи), долевого строительства многоквартирных домов, а также связаны с деятельностью «финансовых пирамид», и повлекли причинение ущерба либо извлечение незаконного дохода в сумме, превышающей 6 млн руб., только следователями. При этом в соответствии с указанием Следственного департамента МВД России от 20 июня 2014 г. № 17/3-16230 в органах предварительного следствия МВД России регионального и городского (окружного) уровня с 1 июля 2014 г. организовано закрепление следователей, специализирующихся на расследовании преступлений в сфере информационных технологий, с учетом достаточного опыта работы в органах предварительного следствия и наличия специальных познанийв указанной области. Аналогичное требование содержится и в указании Следственного департамента МВД России от 15 августа 2014 г.№ 17/2-21427 с тем лишь уточнением, что количество закрепленных за данным направлением следователей должно быть не менее двух, а также в иных организационно-управленческих документах[1].

Указанием Следственного департамента МВД России от 26 декабря 2017 г. исх. № 17/3-4125 «Об организации расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий» начальникам следственных органов регионального уровня и приравненных к ним следственных органов МВД России поручено обеспечить заблаговременное обсуждение материалов доследственных проверок в аппаратах следственных органов МВД России по

[1]См.: п. 4 указания Следственного департамента МВД России от 26 декабря 2017 г. исх. № 17/3-4125 «Об организации расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий».

субъектам Российской Федерации, уделяя особое внимание их полноте и качеству, проведению необходимых исследований, результатам оперативно-розыскных мероприятий по изобличению лиц, совершивших преступления, организовать результативное взаимодействие с оперативными подразделениями.

Практика показывает, что оперативное сопровождение расследования уголовных дел осуществляется лишь на первоначальном этапе – «по горячим следам» до установления лица, подлежащего привлечению в качестве обвиняемого. В дальнейшем активность участия оперативных подразделений по установлению похищенного имущества, дополнительных свидетелей и иных обстоятельств, подлежащих доказыванию, снижается. Оперативное сопровождение, вплоть до окончания расследования и направления уголовного дела в суд, осуществляется лишь по резонансным преступлениям, а по остальному массиву уголовных дел – в единичных случаях, в виде сбора дополнительной информации или обеспечения привода потерпевших, свидетелей, обвиняемых.

Еще одним направлением повышения эффективности внешнего взаимодействия участников расследования является использование территориальными органами внутренних дел систем электронного документооборота, а также заключение соглашений об информационном обмене с кредитно-финансовыми организациями и организациями связи. Во исполнение п. 1.1. Решения Коллегии МВД России от 24 октября 2017 г. № 3км «О мерах по совершенствованию организации раскрытия и расследования мошенничеств» в Следственном департаменте МВД России проанализирована организация деятельности территориальных органов МВД России на окружном, межрегиональном и региональном уровнях по заключению соглашений с подразделениями ПАО «Сбербанк России», другимикредитно-финансовыми организациями, в том числе не имеющими собственной филиальной сети в регионах, территориальными органами ФНС России и Росреестра, уполномоченными многофункциональными центрами

(далее – МФЦ), органами социальной защиты населения, расположенными на территориях субъектов Российской Федерации, об электронном обмене документами и информацией, а также эффективность взаимодействия с данными организациями при раскрытии и расследовании мошенничеств.

Результаты анализа показали востребованность систем электронного документооборота с ведущими кредитными учреждениями и операторами сотовой связи с возможностью получения информации по всей территории Российской Федерации.

По состоянию на март 2018 г. на основе соглашения между МВД России и ПАО «Сбербанк России» от 23 октября 2017 г. об обмене информацией в электронном виде 24 территориальными органами внутренних дел заключены договоры с региональными представительствами указанной кредитной организации, еще в ряде субъектов Российской Федерации данный вопрос находится в стадии согласования. В соответствии с вышеназванным соглашением электронный документооборот между сторонами осуществляется на принципах конфиденциальности, согласованности действий, взаимопомощи и безвозмездности при соблюдении требований федеральных законов, в частности от 27 июля 2006 г. № 147-ФЗ «Об информации, информационных технологиях и о защите информации», от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» и иных нормативных правовых актов.

Отдельными территориальными органами внутренних дел дополнительно заключены соглашения об электронном обмене информацией с КИВИ Банк (АО), которые позволяют получить в срок до 3 суток необходимые сведения о владельце «QIWI- кошелька» и произведенных им транзакциях за интересующий период.

Кроме того, существует положительная практика заключения соглашений об электронном документообороте с организациями связи, в частности с ПАО «Мегафон», в рамках которых в срок до 10 дней становится возможным получение сведений об анкетных данных абонента по номерам телефона и

SIM-карты, ИНН юридического лица, а также подключенных услугах и платежах.

Так, МВД по Республике Татарстан с января 2016 г. в рамках заключенного с территориальным отделением ПАО «Сбербанк России» соглашения используется система удаленного доступа«SBERSIGN», предоставленная кредитной организацией, позволяющая посредством электронного документооборота в срок до 7 дней получать информацию об открытых расчетных счетах клиента, движении денежных средств, а также данные о подключении услуг дистанционного банковского обслуживания «Мобильный банк» и соответствующих номерах телефонов.

Сведения о производимых по банковским картам транзакциях предоставляются на основании ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» без получения судебного решения, что позволяет существенно уменьшить временные затраты на получение необходимой информации и сократить срок предварительного следствия.

Помимо этого, в указанном подразделении функционируют системы по электронному обмену документами и информацией с ПАО «Мегафон» и ПАО «Вымпелком».

В ГУ МВД России по Пермскому краю успешно используется система электронного документооборота в рамках заключенного в 2015 г. соглашения с ПАО «Сбербанк России». Соглашение пред- усматривает возможность осуществления блокировки лицевых счетов абонентов на стадии регистрации заявления о преступлении. Кроме того, подписаны соответствующие соглашения с КИВИ Банк (АО), ПАО «Почта Банк», ПАО «Мегафон», а также Федеральной службой по государственной регистрации кадастра и картографии по Пермскому краю.

Восточно-Сибирским ЛУ МВД России на транспорте с июля 2017 г. действует соглашение о сотрудничестве с КИВИ Банк (АО) в области обмена оперативной и иной информацией по уголовным делам и делам оперативной

проверки, предусматривающее возможность предоставления посредством электронного документооборота в течение 1–2 суток необходимых сведений о владельце «QIWI- кошелька» и произведенных им транзакциях за интересующий период.

С сентября 2016 г. Главным следственным управлением ГУ МВД России по г. Москве в рамках соглашения конкретный сотрудник имеет возможность доступа к автоматизированной системе обработки запросов ОАО «Мегафон». Указанная система предоставляет возможность направления электронных запросов (с приложением соответствующих разрешительных документов) по находящимся в производстве следователей ГСУ уголовным делам о предоставлении различных сведений об абонентах сети и получения ответов на них. Ответ на запрос инициатора поступает в виде сопроводительного письма в формате «pdf», подписанного электронной подписью уполномоченного сотрудника ОАО «Мегафон»,с приложением запрашиваемых данных в формате «xls» с указанием имени, точного размера и отпечатка файла. При этом имеется возможность обработки следующих следственных запросов:

1. Предоставление сведений об анкетных данных абонента по номеру телефона.
2. Предоставление сведений об анкетных данных абонента и номере телефона по номеру SIM-карты.
3. Предоставление сведений о номере телефона и данных абонента по ФИО и иным анкетным данным.
4. Предоставление сведений о номере телефона и данных абонента по ИНН юридического лица.
5. Предоставление сведений о подключенных абонентом услугах, а также платежах.

Предполагается дальнейшее наращивание функционала системы за счет обеспечения возможности направления запросов с обязательным

приложением соответствующих постановлений суда, с последующим получением на электронном носителе в офисе ПАО «Мегафон» информации:

– о телефонных соединениях абонента (детализации) с указанием базовых станций по номеру телефона;

– обо всех телефонных соединениях абонентов оператора связи, находившихся в конкретном месте (биллинга);

– о телефонных соединениях абонента (детализации) с указанием базовых станций по номеру IMEI телефона.

Наличие у правоохранительных органов подобных каналов информационного взаимодействия позволяет повысить эффективность деятельности по выявлению, раскрытию и расследованию преступлений, а также усилить защищенность граждан от противоправных посягательств.

Особенности организации первоначального этапа расследования преступлений против собственности, совершенных с использованием информационно-коммуникационных технологий

Эффективное расследование преступлений, совершенных с использованием информационно-коммуникационных технологий, возможно при выполнении определенного алгоритма действий.

Выполнить комплекс процессуальных действий с заявителем:

– незамедлительно после принятия решения о возбуждении уголовного дела уведомить о принятом решении заявителя. Если уголовное дело возбуждается в отношении конкретного лица, то ему вручается копия постановления о возбуждении против него уголовного дела (п. 1. ч. 4 ст. 46 УПК РФ);

– вынести постановление о признании заявителя потерпевшим;

– допросить потерпевшего об обстоятельствах совершения преступления. Если совершено хищение принадлежащих ему денежных средств, в протоколе допроса подлежит отражению обстоятельства обнаружения хищения: какие именно действия были выполнены потерпевшим лично до и после совершения преступления; с какой целью, предпринимались ли им

какие-либо действия по установлению лица, совершившего преступление, самостоятельно; если да, то с использованием какой техники и программного обеспечения; предоставлялись ли потерпевшим кому-либо сведения о себе, с какими лицами, по каким адресам в сети Интернет он обращался; имеются ли скриншоты переписки; на какие именно электронные кошельки, расчетные счета производил перечисления денежных средств; с использованием каких сервисов осуществлялась коммуникация с лицом, совершившим преступление; какова точная сумма причиненного преступлением ущерба (с учетом имущественного положения физического лица, размера его личных доходов, доходов семьи, наличия иждивенцев, кредитных или иных имущественных обязательств); каков круг лиц, которым могло быть известно о наличии денежных средств на банковских счетах, а также кто из них имел возможность доступа к управлению счетами потерпевшего, в том числе к его мобильному телефону; поступали ли потерпевшему в период, предшествующий хищению денежных средств, SMS-сообщения или электронные письма с указанием попыток осуществления транзакций, которые он не совершал; не было ли сбоев в работе аккаунтов в социальных сетях; сообщал ли данные своих счетов кому-либо в ходе телефонных разговоров, в том числе с сотрудниками банков. Если будут установлены подобные факты, у потерпевшего нужно выяснить всю информацию, касающуюся передачи сведений о своих счетах и режима доступа к ним, принять меры по сохранности поступивших потерпевшему сообщений и иной информации;

– получить исковое заявление, вынести постановление о признании гражданским истцом;

– в случаях наличия у потерпевшего документов, подтверждающих факт совершения хищения (платежных поручений, приходных кассовых ордеров, скриншотов, фиксирующих перевод денежных средств в платежных системах, претензионных требований со стороны третьих лиц), и / или документов, отражающих переписку потерпевшего с лицом, совершившим

преступление (чаще всего скриншоты экрана с перепиской в социальных сетяхили посредством электронной почты), – вынести постановление о производстве их выемки и произвести их изъятие в установленном порядке;

– провести осмотр компьютерной техники потерпевшего, в ходе которого фиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о переводе средств в электронных платежных системах). Целесообразно оформлять приложения к протоколу следственного действия в виде скриншотов экрана компьютера (с целью обеспечения наглядности);

– принять решение о признании и приобщении к материалам уголовного дела в качестве вещественных доказательств изъятых предметов и документов.

Важнейшей задачей данного этапа является установление способа совершения преступления.

Одним из ключевых элементов в расследовании по уголовным делам о преступлениях, совершенных с использованием информационно-коммуникационных технологий, является установление лица, совершившего преступление.

В большинстве случаев на данное лицо указывает местонахождение электронно-вычислительной техники, которая использовалась в качестве орудия преступления.

При совершении хищений денежных средств с использованием систем дистанционного банковского обслуживания осуществляется управление электронными счетами и (или) ведется переписка с потерпевшими. В данной ситуации с целью установления лица, совершившего хищение денежных средств, необходимо:

– получить сведения о движении денежных средств потерпевшего в кредитной организации или у оператора платежной системы на основании запроса следователя, согласованного с руководителем следственного органа (в соответствии с требованиями ст. 26 Федерального закона от 27 июня 2011

г. № 161-ФЗ «О национальной платежной системе» и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1
«О банках и банковской деятельности»);

– на основании запросов в обозначенные организации необходимо также получить сведения, указанные владельцем счета при его регистрации, а также сведения об IP-адресах, с которых осуществлялась регистрация в системе дистанционного банковского обслуживания и доступ к счету при совершении сомнительной транзакции;

– в случаях перемещения похищенных денежных средств с использованием платежных систем, операторами которых являются юридические лица, зарегистрированные за пределами Российской Федерации, следует в установленном порядке направить запрос об оказании международно-правовой помощи;

– полученную на основании вышеуказанных запросов информацию об IP-адресах проверить посредством открытого интернет-сервиса, расположенного по адресу https://www.ripe.net/, или любого другого схожего с ним по функциональности сервиса, позволяющего установить принадлежность IP-адреса к конкретному провайдеру. Дальнейшие действия будут зависеть от того, каков этот IP-адрес: статический или динамический;

– в случае совершения спорных транзакций со статического IP-адреса на основании судебного решения необходимо произвести выемку сведений об абонентах в организации-провайдере, которой принадлежат интересующие следствие IP-адреса, либо в порядке п. 4. ч. 2 ст. 38 УПК РФ дать поручение органам дознания на получение данной информации.[1]

В соответствии с положениями ст. 53 Федерального закона от 7 июля 2003 г. № 126-ФЗ«О связи» к сведениям об абонентах относятся фамилия, имя,

[1]В соответствии с п. 1.1. ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безо- пасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента – юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента. Данные сведения укажут, что именно с компьютерной техники конкретного абонента или организации, находящейся по конкретному адресу, осуществлялись спорные онлайн-транзакции, велась определенная переписка и т. д.

При установлении конкретного лица, совершившего противоправные действия с использованием статического IP-адреса, следует принять во внимание, что такими адресами пользуются, как правило, крупные организации или государственные органы. В таких организациях нередко предоставляется публичный (свободный) доступ в сеть Интернет всем желающим (на основании процедуры регистрации) либо имена и пароли для своих сотрудников и посетителей. В обоих случаях конкретному пользователю выделяется IP-адрес, под которым он получает доступ в Интернет. Сведения, содержащиеся в этом журнале (IP-адрес, предоставленный конкретному пользователю, сведения об интернет-адресах, к которым осуществлялось подключение с данного IP-адреса, дата, место, время начала и окончания доступа, MAC-адрес сете- вой карты, номере SIM-карты, через которую произошла авторизация пользователя при подключении к Интернету, используемая им операционная система и браузер), также подлежат изъятию посредством выемки;

– если доступ в сеть Интернет осуществлялся с динамического IP-адреса и с использованием SIM-карты оператора сотовой связи, то для идентификации соответствующего лица необходимо запросить у оператора сотовой связи детализацию звонков, а также данные о способах пополнения финансового баланса SIM- карты. Если для пополнения баланса

использовался электронный кошелек отечественной платежной системы (Яндекс.Деньги) или банковские карты, эмитированные отечественными банками, то последующие запросы необходимо направить этим субъектам для предоставления сведений о том, кто является владельцем электронного кошелька либо кто является клиентом (держателем) счета банковской карты.

Для установления лица, разместившего в социальной сети какую-либо противозаконную информацию, необходимо:

– направить запрос администратору социальной сети с постановкой следующих вопросов: когда и во сколько была создана группа (указывается название соответствующей группы в социальной сети) или размещено фото-, видеоматериал (указывается название файла в конкретной группе) по адресу (приводятся данные из адресной строки); каков логин пользователя социальной сети, создавшего группу или разместившего фото-, видеоматериал; во сколько зашел и во сколько вышел пользователь с сайта социальной сети при создании группы (размещении фото-, видеоматериала); какие идентификационные данные сообщил при регистрации пользователь (фамилия, имя, отчество, номер мобильного телефона, адрес электронной почты и т. д.); каков IP-адрес пользователя, создавшего группу или разместившего фото-, видеоматериал в указанные дату и время доступа; какие операционная система и браузер используются на компьютере указанного пользователя.

Почтовые адреса администраторов социальных сетей

Социальнаясеть	Организация	Адрес
Mail.ru (Моймир)	ООО «Мэйл.ру»	Ленинградский проспект, д. 79, стр. 39, г. Москва, 125167
Odnoklassniki.ru	ООО «Мэйл.ру»	Ленинградский проспект, д. 79, стр. 39, г. Москва, 125167
Vkontakte.ru (vk.com)	ООО «В контакте»	ул.Херсонскаяд.12-14,литерА, помещение1-Н, г. Санкт-Петербург, 191024
Mamba.ru	ЗАО «Мамба»	ул. 2я Звенигородская, д. 3, стр. 42, г. Москва, 123022

vkrugudruzei.ru	ООО «КМ онлайн»	ул.Пришвина,д.8,корп.1, г. Москва,127549
Loveplanet.ru	Группакомпаний «РосБизнесКонсалтинг»	ул.Профсоюзная,д.78,стр.1, г. Москва,117393

– определить провайдера, за которым закреплен IP-адрес, выделенный искомому пользователю, разместившему противоправный контент. Это можно сделать, используя сервис www.whois-service.ru, в поисковую строку которого вводится интересующий IP-адрес, после чего система представит ответ о данных провайдера, который выдал соответствующий адрес[1];

– направить запрос провайдеру с постановкой следующих вопросов: кому из пользователей выделен указанный IP-адрес (указывается дата, время доступа на сайт социальной сети и время выхода из нее, когда была создана группа или размещено видео); к какому виду относится этот IP-адрес – статический или динамический? Использовался ли NAT2 при предоставлении доступа этому клиенту к сети Интернет; если использовался статический IP-адрес, то необходимо потребовать предоставить имеющиеся данные о физическом лице, заключившим договор с провайдером, а также MAC-адрес[2]компьютерного устройства, через который предоставлен доступ к сети Интернет, физический адрес подключения, номер SIM-карты, через которую произошла авторизация пользователя при подключении к Интернету (если использовалась), операционная система и браузер указанного компьютерного устройства; регистрировался ли с кем-либо из пользователей договор по доступу в сеть Интернет, MAC-адрес компьютерного устройства которого установлен провайдером по предыдущему пункту запроса, если да, то с кем; выделялся ли IP-адрес для пользователя, MAC-адрес компьютерного устройства которого был установлен провайдером по предыдущему пункту запроса, если да, то когда, во сколько, по какому адресу был осуществлен доступ в Интернет и какие

[1] Для европейской части сети действует поисковая система по адресу: www.ripe.net.
[2]NAT – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

ресурсы сети Интернет посещал пользователь; если использовался механизм NAT, то необходимо потребовать предоставить адрес местонахождения источника Wi-Fi, через который пользователь получил доступ в Интернет, и количество пользователей, получивших доступ в Интернет через этот источник и находившихся одновременно на сайте социальной сети (название) с (время) по (время).

– направить запросы другим провайдерам в населенном пункте по месту проверки сообщения (расследования уголовного дела) с постанов- кой следующих вопросов: регистрировался ли с кем-либо из пользователей договор по доступу в сеть Интернет, MAC-адрес компьютерного устройства (указывается номер, предоставленный провайдером по предыдущему запросу), если да, то с кем; выделялся ли IP-адрес для пользователя, MAC-адрес компьютерного устройства (указывается номер, пре- доставленный провайдером по предыдущему запросу), если да, то когда, во сколько, по какому адресу был осуществлен доступ в сеть Интернет и какие ресурсы сети Интернет посещал пользователь;

– направить запрос и судебное решение российскому оператору сотовой связи, номер SIM-карты которого использовался для авторизации пользователя при подключении к сети Интернет (может быть предоставлен провайдером исходя из вышеуказанного запроса) или номер SIM-карты которого указан при регистрации пользователя в социальной сети. В запросе ставятся следующие вопросы: на кого зарегистрирована SIM-карта (указывается предоставленный провайдером или администратором социальной сети номер); пополнялся ли баланс указанной SIM-карты способами, позволяющими идентифицировать плательщика (банковская карта, электронный кошелек отечественных платежных систем и т. п.), если да, то указать соответствующие идентификационные данные;

– направить запросы и судебные решения в банки (субъектам отечественных платежных систем и т. п.) с требованием предоставить персональные данные лиц, карты (электронные кошельки и т. п.) которых

использовались для пополнения баланса номера SIM-карты (указывается соответствующий установленный номер);

– направить запрос и судебное решение в организацию, являющуюся администратором сервиса электронной почты, почтовый ящик кото- рой указан при регистрации пользователя в социальной сети.

Сведения о наиболее распространенных в России сервисах электронной почты и организациях, осуществляющих их администрирование

E-mail	Компания	Адрес, телефон
@mail.ru, @inbox.ru, @list.ru, @bk.ru	ООО «Мэйл.Ру»	125167, Россия, Москва, Ленинградский проспект, д. 39, стр. 79 тел. +7 495 725-63-57
@yandex.ru	ООО «Яндекс»	119021, Москва, ул. Льва Толстого, 16, тел: +7 495 739-70-00
@rambler.ru, @lenta.ru, @myrambler.ru, @autorambler.ru, @ro.ru, @r0.ru	ООО «Рамблер Интернет Хол- динг»	117105, Москва, Варшавское ш., 9, стр. 1, БЦ «Даниловская мануфактура», корпус «Ряды Солдатенкова» тел: +7 495 785-17-00
@qip.ru, @pochta.ru, @fromru.com, @front.ru, @hotbox.ru, @Hotmail.ru, @krovatka.su, @land.ru, @mail15.com, @mail333c.com, @newmail.ru, @nightmail.ru, @5ballov.ru, @aeterna.ru, @ziza.ru, @memori.ru, @photofile.ru, @fotoplenka.ru, @pochta.com, @nm.ru	ООО «МедиаМир»	117485, Москва, Профсоюзная 84/32, тел: +7 495 363-11-11

В запросе необходимо поставить вопрос о предоставлении данных пользователя, указанных им при регистрации почтового ящика, сведений о его активности, IP-адреса и MAC-адреса компьютерного устройства, с которого осуществлена регистрация почтового ящика и с которого осуществлен доступ к указанному почтовому ящику за интересующий период времени, а также абонентском номере активации и восстановлении пароля владельца электронного почтового ящика.

Если предоставленные IP-адреса отличаются от уже полученных, то необходимо вновь направить запрос провайдеру с целью получения данных, которые могут идентифицировать владельца почтового ящика.

Если преступление совершено с использованием интернет- сайта (например, интернет-магазина, сайта-клона и т. п.), то порядокустановлениявладельца, следующий:

– используя интернет-сервис Whois, в процессе следственного осмотра с участием специалиста получаем открытую информацию о лице, на которое зарегистрировано доменное имя (регистрант), и организации, на ресурсах которой размещается интернет-сайт с интересующим доменным именем;

– если в качестве владельца сайта указано PrivatePerson (частное лицо), то необходимо направить запрос в компанию- регистратор домена. При этом следует иметь в виду, что в большинстве случаев регистрационные данные, которые предоставляет владелец домена, администрацией не проверяются и могут не соответствовать действительности. Кроме того, сервисом Whois предоставляется информация только для доменов второго уровня вида xxx.ru, информацию для доменов вида yyy.xxx.ru необходимо получать у владельцев домена второго уровня;

– в полученной информации в поле nserver, как правило, указан владелец веб-хостинга (технической площадки) сайта, который может предоставить регистрационные данные (могут быть недостоверными), а также IP-адреса авторизации, достоверные контактные данные, платежные реквизиты;

– при установлении адреса электронной почты – выполнить действия по установлению владельца электронного почтового ящика, описанные выше.

Если преступление совершено с использованием электронного кошелька электронной платежной системы, то порядок действий по установлению его владельца следующий:

– направить администратору платежной системы запрос о предоставлении регистрационных данных участника, зарегистрировавшего электронный кошелек с идентификационным номером …, информации о

всех кошельках, зарегистрированных вышеуказанным участником, и истории операций по ним за весь имеющийся период с указанием IP-адресов, с которых происходила авторизация участника, а также в случае перечисления средств с кошельков, зарегистрированных данным участником, – аналогичной информации по другим участникам электронной платежной системы (за исключением сервисов обмена электронных денег) – получателям денежных средств;

Адреса для направления запросов

Платежная система	Организация	Адрес
«Webmoney»	ООО «ВебМани.Ру»	ул. Коровий вал, д.7, г. Москва, 119049
«Яндекс.Деньги»	ООО «ПС Яндекс. Деньги»	а/я 57, г. Москва, 119021
«QIWI»	ЗАО «QIWI банк»	мкр. Чертаново Северное, д. 1А, корп. 1, г. Москва, 117648.
Деньги@Mail.Ru	ООО «Деньги.Мэйл. Ру»	Ленинградский проспект, д. 39, стр. 79, г. Москва, 125167

– в полученных ответах будет содержаться информация, с каких IP-адресов осуществлялось управление данными кошельками (счетами) и куда переведены (где обналичены) деньги. Далее устанавливается местонахождение владельца запросами соответствующим интернет-провайдерам, которым принадлежат IP-адреса;

§2. Проблемы раскрытия и расследования преступлений в сфере высоких технологий, а также пути их решения

Согласно статистическим данным за 2018 год правоохранительными органами Российской Федерации было зарегистрировано более 100 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий.[1] По сравнению с 2017 годом количество такого рода преступлений возросло более чем на 33 %. За последние 6 лет киберпреступность, согласно статистике, демонстрирует десятикратный рост. Так, в 2013 году подобных преступлений было порядка 11 тыс., в 2014 г. – 44 тыс., в 2016 г. – более 66 тыс. Динамика совершенных за указанные годы преступлений в цифровом пространстве показана на рисунке 1.

По опубликованным данным, следует, что только с 2015 по 2016 год число мошенничеств в области информационных технологий выросло в 6 раз (с 2,2 до 13,4 тыс.), число краж возросло более чем в 3 раза (с 2,3 до 8,5 тыс.), количество преступлений с использованием глобальной сети «Интернет» и иных инфокоммуникационных технологий возросло в 5,5 раз (с 995 до 5,5 тыс.). Наносимый материальный ущерб только по сравнению с предыдущим годом возрос на 33,4 %.

Кроме того, отмечается тенденция снижения уровня раскрываемости преступлений правоохранительными органами (в среднем на 2 %), что является следствием вновь организующихся форм правонарушений в этой области и недостатком применения мер по противодействию им. Удельный вес преступлений с использованием инфокоммуникационных технологий от общего числа зарегистрированных за 2018 год преступлений составляет 8,1 %.

Данная статистика наглядно показывает необходимость решения проблем противодействия преступности в глобальной сети «Интернет» и своевременного принятия мер по предупреждению киберпреступлений.

[1] Информационно-аналитический портал правовой статистики Генеральной прокурату- ры РФ. URL: http://crimestat.ru/analytics (дата обращения: 12.04.2020).

Актуальность данной темы также обусловлена множеством выявленных фактов нарушения целостности и конфиденциальностиданных, в том числе утечкой информации в сеть «Интернет». Так, в апреле 2019 года согласно сведениям информационного портала «ItSec – Информационная безопасность»[1], неправомерно был обнародован реестр лиц, сформированный банковскими структурами в соответствии с требованиями Федерального закона от 7 августа 2001 г.№ 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Сложившая ситуация негативно может сказаться на статусе лиц, входящих в обнародованный список, а также подорвать экономическую ситуацию страны в целом.

Решение проблемы кроется не только в шифровании информации и использовании сертифицированных средств криптографической защиты информации, но и в грамотном подходе к проектированию систем защиты информации, повышению ответственности за несоблюдение условий конфиденциальности. Преступления такого рода подпадают под статью о незаконном получении и разглашении сведений, составляющих банковскую тайну, и влекут за собой ответственность в виде лишения свободы сроком до семи лет.

Основными проблемами противодействия преступности в сети «Интернет» на сегодняшний день являются:

1. Низкое количество сообщений от потерпевших в правоохранительные органы о совершении преступлений с использованием инфокоммуникационных технологий.
2. Недостаточный уровень квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий.
3. Недостаточное финансирование сферы противодействия киберпреступлениям (проблема оснащения подразделений, занимающихся

[1] Всестороннее исследование проблемы киберпреступности. Официальный Интернет-портал Управления ООН по наркотикам и преступлениям. URL: www. unodc.org/documents/organized-crime/cybercrime/cybercrime_study_210213.pdf (датаобращения: 12.04.2020).

раскрытием киберпреступлений, современными техническими средствами).

4. Нарушение прав на неприкосновенность частной жизни при расследовании киберпреступлений.

5. Наличие лишь общезаконодательных мер и отсутствие положений, наиболее полно рассматривающих порядок расследования преступлений в сети «Интернет».

6. Идентификация преступников в случаях, когда преступление совершено с использованием незащищенной сети передачи данных (открытые Wi-Fi сети, локальные сети предприятий, облачные хранилища и пр.).

7. Недостаточный уровень стратегически спланированных мер по предотвращению преступлений в сети «Интернет».

Согласно опубликованному всестороннему исследованию проблем киберпреступности Управления Организации Объединенных Наций по наркотикам и преступлениям (далее – УНП ООН)[1] в среднем по всему миру в правоохранительные органы обращается лишь 1 % жертв преступных посягательств в области информационных технологий, в ряде международных исследований частного сектора приводится статистика об обращении лишь 20 % лиц, ставших жертва- ми киберпреступлений.

Часто бездействие потерпевших обусловливается безосновательным предположением о крайне низкой вероятности раскрытия преступления. Кроме того, в случае обращения в правоохранительные органы потерпевшие зачастую не могут предоставить минимально необходимые данные и электронные доказательства для создания картины рас- следования (точки доступа к данным, параметры входа в сеть, учетные данные и пр.), что является следствием пока еще низкого уровня просвещенности населения в области информационно-коммуникационных

[1]Всестороннееисследованиепроблемыкиберпреступности.ОфициальныйИнтернет-портал Управления ООН по наркотикам и преступлениям. URL: www. unodc.org/documents/organized-crime/cybercrime/cybercrime_study_210213.pdf (датаобращения:12.04.2019).

технологий, в частности, в странах с низким показателем индексачеловеческого развития. Также, как отмечается в некоторых источниках, крупные компании и корпорации не желают сообщать в правоохранительные органы о совершенных преступлениях в сети«Интернет» в связи с действующей репутационной политикой.

В связи с этим предлагается повышать уровень информированности населения, активизировать просветительскую деятельность, отдельные виды преступлений, в частности, расследования в отношении крупных корпораций и компаний следует брать под особый контроль с учетом сохранения репутационной политики.

Недостаточный уровень квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий, обусловлен цифровой революцией. Часто обучение специалистов осуществляется с большим временным отрывом, что особенно заметно в данной области в условиях глобализации. Для определения уровня развития ведомств по раскрытию преступлений в глобальной сети «Интернет» введен показатель – количество специалистов на 100 тыс. пользователей[1]. Так, в развитых странах, согласно данным, приводимым УНП ООН, показатель варьируется в пределах от 0,4 до 1, в менее развитых странах показатель достигает 0,2. Отдельной проблемой является отставание стран в сфере высоких технологий (например, по индексу развития человеческого потенциала), как следствие, уровень национальной информационнойбезопасности таких стран обеспечивается недостаточно.

Решение данной проблемы кроется в разработке образовательных программ с учетом необходимости изучения не только основ информационной безопасности на правовом и организационном уровнях, но и с учетом специфики киберпреступлений на техническом уровне –

[1]Всестороннееисследованиепроблемыкиберпреступности.ОфициальныйИнтернет-портал Управления ООН по наркотикам и преступлениям. URL: www. unodc.org/documents/organized-crime/cybercrime/cybercrime_study_210213.pdf (датаобращения:12.04.2020).

физическом, аппаратном, программном и криптографическом. При подготовке специалистов отдельно следует рассматривать компьютерную криминалистику (форензику), уделять внимание методам сбора цифровых доказательств, изучению фреймворков для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках, анализу сетевого взаимодействия, средств извлечения ин- формации с исследуемых образов операционных систем, жестких дисков и энергозависимой памяти, средств изучения машинных носителей информации, цифровых устройств и тому подобных элементов.

Отдельной проблемой является недостаточный уровень оснащения подразделений, занимающихся раскрытием киберпреступлений, современными техническими средствами, например:

– средствами выемки аппаратного обеспечения и электронных доказательств;

– средствами создания электронных образов и хэш-кодов, восстановления данных по «отпечаткам» в памяти жестких дисков, обработки и расшифровки данных;

– средствами удаленной экспертизы оборудования и уничтожения информации.

Увеличение финансирования этой области является, пожалуй, неотъемлемым условием повышения качества раскрытия киберпреступлений. Кроме того, получение правоохранительными органами электронных доказательств от поставщиков услуг сети «Интернет» часто требует дополнительных вмешательств, связанных с оформлением документов, разрешающих сбор, обработку и перехват интересующей информации. В Российской Федерации признание электронных доказательств введено лишь с 1 января 2017 года. Так, в качестве доказательств допустимо использовать письменные и вещественные доказательства, сведения в виде аудиозаписей и видеоматериалов, в том числе электронную переписку.

Согласно ч. 3 ст. 75 Арбитражного процессуального кодекса Российской Федерации от 24 июля 2002 г. № 95-ФЗ в качестве письменных доказательств допускаются документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием глобальной сети «Интернет». Также в качестве доказательств допустимо использовать документы, подписанные электронной цифровой подписью.[1]

Использование клавиатурных шпионов, программного обеспечения удаленного администрирования и программ сбора данных является вмешательством в частную личную жизнь, лишь ряд международных документов (МСЭ/КАРИКОМ/КСЭ) предусматривает порядок проведения удаленной судебной экспертизы сотрудниками правоохранительных органов и экспертами. Для исключения трудностей передачи данных от оператора-обработчика конфиденциальных данных целесообразно пересмотреть механизм предоставления данных.

Отдельной проблемой является невозможность или сложность получения экстерриториальных данных, информации, хранящейся на серверах иностранных государств и находящейся вне юрисдикции следственных органов.[2] В этих целях целесообразно налаживать связь с поставщиками услуг и разработчиками информационных систем, обладающими правами использования, хранения и обработки данных о пользователях, в том числе о совершаемых ими действиях.

Часто при получении запросов от правоохранительных органов Интернет-провайдеры и поставщики услуг ссылаются на нормы права, ограничивающие передачу конфиденциальных данных. Под передаваемыми данными понимаются IP-адреса, истории соединений, точки доступа, истории сеансов, идентификационные данные, переписки, cookie-файлы, информация об используемом пользователем устройстве и

[1] Арбитражный процессуальный кодекс РФ от 24 июля 2002 г. № 95-ФЗ // СПС «Консультант- Плюс».(дата обращения: 15.04.2020)

[2] Харисова, З. И. Международно-правовые основы информационной безопасности в целях устойчивого развития // Правовое обеспечение развития социального государства в свете целей устойчивого развития: сборник материалов Международной научно-практической конференции. Уфа: РИЦ БашГУ, 2018.

его параметрах, данные о местоположении, так называемые артефакты. Как правило, передача данных производится на основании официальных запросов, что требует значительных усилий специалистов по оформлению всех необходимых для этого документов и продолжительного времени.

Встречаются случаи, когда невозможность причисления отдельных форм преступлений в цифровом пространстве к существующим правовым нормам затрудняет и затягивает ход расследуемого дела. Так, невзирая на наличие общезаконодательных мер, отсутствуют положения, рассматривающие подкатегории киберпреступлений в отдельности, по степени нанесения вреда и пр., в связи с этим намечается необходимость проведения мониторинга совершаемых киберпреступлений с целью выработки объективных законодательных мер.

Отдельной проблемой является идентификация преступников в случаях, когда преступление совершено с использованием незащищенной сети передачи данных (открытые Wi-Fi сети, локальные сети предприятий, облачные хранилища и пр.).

Несмотря на то что на сегодняшний день практически все общественные сети используют идентификацию абонента, вероятность подмены учетных данных все равно остается. Ежедневно совершаются сотни преступлений с использованием подменных учетных данных, как правило, ситуации такого родавозникают по халатности самих пользователей-потерпевших.

В качестве примера можно привести сохраненные связки учетных данных в общественной точке доступа, использование несертифицированного программного обеспечения персональных компьютеров, а также мобильных устройств. Определенную опасность несут неаттестованные информационные системы предприятий, нешифрованные локальные и облачные хранилища без использования специализированного криптографического программного обеспечения.

Как показывает статистика, раскрытие преступлений, связанных с внедрением злоумышленников в локальные сети и облачные хранилища

при отсутствии защищенного с помощью сертифицированных технических и программных средств сегмента сети и несоблюдении требований информационной безопасности, практически сводится к нулю.

Поскольку сеть «Интернет» посредством глобального адресного пространства связывает между собой множество информационных систем и сетей электросвязи всех стран и предоставляет возможность коммуникации лиц с помощью протокола передачи данных, постольку важно обеспечивать надлежащее функционирование данной сети для предотвращения в целях, противоречащих концепциям информационной безопасности. Кроме того, важна своевременность введения поправок в Стратегию национальной безопасности[1] и План реализации мероприятий по ее укреплению. В этих целях разработана концепция безопасного функционирования и развития сети «Интернет» (проект концепции Конвенции ООН)[2], где приводятся принципы поведения государств по управлению глобальной сетью «Интернет» и оказанию содействия.

В последние годы виды преступлений в сфере информационных технологий качественно меняются и продолжают непрерывно эволюционировать, становясь высокоорганизованными и более изощрёнными. Возрастает также техническая оснащенность преступников, в связи со стремительным развитием информационных технологий появляются новые способы совершения противоправных деяний, а это диктует необходимость принятия незамедлительных и адекватных мер по противодействию преступлениям в сфере обращения цифровой информации, развития компьютерной криминалистики (форензики) и своевременному внесению изменений в программы обучения специалистов по раскрытию преступлений в области инфокоммуникационных

[1] Харисова, З. И. О некоторых проблемах обеспечения информационной безопасности госу- дарства и общества от современных киберугроз // Актуальные проблемы права и государства в XXI веке: сборник материалов XI Международной научно-практической конференции (г. Уфа, 18 апреля 2019 г.). Уфа: Уфимский ЮИ МВД России, 2019.

[2] Проект-концепция конвенции ООН − концепции безопасного функционирования и разви- тия сети «Интернет». Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций РФ. URL: https://digital.gov.ru/ru/events/36739/ (дата обращения: 12.04.2019).

технологий, в частности, в глобальной сети «Интернет».

Рассмотренные методы раскрытия наиболее часто встречающихся в настоящее время киберпреступлений предлагаются для включения в программы подготовки специалистов в области защиты информации, в том числе специалистов в области правоохранительной деятельности, что будет способствовать решению одной из заявленных проблем противодействия преступности в сети «Интернет» в части обеспечения достаточного уровня квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий. Кроме того, одним из доступных на сегодняшний день методом противодействия киберпреступности является повышение уровня информированности населения в этой сфере. В этих целях возможно решение проблемы, например, в виде размещения на рекламных площадках региона социально направленных баннеров и проведения плановой просветительской работы среди граждан.

ЗАКЛЮЧЕНИЕ

С повышением роли информации во всех сферах деятельности повышается роль и значение компьютерной информации как одной из

самых популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер.

Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных.

Анализируя материал данной дипломной работы можно сделать вывод о необходимости внесения значительного массива дополнений и изменений в действующее законодательство Российской Федерации. Кроме того, требуется издание новых законов вносящих правовое регулирование в информационные отношения.

Недостаток комплексных мер противодействия, их противоречивость и фрагментарность, высокая латентность преступности в сфере компьютерной информации приводят к неэффективности выработанных мер ее предупреждения, обуславливая трудности в противодействии и борьбе с данным видом общественно опасных деяний.

Снижению латентности преступлений в сфере компьютерной информации будет способствовать как международное, так и внутреннее сотрудничество между государством и правоохранительными органами. Разъяснительная работа по поводу необходимость защиты законных интересов в сфере использования и развития информационных технологий; повышение уровня технического оснащения и развитие специальных навыков у сотрудников правоохранительных органов для эффективного выявления подобных преступлений.

Так же необходимо осуществить следующие организационные и правовые меры:

- увеличение штатной численности подразделений, специализирующихся на выявлении и раскрытии преступлений в сфере компьютерной

информации;

- подбор в указанные подразделения специалистов, имеющих исчерпывающие знания в области информационно-телекоммуникационных технологий и дальнейшее постоянное и динамичное совершенствование их квалификации;

- постоянное совершенствование научных методик, программных средств и технических устройств для получения и закрепления доказательств совершения компьютерного преступления в ответ на внедрение новых механизмов и средств передачи данных;

- законодательное ограничение использования пользователями сетей передачи данных различных «анонимайзеров», предоставляющих услуги по маскировке реальных идентификаторов (например, IP-адресов) их оконечного оборудования;

- обязать компании, предоставляющие информационно - телекоммуникационные услуги, разработать реальный механизм идентификации конкретных пользователей в сетях передачи данных, исключив факты присвоения одинаковых динамических IP-адресов массиву оконечных устройств в ограниченный период времени. Ввести обязательный учет уникальных идентификаторов сетевого оборудования (IMEI, MAC-адресов), используемого конечными пользователями;

- ужесточить ответственность за отсутствие либо внесение заведомо недостоверных сведений о пользователях информационно - телекоммуникационными услугами и услугами связи, предоставляемыми на территории Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: офиц. текст // Собр.

законодательства Рос. Федерации. – 2014. – № 15. – Ст. 1691.

2. Уголовный кодекс Российской Федерации [Электронный ресурс]: федер. закон: [принят Гос. Думой 24 мая 1996 г.: по состоянию на 18 февраля 2019 г.] // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru. Уголовно-процессуальныйкодекс Российской Федерации [Электронный ресурс]: федер. закон: [принят Гос. Думой 22 ноября 2001 г.: по состоянию на 18 февраля 2019 г.] // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru.
3. О банках и банковской деятельности: федер. закон от 2 декабря 1990 г. № 395-1 // Собр. законодательства Рос. Федерации. – 1996. – № 6. – Ст. 492.
4. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ // Собр. законодательства Рос. Федерации. – 2003. – № 28. – Ст. 2895.
5. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (Ч. 1). – Ст. 3448. О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ // Собр.законодательства Рос. Федерации. – 2011. – № 7. – Ст. 900.
6. Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации: постановление Правительства Рос. Федерации от 31 июля 2014 г. № 743 // Собр. законодательства Рос. Федерации. – 2014. – № 32. – Ст. 4516.
7. Об утверждении Правил уведомления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале осуществления деятельности по обеспечению функционирования информационных

систем и (или) программ для электронных вычислительных машин, предназначенных и (или) используемых для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети «Интер- нет», а также ведения реестра указанных организаторов : постановление Правительства Рос. Федерации от 31 июля 2014 № 746 // Собр. законодательства Рос. Федерации. – 2014. – № 32. – Ст. 4519.

8. Об утверждении Правил хранения организатором распространения информации в информационно-телекоммуникационной сети«Интернет» текстовых сообщений пользователей информационно-телекоммуникационной сети «Интернет», голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет»: постановление Правительства Рос. Федерации от 26 июня 2018 г.№ 728 // Собр. законодательства Рос. Федерации. – 2018. – № 27. – Ст. 4081.
9. Об основах организации ведомственного контроля за деятельностью органов внутренних дел Российской Федерации: приказ МВД России от 3 февраля 2012 г. № 77.
10. Об организации рассмотрения сообщений об отдельных видах преступлений экономической направленности: приказ МВД России от 1 декабря 2016 г. № 785.
11. Об утверждении Требований к оборудованию и программ- но-техническим средствам, используемым организатором распространения информации в сети «Интернет» в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими оперативно- розыскную деятельность или обеспечение безопасности Российской Федерации, мероприятий в целях реализации возложенных на них задач [Электронный ресурс] : приказ Минкомсвязи России от 29 октября 2018 г. № 571 // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа:

http://www.consultant.ru.

12. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru.

Монографии, учебники, учебные пособия

13. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.
14. Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2017. – № 4. – С. 45–50.
15. Грибунов О. П. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие / О. П. Грибунов, М. В. Старчиков. – М. : ДГСК МВД России, 2017. – 159 с.
16. Климов Д. В. Расследование хищений, связанных с использованием сети «Интернет»: учеб. пособие / Д. В. Климов. – Н. Новгород.: Нижегородская академия МВД России, 2017. – 24 с.
17. Основы теории электронных доказательств: монография / под ред. С. В. Зуева. – М. :Юрлитинформ, 2019. – 400 с.
18. Петров В. А. Выявление, квалификация и организация расследования преступлений, совершенных с использованием криптовалюты : учеб.-метод. пособие / В. А. Петрова. – М. :Юрлитинформ, 2017. – 200 с.
19. Расследование мошенничества в сфере компьютерной информации: учеб. пособие / авт.-сост. П. А. Капустюк [и др.]. – Иркутск: Восточно-Сибирский ин-т МВД России, 2018. – 47 с.
20. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них: учеб. пособие / А. А. Кузнецов [и др.]. – Омск: Омская академия МВД России, 2015. – 115 с.

21. Электронные носители информации в криминалистике: моно- графия / под ред. О. С. Кучина. – М.: Юрлитинформ, 2017. – 304 с.

Статьи, научные публикации

22. Смирнов Игорь Смирнов Игорь Владимирович Партнерство Сбербанка и Университета МВД в борьбе с киберпреступностью // Вестник экономической безопасности. 2018. №3. URL: https://cyberleninka.ru/article/n/partnerstvo-sberbanka-i-universiteta-mvd-v-borbe-s-kiberprestupnostyu (дата обращения: 14.03.2020).
23. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки Казанского юридического института МВД России. 2016. №1 (1). URL: https://cyberleninka.ru/article/n/osobennosti-raskrytiya-i-rassledovaniya-kiberprestupleniy-problemy-i-puti-resheniya (дата обращения: 14.06.2020).
24. Никеров Дмитрий Михайлович, Хохлова Ольга Михайловна Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2019. №2 (89). URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-vysokih-tehnologiy-v-sovremennoy-rossii (дата обращения: 14.06.2020).
25. Мазуров Валерий Анатольевич Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции // Вестн. Том. гос. ун-та. 2007. №300-1. URL: https://cyberleninka.ru/article/n/prestupnost-v-sfere-vysokih-tehnologiy-ponyatie-obschaya-harakteristika-tendentsii (дата обращения: 14.06.2020).
26. Жиделев Василий Геннадьевич Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник Удмуртского университета. Серия «Экономика и право». 2011. №4. URL: https://cyberleninka.ru/article/n/evolyutsiya-zakonodatelstva-ob-ugolovnoy-otvetstvennosti-za-sovershenie-prestupleniy-v-sfere-vysokih-tehnologiy (дата

обращения: 14.06.2020).

27. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. URL: https://cyberleninka.ru/article/n/istoriya-i-zarubezhnyy-opyt-pravovoy-reglamentatsii-kompyuternoy-prestupnosti (дата обращения: 14.06.2020).
28. Комиссарова Ярослава Владимировна Понятие и классификация следов в криминалистике // Вестник Университета имени О.Е. Кутафина. 2019. №3 (55). URL: https://cyberleninka.ru/article/n/ponyatie-i-klassifikatsiya-sledov-v-kriminalistike (дата обращения: 14.06.2020).
29. Смирнова Ирина Георгиевна, Коломинов Вячеслав Валентинович Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // BaikalResearchJournal. 2015. №3. URL: https://cyberleninka.ru/article/n/takticheskie-osobennosti-proizvodstva-doprosa-po-delam-o-prestupleniyah-v-sfere-kompyuternoy-informatsii (дата обращения: 14.06.2020).

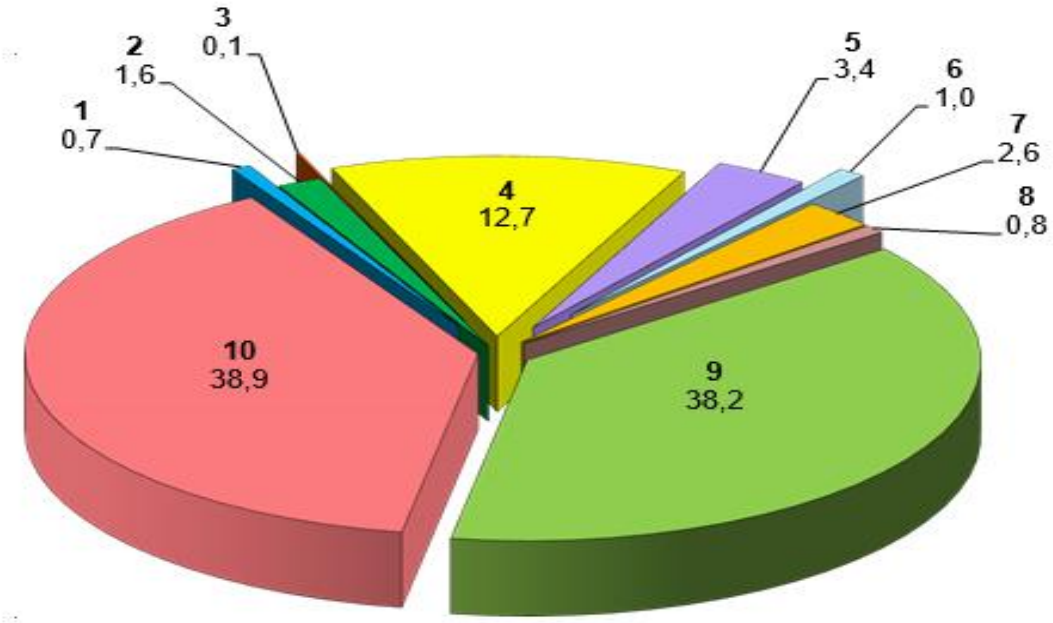
Эмпирические материалы (материалы судебной и следственной практики и т.д.)

Рис. 1.1

СОСТОЯНИЕ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

СТРУКТУРА ПРЕСТУПНОСТИ (в %)

январь – декабрь 2019г.



1 - взяточничество
2 - убийство, умышленное причинение тяжкого вреда здоровью, изнасилование
3 - хулиганство
4 - мошенничество
5 - нарушение правил дорожного движения лицом, подвергнутым административному наказанию
6 - нарушение правил дорожного движения и эксплуатации транспортных средств
7 - грабеж, разбой
8 - присвоение или растрата
9 - кража
10 - прочие

Рис.1.2

СВЕДЕНИЯ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С

ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ(за январь-декабрь 2019г.)

	ЗАРЕГИСТРИРОВАНО		в том числе		
			выявленных сотрудниками		
	Всего	+,- в %	СО СК РФ	ОВД РФ	ФСБ РФ
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий	**294409**	**68,5**	**1111**	**289796**	**1881**
из них					
тяжких и особо тяжких	142728	149	648	140475	876
в том числе совершенных с использованием или применением:					
расчетных (пластиковых) карт	34383	109,3	133	33966	163
компьютерной техники	18261	21,5	171	17269	466
программных средств	6283	43,6	68	5823	273
фиктивных электронных платежей	984	101,2	4	966	7
сети "Интернет"	157036	45,4	722	154151	1111
средств мобильной связи	116154	89,5	235	115358	284
в том числе					
кража ст. 158 УК РФ	98798	202,4	185	98431	28
мошенничество ст. 159 УК РФ	119903	32,2	55	119485	117
мошенничество с использованием платежных карт ст. 159.3 УК РФ	16119	280	27	16056	11
мошенничество в сфере компьютерной информации ст. 159.6 УК РФ	687	-29,2	0	676	7

незаконные организация и проведение азартных игр ст. 171.2 УК РФ	842	-3,8	26	766	22
публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма ст. 205.2 УК РФ	212	25,4	0	84	120
незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества ст. 228.1 УК РФ	24677	31,2	171	24027	281
изготовление порнографических материалов ст. 242, 242.1, 242.2 УК РФ	1916	30,5	82	1805	0
публичные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ	257	1,6	4	108	124
преступления в сфере компьютерной информации глава 28 УК РФ	2883	15,3	5	2562	270
в том числе					
неправомерный доступ к компьютерной информации ст. 272 УК РФ	2420	37,4	5	2211	162
создание, использование и распространение вредоносных компьютерных программ ст. 273 УК РФ	455	-37,9	0	350	101

Окончание таблицы

Из числа находившихся в производстве												Выявлено лиц, совершивших преступления (по наиболее тяжкому)	
РАСКРЫТО		в том числе						раскрыва-емость	НЕ РАСКРЫТО			
		СО СК РФ	ОВД РФ	ФСБ РФ	уголовные дела о которых направлены в суд с обвинительным заключением, обвинительным актом, обвинительным постановлением							
	+,-					+,-	уд. вес от			+,-		+,-
Всего	в %				Всего	в %	раскрытых в %		Всего	в %	Всего	в %
65238	**50,4**	**8812**	**55585**	**808**	**57221**	**55,6**	**87,7**	**24**	**206594**	**72,5**	**44158**	**84**
38599	98	5423	32843	333	37961	97,6	98,3	30,2	89097	244,2	27301	153,3
14182	114,7	1056	13118	8	11499	123,7	81,1	44,7	17547	133,6	11438	130,7
6553	37,5	2517	3768	260	5201	38,3	79,4	39,3	10116	54,2	2876	73,6
2463	28,7	904	1426	125	1934	31,7	78,5	45,5	2949	49,6	1149	70,2
237	104,3	68	166	3	218	101,9	92	28,8	585	104,5	136	81,3
35181	41,9	5359	29187	613	31273	44,8	88,9	24,1	110953	47	20656	57,9
16339	50,5	1157	15083	99	14969	61,1	91,6	15,5	88788	86,4	11307	73,2
21009	101,9	1609	19400	0	19768	142,8	94,1	23,7	67503	273,5	18670	135
9798	7	351	9436	11	8040	6,7	82,1	8,6	104145	29,5	3556	22
4794	722,3	101	4693	0	2971	667,7	62	33,3	9581	276,2	3789	720,1
66	-46,3	1	62	3	54	-30,8	81,8	8,7	690	-23,2	69	3
724	0,6	722	2	0	470	4,4	64,9	85,8	120	13,2	1290	12,9

145	10,7	61	0	84	132	8,2	91	83,3	29	45	100	26,6
10220	36,4	711	9395	114	10169	36,3	99,5	45,2	12368	43,5	4769	38,8
1317	21,5	1032	285	0	1268	22,3	96,3	81,3	303	17,9	452	5,6
203	-6	24	1	178	165	-7,3	81,3	89	25	13,6	142	23,5
729	27	163	374	192	468	13,3	64,2	26,1	2064	20,5	319	39,3
483	51,4	119	247	117	311	27,5	64,4	21,1	1802	41,9	186	57,6
234	-7,9	43	123	68	149	-11,3	63,7	47,2	262	-40,6	127	14,4

АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

Казанский юридический институт МВД России

СПРАВКА
о результатах проверки текстового документа на наличие заимствований

Проверка выполнена в системе Антиплагиат.ВУЗ

Автор работы	**Скрябин Никита Алексеевич**
Подразделение	КЮИ МВД России
Тип работы	Выпускная квалификационная работа
Название работы	ВКР Скрябин(изм.2)
Название файла	ВКР Скрябин(изм.2).pdf
Процент заимствования	**28.56 %**
Процент самоцитирования	**0.00 %**
Процент цитирования	**17.11 %**
Процент оригинальности	**54.34 %**
Дата проверки	**22:26:49 30 июня 2020г.**
Модули поиска	Модуль поиска ИПС "Адилет"; Сводная коллекция ЭБС; Коллекция РГБ; Цитирование; Модуль поиска переводных заимствований; Модуль поиска переводных заимствований по elibrary (EnRu); Модуль поиска переводных заимствований по интернет (EnRu); Коллекция eLIBRARY.RU; Коллекция ГАРАНТ; Модуль поиска Интернет; Модуль поиска "КЮИ МВД РФ"; Коллекция Медицина; Сводная коллекция вузов МВД; Модуль поиска перефразирований eLIBRARY.RU; Модуль поиска перефразирований Интернет; Коллекция Патенты; Модуль поиска общеупотребительных выражений; Кольцо вузов
Работу проверил	Усманов Ильгиз Миншакирович
	ФИО проверяющего
Дата подписи	22.06.2020г.

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

РЕЦЕНЗИЯ
на выпускную квалификационную работу
слушателя 051 учебной группы

Скрябина Никиты Алексеевича
на тему «Организационные основы оперативно-розыскной деятельности по раскрытию преступлений, совершаемых с использованием высоких технологий»

В современных условиях жизнедеятельности общества сети Интернет являются основополагающим фактором сферы коммуникаций: с их помощью осуществляются различные операции с денежными средствами (с использованием компьютеров, банкоматов, иных платежных систем), осуществляется поиск различных товаров и услуг, информации. Эти действия напрямую зависят от различных информационных технологий, в результате чего ряд пользователей ежедневно подвергаются атакам со стороны киберпреступников.

Имеющаяся в современных реалиях нормативно-правовая база (правоохранительных органов и иных государственных учреждений, общественных организаций, коммерческих структур, и т. п.) отличается своей разнородностью, следовательно, в вопросах расследования преступлений в сфере высоких технологий неизбежны проблемы взаимодействия в процессе правоприменения, «размытость» правовой базы не позволяет эффективно противодействовать преступности, поэтому совершенствование научного знания, методического обеспечения этого вида деятельности – одна из основных задач правоохранительных органов, государственных и других взаимодействующих структур. Важными и необходимыми элементами научного обеспечения предупреждения преступности является унификация и легитимизация терминов и определений, заметно сужающие возможность их расширительного толкования, включая и процесс правоприменения.

Следует отметить, что научной разработанности данной темы исследования, актуальности, а также ее сложности и многоплановости в науке уделялось существенное внимание.

Заявленная тема автором раскрыта в полном объеме, цели, структура и задачи соответствуют содержанию и теме работы.

При изучении и раскрытии вопросов дипломной работы, автору удалось отразить имеющиеся спорные точки различных авторов, а также отобразить свою позицию, аргументировав ее, что позволяет сделать вывод о том, что теоретический и практический уровень дипломной работы достаточно высок.

Структура работы соответствует теме и поставленным целям, и задачам и состоит из введения, двух глав (объединяющих пять параграфов), заключения, списка использованной литературы и приложений.

Список использованной литературы по данной теме достаточно полный, актуальный и отражает современное состояние исследуемой проблемы. В дипломной работе автором отмечается выработка рекомендаций по совершенствованию нормативной базы.

Среди основных положительных моментов работы следует отметить подробное и детальное изучение ключевых проблем по данной теме, выработке предложений по их решению. В работе автор приводит различные точки зрения на все имеющиеся спорные вопросы и не ограничивается простой констатацией спорности взглядов, которые имеются в современной литературе.

Также следует отметить то, что автором весьма качественно осуществлена подборка материала для изучения рассматриваемой темы, проведение самостоятельного анализа литературы и судебной практики.

Работа логически выстроена, написана научным языком.

Автор работы проявил достаточную степень самостоятельности в подборе и анализе литературы, наличии и обоснованности теоретических и практических выводов и предложений.

Выводы и умозаключения, полученные в результате проведения автором собственного авторского исследования, логически правильно обоснованы и доказаны.

К достоинствам дипломной работы следует отнести четкий, грамотный, понятный стиль изложения, глубокое и тщательное изучение проблем по данной теме и выработке рекомендаций по их решению, оправданную и законченную аргументацию выдвинутых тезисов.

Оформление выпускной квалификационной работы осуществлено в соответствии с предъявленными требованиями, библиография составлена верно и является актуальной для анализа данной проблемы.

Существенных недостатков в работе не выявлено. Работа оставляет положительные впечатления, соответствует всем предъявленным требованиям.

Выпускная квалификационная работа Скрябина Н.А. представляет собой самостоятельное исследование и заслуживает оценки «отлично».

Оценка рецензента Отлично

Рецензент

Начальник ОП№6 «Савиново»
УМВД России по г. Казань
подполковник полиции
Каримов Айрат Генадьевич М.П.

«1» июня 2020 г.

Ознакомлен
Н.А. Скрябин

Ознакомлен
05.06.2020 г. А.Ф. Каримов

Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра оперативно-разыскной деятельности

УТВЕРЖДАЮ

Начальник кафедры
полковник полиции
_____ Е.П. Шляхтин
(подпись)
«____» _____ 20__ г.

ПЛАН-ГРАФИК
выполнения выпускной квалификационной работы

Тема: Организационные основы оперативно-розыскной деятельности по раскрытию преступлений, совершаемых с использованием высоких технологий

Курсант (слушатель): Скрябин Никита Алексеевич (фамилия, имя, отчество) Учебная группа № 051

Специальность 40.05.02 – Правоохранительная деятельность

Форма обучения очная Год набора 2015

№ п/п	Характер работы (главы, параграфы и их содержание)	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1	Изучение литературных источников и иных материалов	10%	До 15.09.2019 года	
2	Составление плана ВКР	10%	До 01.10.2019	
3	Подготовка введения	30%	До 30.11.2019 года	
4	ГЛАВА 1 ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ §1. История возникновения и развития преступлений в сфере высоких технологий §2. Криминалистическая характеристика преступлений §3. Правовая основа и современное состояние преступности в данной сфере	50%	До 31.12.2019 года	
5	ГЛАВА 2 ОРГАНИЗАЦИЯ И ТАКТИКА РАСКРЫТИЯ И РАССЛЕДОВАНИЯ	80%	До 30.01.2020 года	

	ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ §1. Организационно-тактические приемы раскрытия преступлений в сфере высоких технологий §2. Проблемы раскрытия и расследования преступлений в сфере высоких технологий, а также пути их решения			
6	Заключение	90%	До 1.05.2020	
7	Сдача на проверку научному руководителю и Начальнику отдела	100%	До 10.05.2020	

СОГЛАСОВАНО

Руководитель _____

Подпись выпускника _____

«01» 09 20 19 г.

ОТЗЫВ
о ходе выполнения выпускной квалификационной работы

слушателем Скрябин Никита Алексеевич
(фамилия, имя, отчество)
051 группа, 5 курс, правоохранительная деятельность, ФПС ПВО
(№ группы, курс, специальность, факультет)

Тема: «Организационные основы оперативно-розыскной в деятельности по раскрытию преступлений, совершаемых с использованием высоких технологий»

Тема выпускной квалификационной работы «Организационные основы оперативно-розыскной деятельности по раскрытию преступлений, совершаемых с использованием высоких технологий» выбрана слушателем Н.А. Скрябиным из списка тем, предложенного кафедрой. Мотивом в выборе темы послужило актуальность проблемы обусловленная практической и теоретической значимостью вопросов, связанных со становлением и развитием механизмов обеспечения информационной безопасности в России. Открытия в различных областях науки, развитие информационно-коммуникационных технологий, технологическое перевооружение промышленности привели к кардинальным переменам во всем мире, обусловили переход к новому типу общества – информационному.

Цель исследования заключается в комплексном уголовно-правовом и криминологическом научном исследовании состояния, тенденций, характерных черт преступлений в сфере компьютерной информации в Российской Федерации.

Во введении Н.А. Скрябиным обосновывается актуальность темы исследования, показывается степень ее научной разработанности. Определяются цели, объект и предмет. Раскрывается методологическая основа, показывается ее новизна, излагаются основные положения рассматриваемые в работе.

В первой главе «Характеристика преступлений в сфере высоких технологий» дается криминалистическая характеристика мошенничества,. Рассматриваются история возникновения и развития преступлений в сфере высоких технологий, правовая основа и современное состояние преступности в данной сфере

Во второй главе «Организация и тактика раскрытия и расследования преступлений в сфере высоких технологий» подробно рассмотрены вопросы раскрытия и расследования преступлений в сфере высоких технологий, а также пути их решения.

В заключении излагаются основные выводы и предложения, направленные на совершенствование организации и тактики раскрытия рассматриваемых видов преступлений.

Таким образом, следует отметить, что выпускная квалификационная работа Н.А. Скрябина имеет выраженный исследовательский характер. В ней автором грамотно изложена теоретическая часть, которая имеет логичное и последовательное изложение материала с соответствующими выводами и обоснованными предложениями.

Методологическую основу работы составляют общенаучные (диалектический, системный), частные (формально-юридический, системно-структурный, описательно-аналитический, статистический) методы исследования.

Цели и задачи слушателем определены самостоятельно в соответствии с темой дипломной работы, работа написана доступным языком легким для восприятия.

В целом, анализ выпускной квалификационной работы Н.А. Скрябина показывает его не плохие знания вопросов исследуемой темы. В своей работе он уверенно оперирует данными научной литературы профессиональной направленности, свободно ориентируется в источниках права и использует методы системного анализа.

Недостатком представленной выпускной квалификационной работы является отсутствие эмпирической базы исследования.

К плюсам данной работы можно отнести качественную проработку имеющихся по данной проблеме научных источников, умелое оперирование юридическими терминами и категориями в тексте представленной работы.

Автором выпускной квалификационной работы изучен опыт оперативных подразделений полиции, проанализирован комплекс оперативно-профилактических и розыскных мероприятий по данному направлению работы. Н.А. Скрябин исследовал состояние, тенденции, характерные черты преступлений в сфере компьютерной информации в Российской Федерации. Это позволило ему сформулировать ряд основных выводов, решение которых по ее мнению, будет способствовать совершенствованию существующих методов воздействия на данное общественно опасное явление с учётом специфики информационных технологий.

После выбора и утверждения темы выпускной квалификационной работы Н.А. Скрябина совместно с научным руководителем был составлен план выпускной квалификационной работы. Все параграфы и главы автором работы представлялись для проверки научному руководителю строго в установленные сроки. После проверки научным руководителем структурных частей дипломной работы Н.А. Скрябин добросовестно устранял имеющиеся недостатки.

В ходе написания работы Н.А. Скрябин показал уверенное владение компьютерными методами сбора, хранения и обработки информации, применяемой в сфере профессиональной деятельности. Умение и навыки работы с компьютерными программами (Word, PowerPoint, Excel и т.п.),

информационно-справочными ресурсами, работы в системе интернет.

С учетом изложенного полагал бы необходимым сделать вывод, что выпускная квалификационная работа «Организация и тактика раскрытия мошенничеств, совершенных в сети «Интернет» оперативными подразделениями ОВД» представленная слушателем Н.А. Скрябиным в достаточной степени является актуальной обладает новизной темы, план составлен грамотно и соответствует выбранной теме, структура работы выдержана, цели поставленные в работе достигнуты, работа написана научным языком легким для восприятия, теоретически проанализирована, выполнена самостоятельно автором в срок. Выводы и предложения могут быть использованы для совершенствования практической направленности оперативных подразделений. При написании работы были использованы нормативные акты и другие литературные источники, что позволило слушателю решить поставленные цели, к каждому параграфу имеются обоснованные выводы, а в конце работы логическое заключение. Работа оформлена в соответствии с требованиями, предъявляемыми к работам такого рода.

С учетом изложенного и итогов ее устного выступления во время защиты, полагал бы необходимым выпускную квалификационную работу Н.А. Скрябина оценить на оценку «отлично».

Оценка «отлично» (которая может быть изменена с учетом результатов устной защиты выпускной квалификационной работы Н.А. Скрябина).

Руководитель выпускной
квалификационной работы

Кандидат юридических наук, доцент,
(ученая степень, ученое звание,
доцент кафедры ОРД КЮИ МВД России,
должность, специальное звание)
подполковник полиции — И.М. Усманов
(подпись) (инициалы, фамилия)

«01» июля 2020 г.

Подпись И.М. Усманова
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

Ознакомлен
03.07.2020 Н.А. Скрябин