МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тюменский институт повышения квалификации
сотрудников МВД России

А.Ю. Коптяев

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Тюмень
2022

УДК 343.985.7:004
ББК 67.99(2)94
К 65

Рекомендовано к изданию редакционно-издательским советом
Тюменского института повышения квалификации сотрудников МВД России

Рецензенты:
профессор кафедры организации следственной работы УНК по ПС в ОВД
Волгоградской академии МВД России кандидат юридических наук, доцент *С.А. Янин;*
начальник кафедры информационного обеспечения органов внутренних дел
Уральского юридического института МВД России *А.П. Леонов*

Коптяев А.Ю.

К 65 Расследование преступлений, совершённых с использованием современных информационно-коммуникационных технологий: учебное пособие. Тюмень: Тюменский институт повышения квалификации сотрудников МВД России, 2022. 78 с.

ISBN 978-5-93160-331-5

В учебном пособии рассматриваются вопросы, связанные с расследованием преступлений, совершённых с использованием современных информационно-коммуникационных технологий. Представлена методика и тактика расследования преступлений данной категории.

Адресовано профессорско-преподавательскому составу образовательных организаций системы МВД России, слушателям, обучающимся по основным программам профессионального обучения – программам профессиональной подготовки по должности служащего «Полицейский», по дополнительным профессиональным программам, реализуемым для сотрудников органов внутренних дел, с целью использования на занятиях лекционного и семинарского типа по дисциплинам «Криминалистика», «Уголовный процесс», «Уголовное право», «Информационные технологии».

УДК 343.985.7:004
ББК 67.99(2)94

ISBN 978-5-93160-331-5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Современный мир характеризуется формированием информационных систем. Чем более развитым является государство, тем активнее в нем идет процесс цифровизации, использования мобильной связи, компьютерной техники и совершенствования электронных услуг. Информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан.

Однако цифровизация, рост технологий, инновационные достижения, как известно, создают дополнительные риски и угрозы, в том числе криминогенного характера. Эти и другие глобальные изменения в сфере информационных технологий влияют и на состояние преступности.

В последние годы констатируется рост числа преступлений, совершённых в сфере высоких технологий. Согласно официальным статистическим данным МВД России, в I полугодии 2022 г. зарегистрировано 249,0 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий. В общем числе зарегистрированных преступлений их удельный вес составляет 24,8 %. Больше половины таких преступлений (53 %) относится к категориям тяжких и особо тяжких, 73,3 % – совершается с использованием сети «Интернет», 38,2 % – средств мобильной связи. Почти три четверти таких преступлений (70,2 %) совершается путем кражи или мошенничества, каждое восьмое (12,4 %) – с целью незаконного производства, сбыта или пересылки наркотических средств[1].

Различные информационные технологии становятся орудием совершения тяжких и особо тяжких преступлений как общеуголовной направленности, так и в области экономической сферы.

Характерным признаком совершения преступлений в сфере информационно-коммуникационных технологий (ИКТ) является использование различных новейших достижений науки и техники посредством обладания определенными специальными познаниями, что в свою очередь усложняет расследование уголовных дел данной категории, поскольку зачастую у субъектов расследования отсутствуют базовые знания в сфере информационных технологий. Раскрытие таких преступлений вызывает трудности еще и потому, что компьютерная техника и глобальные цифровые системы позволяют лицам, совершающим преступления данной категории, действовать анонимно, совершать преступления с территории других государств.

Например, в рамках действующего законодательства Российской Федерации отсутствует запрет на использование виртуальных частных сетей (VPN), которые делают пребывание в Интернете конфиденциальным. Нередко с помощью указанных технологий правонарушители пытаются совершать кражи личных данных граждан, при этом оставаясь не замеченными

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-июнь 2022 года: сайт ГИАЦ МВД России. URL: https://мвд.рф (дата обращения: 20.07.2022).

для провайдеров, которые обеспечивают соединение с Интернетом. В результате использования технологий (VPN) провайдер не знает о действиях пользователей в Интернете, а сайты, посещаемые ими, видят адрес (VPN) сервиса вместо адресов пользователей. Причем эти серверы находятся по всему миру, поэтому правонарушители легко меняют свое виртуальное местоположение.

Приведенные выше статистические данные и имеющиеся проблемы нормативно-правового регулирования в указанной сфере, а также особенности расследования преступлений этой направленности свидетельствуют о необходимости актуализации борьбы с преступностью в сфере информационно-коммуникационных технологий, принятия исчерпывающих мер по эффективному раскрытию и расследованию данных преступлений и необходимости осуществления своевременных и эффективных мер по предотвращению таких преступлений.

Предпринимаемые МВД России меры по раскрытию, расследованию и предотвращению преступлений данной категории и взаимодействие с другими правоохранительными ведомствами свидетельствуют о том, что оперативная обстановка во всех субъектах Российской Федерации остается стабильной и контролируемой.

Однако, несмотря на принимаемые меры органами законодательной и исполнительной власти по противодействию и борьбе с преступлениями в сфере информационно-коммуникационных технологий, существует ряд вопросов, подлежащих разрешению, а именно: определение понятийного аппарата, например, что относится к преступлениям в сфере информационно-коммуникационных технологий, к киберпреступности, к преступлениям в сфере высоких технологий или в сфере информационно-телекоммуникационных технологий. В правоприменительной практике до сих пор остаются актуальными вопросы общей характеристики преступлений в сфере компьютерной информации, квалификации преступлений данного вида, тактики и методики расследования преступлений в сфере информационно-коммуникационных технологий.

Настоящее учебное пособие направленно на формирование у слушателей образовательных организаций системы МВД России знаний, умений по выявлению преступлений, совершённых с использованием информационно-коммуникационных технологий, их квалификации с учетом требований действующего законодательства, сложившейся правоприменительной практики, методики и тактики их расследования.

ГЛАВА 1. ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Понятие и характеристика преступлений в сфере информационно-коммуникационных технологий, их классификация

Развитие и активное внедрение в жизнь информационных технологий, к сожалению, порождает не только блага для людей, использующих данные технологии, но и создает новые виды преступности, в частности преступления в сфере информационно-коммуникационных технологий. Использование технических средств позволяет преступным лицам эффективно координировать свои действия, применять такие способы совершения преступлений, которые ранее были не известны уголовному праву. В частности, злоумышленники из состава групп, созданных с использованием сети «Интернет», могут не иметь информации о других членах группы и никогда не встречаться с ними[2], что создает ряд трудностей при расследовании преступлений этой категории.

Принимая во внимание сложность расследования данных преступлений, а также появление новых видов и форм их совершения, для правильного применения норм уголовного законодательства необходимо определить понятийный аппарат, иными словами, критерии и характерные признаки, при наличии которых совершённое преступление следует классифицировать как преступление, относящееся к сфере информационно-коммуникационных технологий.

В юридической литературе преступления, совершаемые в сфере информационно-коммуникационных технологий, толкуются неоднозначно и понимаются по-разному. Различие в толковании данного вида преступлений, на наш взгляд, связанно не только с терминологией «кому как нравится наименовать подобный вид преступления», но и с тем, что в законодательстве официальное закрепление получила только одна группа деяний, предусмотренная в главе 28 Уголовного кодекса Российской Федерации[3] «Преступления в сфере компьютерной информации». В некоторых других статьях Особенной части УК РФ данный вид преступления предусмотрен в качестве квалифицирующего признака – совершённое с использованием информационно-телекоммуникационных технологий.

В научной литературе, правоприменительной практике и средствах массовой информации используются различные понятия преступлений данного вида, в частности понятия «преступления, свершенные с использованием информационно-коммуникационных технологий», «преступления, со-

[2] См.: Тропина Т.Л. Борьба с киберпреступностью: Возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86.

[3] Далее – УК РФ.

вершаемые при помощи телекоммуникационных сетей, включая сеть “Интернет”», «киберпреступления», «компьютерные преступления», «преступления в сфере компьютерной информации»[4].

Учеными-правоведами предпринимаются попытки выработать и закрепить единую терминологию понимания данных видов преступлений. Проблема выработки дефиниции вызвана отсутствием однообразного подхода относительно круга деяний, которые следует определять как преступления, совершаемые в сфере информационно-коммуникационных технологий.

Например, первое определение киберпреступности отражено в рекомендациях экспертов ООН, где термин «киберпреступность» характеризуется как преступление, совершённое с использованием компьютерной системы или глобальной сети, внутри компьютерной системы или сети, а также против компьютерной системы или сети[5].

В законодательстве Российской Федерации в настоящий момент официально не закреплено понятие «киберпреступность», что влечет различное и неоднозначное понимание внутреннего содержания данного определения и неоднозначное понимание преступлений в сфере информационно-коммуникационных технологий.

В научной литературе высказываются различные трактовки понятия киберпреступности. Например, И.М. Рассолов считает, что к киберпреступности относятся преступления, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете[6]. Аналогичной точки зрения придерживается М.М. Сериева, определяя киберпреступность как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем и компьютерных сетей[7].

Анализ научной и юридической литературы показывает, что понятие преступлений в сфере информационно-коммуникационных технологий шире понятий киберпреступности, преступлений, совершаемых посредством телекоммуникационных сетей, и преступлений в сфере компьютерной информации.

Для понимания единого толкования понятия преступлений в сфере информационно-коммуникационных технологий необходимо определить поня-

---

[4] См.: Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / А.Ф. Абдулвалиев [и др.]. Тюмень: Изд-во ТюмГУ, 2021 С. 230-231.

[5] Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями: док. ООН A/CONF.187/1.

[6] Рассолов И.М. Право и Интернет. Теоретические проблемы. М.: Норма, 2009. С. 132-133.

[7] См.: Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. № 1 (1). С. 104-106.

тие информационных технологий, проанализировать объект и предмет преступного посягательства, преступлений, предусмотренных главой 28 УК РФ, а также признаки объективной стороны состава других уголовно наказуемых деяний (способ, орудие, средства), не имеющих объектом посягательства компьютерную информацию, которые образуют иной объект преступления, но могут быть совершены с использованием средств информационно-коммуникационных технологий (например, ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» и другие составы преступлений, предусмотренных Особенной частью УК РФ).

В соответствии с п. 2 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» под информационными технологиями следует понимать процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[8].

В приведенном понятии ключевым является слово «информация». Если рассматривать информацию в юридической плоскости, в частности, как объект преступного посягательства, то анализ преступлений, предусмотренных главой 28 УК РФ, позволяет сделать вывод, что объектом преступного посягательства указанных деяний выступает безопасность компьютерной информации.

Предметом преступления в сфере компьютерной информации могут являться информация, объекты информатизации, информационные системы, сайты, сети связи, информационные технологии[9].

Также к преступлениям, совершённым в сфере информационно-коммуникационных технологий, следует отнести уголовно наказуемые деяния, объектом преступления которых информация не является, но данные деяния совершаются посредством информационно-коммуникационных технологий (например, ст. 159.6 «Мошенничество в сфере компьютерной информации»). Объектом такого преступления выступает чужая собственность. Однако хищение чужой собственности происходит посредством информационно-коммуникационных технологий.

Информационные программы, методики (информация, коды, пароли), с использованием которых было совершено преступление, являются средствами совершения преступления, а оборудование и устройства следует считать орудием. Все это в совокупности выражается через способ совершения преступления – юридически значимый признак объективной стороны состава преступления.

---

[8] Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ: ред. 8 июня 2020 г. № 90-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. I). Ст. 3448; Официальный интернет-портал правовой информации. URL: http: //www.pravo.gov.ru.

[9] См.: Попов А.Н. Преступления в сфере компьютерной информации: учеб. пособие. СПб: С.-Петерб. юрид. ин-т (филиал) ун-та прокуратуры Рос. Федерации, 2018. С. 22-23.

На основании вышесказанного к преступлениям в сфере информационно-коммуникационных технологий следует относить:

– преступления в сфере компьютерной информации (гл. 28 УК РФ);

– преступления, предусмотренные Особенной частью УК РФ, совершаемые посредством использования информационно-коммуникационных технологий, к которым, в частности, относятся программные комплексы, программно-аппаратные комплексы, технические средства и устройства, обеспечивающие операции по сбору, продуцированию, накоплению, хранению, обработке, передаче информации и возможность доступа к информационным ресурсам локальных и глобальных компьютерных сетей.

В связи с изложенным сформулировано следующее определение рассматриваемого понятия: преступление в сфере информационно-коммуникационных технологий – это общественно опасное, противоправное деяние, совершаемое посредством сети (локальной сети, сети «Интернет»), причиняющее вред общественным отношениям в сфере безопасности информационных технологий (компьютерной информации), а также иное запрещенное уголовным законом деяние, совершаемое с использованием различных технологических средств, аппаратно-программных комплексов.

Таким образом, к преступлениям в сфере информационно-коммуникационных технологий следует относить как преступления, предусмотренные главой 28 УК РФ, – преступления в сфере компьютерной информации, так и другие преступления, предусмотренные Особенной частью УК РФ, совершаемые с использованием технических средств и сети «Интернет».

Вопросы для самоконтроля

1. Перечислите нормативные правовые акты, регулирующие общественные отношения в сфере информации, информационных технологий и защиты информации.

2. Сформулируйте следующие основные понятия: информация, информационные технологии, информационные системы, информационно-телекоммуникационная сеть.

3. Перечислите преступления, предусмотренные УК РФ, совершаемые в сфере информационно-коммуникационных технологий.

4. Определите, какие, на Ваш взгляд, обязательные критерии позволяют отнести преступления, предусмотренные Особенной частью УК РФ, к преступлениям, совершённым с использованием информационно-коммуникационных технологий.

Задания для самостоятельной работы

1. Изучите Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Изучите Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности».

3. Проанализируйте Конвенцию о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.).

4. Изучите Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.).

§ 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием средств информационно-коммуникационных технологий, их квалификация

В Стратегии национальной безопасности Российской Федерации немаловажное значение отведено вопросам развития безопасного информационного пространства, а также, предупреждению и пресечению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий[10]. В связи с этим противодействие преступлениям в сфере компьютерной информации как одному из видов преступлений в сфере информационно-коммуникационных технологий приобретает огромное значение, так как преступления данного вида представляют реальную угрозу не только конкретному человеку или группе граждан, но и в целом интересам национальной безопасности страны, поскольку нацелены в том числе на нарушение нормального функционирования систем оборонно-промышленного комплекса, стратегических предприятий, других важных социальных объектов, системы здравоохранения и др. Остановить различного рода угрозы в рассматриваемой сфере возможно лишь при совершенствовании законодательства и подготовке специалистов как в области защиты компьютерной информации, так и в правоохранительной деятельности.

В настоящее время в юридической науке отсутствует четкое определение понятия компьютерного преступления. Существуют различные формулировки понятия, а также ведутся дискуссии о классификации компьютерных преступлений.

[10] О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «ГАРАНТ».

По мнению А.П. Полежаева, компьютерная преступность охватывает преступления, совершаемые с помощью компьютеров, информационно-вычислительных систем и средств телекоммуникаций или направленные против них с корыстными либо некоторыми другими целями.

М.В. Богомолов считает, что компьютерное преступление – это противоправное, виновно совершённое, наказуемое уголовное деяние, причиняющее вред либо создающее угрозу причинения вреда общественным отношениям по законному использованию компьютерной информации.

С точки зрения В.Б. Вехова, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть[11].

Как следует из приведенных выше мнений ученых-правоведов, в теории юриспруденции существует три подхода к определению данного термина. Однако компьютерными чаще всего называют преступления, связанные с компьютерами и высокими технологиями, то есть преступления, при совершении которых компьютерная техника является орудием, средством или целью их совершения.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации следует понимать действия, посягающие на информационную безопасность, предметом которых являются информация и компьютерные средства. Уголовная ответственность за совершение преступлений указанной группы предусмотрена главой 28 УК РФ «Преступления в сфере компьютерной информации», к которым, в частности, отнесены: неправомерный доступ к компьютерной информации (ст. 272); создание, использование, и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274); неправомерное воздействие на критическую инфраструктуру Российской Федерации (ст. 274.1).

В результате проведенного анализа различных мнений, предлагаемых в научной литературе, объектом преступлений, предусмотренных главой 28 УК РФ, следует считать общественные отношения, складывающиеся в сфере охраны компьютерной информации, ее целостности или иных интересов ее собственника. Иными словами, объектом рассматриваемого вида преступлений, наряду с охраной компьютерной информации, выступает состояние безопасности компьютерной информации, поскольку безопасность

[11] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.- метод. пособие. Волгоград: Перемена, 1998. С. 13.

компьютерной информации дает возможность стабильной работы всех информационных систем и защищает от возможных опасных последствий при вредном воздействии на информационную сферу.

Определяющим юридическим документом, раскрывающим понятие информационной безопасности, является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, в которой под информационной сферой следует понимать совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[12].

Информационная безопасность Российской Федерации определяется Доктриной как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз.

Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Объективная сторона рассматриваемых деяний состоит в неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

С субъективной стороны преступления характеризуются виной в форме умысла, направленного на неправомерный доступ к охраняемой законом компьютерной информации.

Субъектом преступления является вменяемое физическое лицо, достигшее возраста 16 лет. Субъект преступления, указанный в ч. 3 ст. 272, ч. 2 ст. 273, ч. 4 ст. 274.1 УК РФ, – специальный, это лицо, использующее свое служебное положение.

Крупным ущербом в соответствии с главой 28 УК РФ является ущерб, сумма которого превышает один миллион рублей.

К квалифицирующим признакам рассматриваемого вида преступлений наряду с ущербом относятся тяжкие последствия или угроза их наступления, предусмотренные ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274, ч. 5 ст. 274.1 УК РФ. Однако следует отметить, что тяжкие последствия в указанных статьях уголовного кодекса носят оценочный характер. К таким последствиям могут быть отнесены, например, утрата особо ценной информации, не подлежа-

[12] См.: Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 дек. 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

щей восстановлению, выход из строя важных технических средств или систем оборонного назначения, дезорганизация производства стратегически важных объектов.

Предметом рассматриваемых преступлений выступает компьютерная информация.

По мнению Д.И. Головко, компьютерная информация как предмет преступного посягательства рассматриваемых выше преступлений содержит ряд характерных признаков (физический, экономический, юридический).

Под физическим признаком информации как предмета преступления следует понимать наличие носителя – предмета или сигнала, физические или иные свойства которых используются для хранения, передачи и обработки информации, распознаваемой электронно-вычислительными машинами.

Экономический признак компьютерной информации как предмета преступления выражается в том, что она является целостной, доступной, конфиденциальной и имеет цену.

Юридический признак компьютерной информации выражается в том, что она должна быть чужой для виновного и иметь собственника[13].

Для более точной характеристики преступлений в сфере компьютерной информации, предусмотренных главой 28 УК РФ, рассмотрим указанные составы подробнее, каждый в отдельности.

Неправомерный доступ к компьютерной информации (статья 272 УК РФ)

Данная статья устанавливает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации. Согласно диспозиции статьи условием для наступления общественно опасных последствий и образования состава преступления будет выступать уничтожение, блокирование либо копирование компьютерной информации.

Состав преступления сконструирован по принципу материального, преступление признается оконченным с момента уничтожения, блокирования, модификации либо копирования компьютерной информации.

Объективную сторону рассматриваемого общественно опасного деяния составляют действия виновного, заключающиеся в неправомерном доступе к охраняемой законом компьютерной информации, если они повлекли уничтожение, блокирование, модификацию либо копирование компьютерной информации.

[13] См.: Головко Д.И. Предмет преступлений в сфере компьютерной информации // Гуманитарные и социально-экономические науки. 2012. № 4 (65). С. 126-129.

Доступ к информации – это возможность получения информации и ее использование[14].

Под неправомерным доступом к компьютерной информации понимается незаконное, то есть не разрешенное владельцем информации, использование возможности получения информации, содержащейся на машинном носителе, в электронно-вычислительных системах (компьютерных системах) или компьютерных сетях.

Следует учитывать, что доступ к электронно-вычислительным машинам (компьютерам)[15] и электронным носителям еще не означает доступа к определенной информации. Например, лица, имеющие доступ в помещение, где расположена электронно-вычислительная техника (вычислительная техника, компьютерная техника), но непосредственно не соприкасающиеся с компьютерной информацией (сотрудники, у которых отсутствует доступ к компьютерам, специалисты по предоставлению клининговых услуг и др. лица), не являются лицами, имеющими доступ к данной технике.

Как ранее было отмечено, материальный состав данного преступления подразумевает наличие ряда последствий:

– удаление информации означает полное и безвозвратное ее уничтожение, что в последующем не позволит произвести ее идентификацию. Неправомерные действия лица будут квалифицированы как покушение на уничтожение компьютерной информации (ч. 3 ст. 30 и ч. 1 ст. 272 УК РФ)[16], если существует возможность восстановления удаленной информации посредством программных или технических средств;

– блокирование информации – совершение действий, приводящих к ограничению или закрытию доступа законных пользователей к компьютерной системе и информационным ресурсам, не связанное с уничтожением информации. Иными словами, воздействие на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме;

– изменение информации – это неправомерные не санкционированные владельцем информации действия, направленные на частичное или полное изменение ее содержания, по сравнению с ее первоначальным видом;

– копирование информации – создание копии на другом носителе, то есть перенос информации на другой носитель при сохранении первоначального вида информации, воспроизведение информации в любой материальной форме, включая случаи ее фиксации с монитора компьютерной техники

[14] См.: Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ: ред. от 20 марта 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[15] Далее – ЭВМ, компьютер.

[16] См.: Уголовное право. Особенная часть / под общ. ред. д-ра юрид. наук, проф. Л.М. Прозументова: учебник. Томск: Изд. дом Томского гос. ун-та, 2019. С. 575.

вручную, фотофиксация информации, а также считывание информации посредством внедрения вредоносных программ и атак по компьютерным сетям.

При квалификации действий по рассматриваемой статье уголовного закона важно установить причинно-следственную связь между несанкционированным доступом и наступлением вредных последствий. Например, изменение целостности информации, ее полная утрата, блокирование или уничтожение могут быть вызваны сбоем систем компьютера либо различными ошибками программного обеспечения.

Создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ)

Данная статья устанавливает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Вредоносное программное обеспечение представляет собой вид компьютерных программ, разработанный с целью неправомерного доступа к компьютерной информации пользователя оконечного устройства.

К вредоносным видам программного обеспечения относятся:

– вирусы;

– макровирусы для Word и Excel;

– загрузочные вирусы;

– клавиатурные шпионы;

– программы для кражи паролей;

– шпионские программы;

– рекламные программы и другие типы вредоносных программ;

– сетевые черви.

Программу следует считать вредоносной при наличии в идеальной совокупности трех критериев:

– программа способна блокировать, видоизменять, полностью или частично уничтожать информацию либо копировать ее. Кроме того, программа способна обходить средства защиты компьютерной информации;

– программа заранее не указывает пользователю на характер своего действия и возможные последствия при использовании подобного продукта.

Объектом рассматриваемого преступления выступают общественные отношения, складывающиеся в сфере охраны компьютерной информации.

Объективной стороной состава преступления является создание, распространение, а также использование компьютерного программного обеспечения и иной компьютерной информации, предназначенных для несанк-

ционированного доступа к компьютерной информации, для ее последующего изменения (модификации), уничтожения, блокирования или ее незаконного копирования.

В целях правильной квалификации рассматриваемого преступления следует проанализировать понятия «создание вредоносных программ» и «использование и распространение».

Под созданием вредоносных программ (например, программы-вируса) следует понимать результат деятельности, выразившийся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования информационно-телекоммуникационных сетей, компьютерных устройств с целью несанкционированного уничтожения, блокирования, модификации, копирования информации, а также с целью нарушения работы информационно-телекоммуникационных сетей.

Под использованием, в данном случае – вредоносных программ, в соответствии со ст. 1270 Гражданского кодекса Российской Федерации (ГК РФ) следует понимать воспроизведение произведения, то есть изготовление одного или нескольких его экземпляров в любой материальной форме; запись произведения на электронном носителе, в том числе запись в памяти ЭВМ, в частности, любая демонстрация с помощью технических средств для большого количества людей, импорт, прокат, переработка (любое изменение, в том числе перевод программы с одного языка на другой), доведение до всеобщего сведения через сеть «Интернет».

Распространение – это продажа или иная форма отчуждения оригинала или экземпляров произведения, включая программы для ЭВМ, в том числе посредством сети «Интернет».

Под распространением вредоносных компьютерных программ понимается предоставление доступа любому пользователю различными способами, в том числе посредством розничной продажи в магазинах, а также в сети «Интернет».

По конструкции объективной стороны состав рассматриваемого преступления является формальным. Преступление окончено с момента создания, использования или распространения компьютерных программ или информации, создающих угрозу уничтожения, блокирования, модификации, копирования или нейтрализации средств защиты компьютерной информации вне зависимости от наступления общественно опасных последствий.

Основными способами совершения преступлений, регламентируемых ст. 273 УК РФ, являются:

– распространение вредоносных программ посредством сети «Интернет», социальных сетей (мессенджеров и пр.);

– использование легального программного обеспечения с целью незаконного обогащения посредством внесения изменений в код данного программного обеспечения, за счет которого меняется целевое предназначение данного программного обеспечения в целом или части его модулей;

– создание и использование эмуляторов различных систем разграничения доступа в информационно-коммуникационные системы, обеспечивающих несанкционированный доступ к ним;

– объединение зараженных устройств в единую сеть, выполняющую функции, заданные правонарушителем.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ)

В соответствии с диспозицией рассматриваемой статьи уголовная ответственность возникает за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Квалификация рассматриваемой статьи в настоящее время является наиболее сложной как в теории, так и в правоприменительной практике. Проблемы квалификации вызваны конструкцией самой статьи и отсутствием в законе определения используемых терминов (*эксплуатация средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования*).

Принимая во внимание то факт, что законодатель не дает определения понятия «информационно-телекоммуникационная сеть», считаем целесообразным обратиться к положениям ст. 2 Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации», в которой под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

К средствам электронно-вычислительной техники следует отнести системы аппаратных средств (процессор, оперативное запоминающее устройство, устройство ввода и вывода и т.д.), а также, программное обеспечение (операционная система, сервисные и иные программы).

Объектом данного преступления являются общественные отношения, складывающиеся в сфере охраны компьютерной информации.

Объективная сторона преступления характеризуется двумя альтернативными деяниями:

– нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации или информационно-телекоммуникационных сетей и оконечного оборудования, сопряженное с использованием несертифицированного оборудования либо нарушением правил эксплуатации сертифицированного, а также с нарушениями

правил использования программного обеспечения либо с использованием несертифицированного программного обеспечения;

– нарушение правил доступа к информационно-телекоммуникационным сетям заключается в совершении действий, которые связанны с несоблюдением правил пользования услугами по передаче данных в информационно-телекоммуникационных сетях (например, несогласованная с оператором сети рассылка электронных писем рекламного, коммерческого или агитационного характера, фальсификация пользователем сети своего IP-адреса, получение несанкционированного привилегированного доступа к ресурсам[17].

Субъектом преступления является вменяемое физическое лицо, достигшее возраста 16 лет.

Субъективная сторона преступления характеризуется виной в форме умысла, направленного на нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Квалифицированным видом преступления является деяние, повлекшее тяжкие последствия или создавшее угрозу их наступления.

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ)

Уголовная ответственность по рассматриваемой статье возникает за неправомерное воздействие на критическую информационную структуру Российской Федерации.

В соответствии со ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной структуры Российской Федерации» под критической информационной структурой Российской Федерации следует понимать объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов[18].

К объектам критической информационной инфраструктуры относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

---

[17] См.: Уголовный кодекс РФ: постатейный научно-практический комментарий / Ю.Ф. Беспалов. М.: Эксмо, 2019. С. 480.

[18] О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Субъекты критической информационной инфраструктуры – это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Объектом преступления являются общественные отношения, складывающиеся в сфере охраны компьютерной информации.

Объективная сторона данного преступления состоит из трех альтернативных действий, а именно: 1) создание; 2) использование; 3) распространение вредоносных компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры.

Субъектом преступления является вменяемое физическое лицо, достигшее возраста 16 лет.

Субъективная сторона преступления характеризуется виной в форме прямого умысла, направленного на неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Квалифицированным видом рассматриваемого преступления являются чч. 1-3 – деяния, совершённые группой лиц по предварительному сговору или организованной группой, а также ч. 4 – если оно совершено лицом с использованием своего служебного положения.

Особо квалифицированный вид рассматриваемого преступления предусмотрен ч. 5 – если такое деяние повлекло тяжкие последствия.

Также к преступлениям в сфере компьютерной информации следует отнести мошенничество в сфере компьютерной информации, предусмотренное ст. 159.6 УК РФ. Данный вид деяния отсутствует в главе 28 УК РФ. Подобная точка зрения законодателя обусловлена различием объектов преступного посягательства. Как ранее было отмечено, объектом посягательства преступлений, предусмотренных главой 28 УК РФ, является охраняемая законом компьютерная информация, в отличие от ст. 159.6 УК РФ, в которой объектом посягательства определяется чужое имущество.

На основании вышеизложенного к преступлениям, совершаемым в сфере информационно-коммуникационных технологий, следует относить как преступления, непосредственно предусмотренные главой 28 УК РФ (преступления в сфере компьютерной информации), так и (в зависимости от способа совершения) иные, не компьютерные преступления, предусмотренные Особенной частью УК РФ (ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», ст. 110 УК РФ «Доведение до самоубийства»,

ст. 110.1 «Склонение к совершению самоубийства или содействие совершению самоубийства», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», ст. 151.2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего», статья 228.1 УК РФ «Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», ст. 242 УК РФ «Незаконное изготовление и оборот порнографических материалов», ст.ст. 205.2 и 280 УК РФ «Публичные призывы к осуществлению террористической и экстремистской деятельности» и ряд других статей).

Рассмотренные выше составы преступлений в сфере информационно-коммуникационных технологий имеют особенности не только в квалификации таких деяний с точки зрения уголовного права, но и в расследовании преступлений данного вида, речь о которых пойдет в следующей главе учебного пособия.

Вопросы для самоконтроля

1. Определите объективную сторону состава преступления, предусмотренного ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Что относится к критической информационной инфраструктуре в соответствии с действующими нормативными правовыми актами?

2. Укажите имеющиеся в правоприменительной практике проблемы при квалификации преступления, предусмотренного статьей 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Проанализируйте нормативные правовые акты с целью правильной квалификации преступления.

3. Определите объективную и субъективную стороны состава преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Смоделируйте практическую ситуацию, при которой действия подозреваемого следует квалифицировать по ст. 273 УК РФ.

Задания для самостоятельной работы

1. Изучите вопросы квалификации преступлений, предусмотренных ст.ст. 159.6, 110, 110.1, 159.3, 151.2, 228.1, 242, 205.2, 280 УК РФ, в части совершения указанных преступлений с использованием информационно-коммуникационных технологий. Определите субъективную и объективную стороны состава преступления.

2. Изучите Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

3. Сотрудник администрации г. Тюмени П. решил использовать компьютер коллеги по работе в личных целях. Без разрешения коллеги он проник в его кабинет и стал работать на его компьютере. Из-за отсутствия у П. знаний и навыков работы на компьютере произошли сбои в работе машины, что привело к отключению модема – одного из элементов компьютерной системы.

Определите, подлежит ли уголовной ответственности П. Проанализируйте состав преступления, предусмотренного ст. 274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием по смыслу ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

4. Являясь сотрудником по логистике ООО «Трансиб», Ш. использовал для работы компьютер данного предприятия. В процессе работы Ш. посещал различные сайты, в результате чего в систему компьютера попали вирусы «сетевые черви», которые в последующем проникли в компьютерную сеть предприятия и уничтожили информацию, содержащуюся на компьютерах. Вследствие этого полностью была уничтожена необходимая документация, в том числе сведения о сотрудниках предприятия, расчеты бухгалтерии, были повреждены материалы и договорные документы.

Решите вопрос о правомерности действий Ш. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

5. Системный администратор одного из государственных учреждений С., используя флеш-накопители, получаемые от сотрудников других организаций, не всегда проверял их на наличие компьютерных вирусов, доверяясь заверениям поставщиков о том, что компьютерных вирусов нет. В результате этого в компьютер С., а затем и в компьютерную сеть учреждения попал комбинированный вирус, что привело к утрате информации, содержащей государственную тайну, и поставило под угрозу срыва запуск одного из космических объектов.

Дайте юридический анализ действий С. Что следует понимать под тяжкими последствиями нарушения правил эксплуатации информационно-телекоммуникационных сетей?

6. УМВД России по Тюменской области было возбуждено уголовное дело по факту совершения неправомерного доступа в охраняемую законом компьютерную информацию в кассовых аппаратах одного из индивидуальных предпринимателей. Следствие квалифицировало действие предпринимателя по ч. 2 ст. 272 УК РФ, т.е. изменение информации в контрольно-кассовых аппаратах, на которых записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассо-

вых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат предпринимателя настаивал на изменении квалификации.

Дайте юридическую оценку действиям предпринимателя. Что следует понимать под компьютерной информацией?

8. Программист М. был признан судом виновным в деяниях, предусмотренных ч. 3 ст. 273 и ч. 1 ст. 165 УК РФ. С ноября по апрель М. рассылал клиентам пяти городских Интернет-провайдеров «троянские» программы и получал логины с паролями, которыми пользовался для доступа в Интернет. Всего было доказано наличие 12 эпизодов пользования М. услугами Интернета без оплаты.

Правильно ли суд квалифицировал содеянное? В каких случаях возможна квалификация по совокупности деяний – преступлений, предусмотренных ст.ст. 272-274 УК РФ, с иными составами преступлений? Что следует понимать под тяжкими последствиями применительно к составу преступления, предусмотренного ст. 273 УК РФ?

ГЛАВА 2. МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Криминалистическая характеристика преступлений, совершённых с использованием современных информационно-коммуникационных технологий

Под криминалистической характеристикой компьютерных преступлений понимается совокупность наиболее характерной, криминалистически значимой информации о признаках и свойствах такого ряда преступлений, способной служить основанием для выдвижения версий о событии преступления и личности преступника, позволяющей верно оценить ситуации, возникающие в процессе раскрытия и расследования компьютерных преступлений, обусловливающей применение соответствующих методов, приемов и средств[19].

Криминалистическая характеристика преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, отличается от уже известных преступных посягательств определенной спецификой. В первую очередь выделяют следующие криминалистически значимые сведения:

– предмет преступного посягательства;

– личность правонарушителя;

– мотивы и цели его преступного поведения;

– типичные способы совершения и сокрытия преступления;

– механизм следообразования;

– время, место и обстановка посягательств[20].

Сведения об особенностях личности совершающих преступления с использованием информационно-коммуникационных технологий являются неотъемлемым компонентом криминалистической характеристики преступлений в данной сфере. Возраст данных лиц составляет от 16 до 45 лет. Например, по результатам некоторых исследований, на момент совершения преступления возраст 18,8 % лиц не превышал 20 лет, 55,2 % лиц составлял 20-29 лет, 11,3 % – от 30 до 39 лет и 7,6 % – старше 40 лет[21].

Большинство лиц, совершающих преступления с использованием информационно-коммуникационных технологий, мужского пола (около 90 %). Интеллектуальный уровень указанных лиц в основном средний.

---

[19] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телком, 2002. С. 114.

[20] Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие. М.: ДГСК МВД России, 2017. С. 160.

[21] Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: дис. … канд. юрид. наук. Иркутск, 2006. С. 145.

Также следует выделить такую категорию лиц, как сотрудники и технический персонал организаций, эти лица могут иметь причастность к совершению преступлений в данной сфере (более 85 %).

Мотивами преступлений, совершаемых с использованием информационно-коммуникационных технологий, могут выступать как личные неприязненные отношения (например, месть), так и корыстные побуждения (получение материальной выгоды), а также хулиганские побуждения, что ведет к дезорганизации работы предприятия, сокрытию другого преступления и др.

Время совершения преступлений рассматриваемой категории лишь в относительно редких случаях устанавливается с точностью до дня и очень редко – до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

Местом совершения компьютерных преступлений являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в каком-либо технологическом процессе. Следовательно, по делам данной категории мест совершения преступных посягательств может быть несколько, в том числе значительно удаленных друг от друга и расположенных как в разных странах, так и на различных континентах. Последнее возможно по причине практически неограниченного радиуса действия и мобильности электронных средств связи и телекоммуникаций.

Важнейшим и определяющим элементом криминалистической характеристики любого преступления, в том числе совершаемого с использованием информационно-коммуникационных технологий, является совокупность данных, характеризующих **способ** его совершения.

Обобщение практики расследования преступлений, совершённых с использованием информационно-коммуникационных технологий, позволяет выделить следующие основные обстоятельства, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории:

1. Наличие преступления (либо это правонарушение иного рода); непосредственная причина (причины) нарушения безопасности компьютерной информации и орудий ее обработки; не является ли происшедшее следствием непреодолимых факторов.

2. Объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности).

3. Предмет преступного посягательства.

4. Способ совершения преступления.

5. Наименование и назначение объекта, где совершено преступление.

6. Конкретное место совершения преступления на данном предприятии, в учреждении, организации, на участке территории; способ его совершения – дистанционный, вне помещения (по каналам электросвязи и локальной вычислительной сети).

7. Режим работы объекта.

8. Средства вычислительной техники и компьютерной информации, с помощью которых совершено преступление (тип, вид, модификация, функциональное назначение, техническое состояние и другие характеристики). Конкретный терминал или участок сети (абонентский номер, код, шифр, рабочая частота).

9. Возможность утечки конфиденциальной информации.

10. Период совершения преступления.

11. Размер материального ущерба, из чего он складывается.

12. Служебные действия и операции технологического процесса, с которыми связано преступление; перечень должностных лиц или работников, несущих ответственность и имеющих непосредственное отношение к технологии производства или командно-административному управлению.

13. Мотив совершения преступления (корысть, месть, хулиганские побуждения, демонстрация личных интеллектуальных способностей, сокрытие другого преступления и др.); цели, преследуемые и достигнутые преступником; мотивы совершения преступления (состояние внезапно возникшего сильного душевного волнения, аффекта либо результат психического заболевания – информационный невроз или компьютерная фобия).

14. Характеристика преступника. Если преступление совершено группой лиц, анализ ее состава и роли каждого соучастника.

15. Наличие причинной связи деяний с наступившими последствиями. Необходимо проверить и доказать, что именно деяния данного лица и обязательно те, которые ему инкриминируются, являются причиной наступивших последствий (например, наличие минимально необходимых специальных познаний).

16. Причины и условия, способствовавшие совершению и сокрытию преступления; факторы, усугубившие их проявление (нарушения нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам; не подлежат ли они привлечению к уголовной ответственности за допущенные нарушения, способствовавшие совершению расследуемого преступления, например, по ст. 274 УК РФ).

Вопросы для самоконтроля

1. Криминалистическая характеристика компьютерных преступлений – это…

2. Криминалистическая характеристика личности преступника.

3. Мотивы и цели совершения преступлений в сфере в сфере информационно-коммуникационных технологий.

4. Время и место совершения преступлений в сфере в сфере информационно-коммуникационных технологий.

Задания для самостоятельной работы

1. Гр-н А. с целью проверки информации, расположенной на личной странице в социальной сети «VK» своего партнера по бизнесу гр-на Б., используя ранее полученный неправомерным путем логин и пароль, осуществил визуальный просмотр содержимого его страницы. Никаких действий по копированию, изменению, уничтожению информации на его странице он не предпринимал.

Дайте обоснованную правовую оценку действиям гр-на А.

2. Гр-н Б. получил доступ к личному кабинету гр-на С., зарегистрированному в ПАО «Сбербанк России», используя ранее полученный неправомерным путем логин и пароль, и осуществил перевод с банковского счета гр-на С. на свой банковский счет 1000 руб., а также оплату своих счетов на сумму 500 руб.

Дайте обоснованную правовую оценку действиям гр-на Б.

§ 2. Этапы расследования преступлений, совершённых с использованием информационно-коммуникационных технологий

Развитие информационных технологий повлекло преобразование имеющихся и появление новых форм противоправных деяний, сопряженных с применением высоких технологий.

Преступления, совершённые с использованием информационно-коммуникационных технологий, принимают транснациональный, организованный и групповой характер. С применением информационных технологий преступление может быть совершено на территории другого государства и даже нескольких государств одновременно, при этом правонарушитель потратит на его совершение всего несколько минут и будет общаться с представителями разных организаций, не выходя из своего дома.

В настоящее время для совершения и сокрытия преступлений данной категории используются как персональные компьютеры, так и мобильные телефоны, различные платежные инструменты, задействуются возможности, предоставляемые ресурсами сети «Интернет».

Расследование преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, можно разделить на несколько этапов. На начальном этапе расследования производится анализ исходных данных. По итогам переработки первичной информации выдвигаются версии и определяются задачи расследования. В ходе анализа следователь должен прогнозировать расследование в целом.

Для первичного этапа расследования преступлений, совершённых с использованием информационно-коммуникационных технологий, наиболее характерны следующие условия:

– собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее;

– собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления, но преступник не известен;

– преступление выявлено органом дознания в результате проведенной оперативно-розыскной деятельности[22].

Изучение первичной информации, вне зависимости от обстоятельств, осуществляется в результате синтеза имеющихся в материалах сведений о криминалистических признаках, указывающих на совершение преступления с использованием информационно-коммуникационных технологий. Это могут быть следующие признаки:

– сбои в работе компьютерной системы или локальной вычислительной сети собственника или правообладателя;

– уничтожение, блокирование, модификация или копирование компьютерной конфиденциальной информации;

– утрата значительных массивов информации или баз данных;

– необычные проявления в работе компьютера: замедленная или необычная загрузка операционной системы, замедление работы машины с внешними устройствами, неадекватные реакции компьютера на команды пользователя и пр.;

– копии чужих файлов в файловой системе правообладателя;

– файлы с вредоносными программами;

– наличие программного обеспечения подбора паролей для неправомерного доступа в Интернет либо иного проникновения в компьютерные сети, а также содержащего функции по уничтожению, блокированию, модификации либо копированию информации, нарушению работы компьютера, системы ЭВМ или их сети;

– внесение в конструкцию компьютера встраиваемых устройств, дополнительных жестких магнитных дисков, устройств для расширения оперативной памяти, считывания оптических дисков и т.д.;

– наличие нестандартных периферийных устройств;

– изменения в оперативном запоминающем устройстве, зафиксированные при задержании подозреваемого с поличным в момент работы на компьютере при совершении неправомерного доступа к компьютерной информации;

– особенности поведения подозреваемого и другие признаки.

[22] Густов Г.А. Проблемы методов научного познания в организации расследования преступлений: автореф. дис. … д-ра юрид. наук. М., 1993. С. 28-52.

При анализе указанных признаков выдвигаются общие и частные типовые версии.

Основными из них являются следующие:

– имело место компьютерное преступление, правообладатель правильно отразил в заявлении его обстоятельства;

– совершено иное преступление, сбой компьютерного оборудования применен для запутывания следов преступления;

– имеет место оговор или ложное заявление о преступлении с целью отвести подозрение от себя или избавиться от нежелательного лица;

– имеет место заблуждение или ошибка заявителя.

На начальном этапе расследования преступлений, совершённых с использованием информационно-коммуникационных технологий, осмотр места происшествия, осмотр компьютерного оборудования и информации, обыск и выемка с целью обнаружения, фиксации и изъятия компьютерной информации и компьютерных средств, относящихся к расследуемому событию, оказываются особо значимым следственным действием. Поскольку компьютерная информация по данной категории преступлений выступает предметом преступного посягательства, необходима своевременная процессуальная фиксация неправомерного доступа к ней.

Одним из важнейших доказательств по уголовным делам о преступлениях, совершённых с использованием современных информационно-коммуникационных технологий, являются данные, содержащиеся на машинном носителе информации компьютеров.

Своевременное получение таких доказательств, их дальнейшая проверка позволят использовать цифровые следы для установления обстоятельств, имеющих значение для правильного разрешения уголовного дела. В связи с этим следователи должны знать, каким образом они могут обнаружить, зафиксировать, изъять подобные доказательства.

Например, при успешной организации и проведении указанных следственных действий могут быть обнаружены и изъяты различные средства компьютерной техники, содержащие информацию, необходимую для расследования уголовного дела.

На подготовительном этапе необходимо осуществить следующие мероприятия:

– установить, какие средства компьютерной техники могут находиться в месте проведения следственного действия, а также порядок доступа к ним (при проведении действий в помещении какой-либо организации) и содержащейся на машинных носителях информации;

– изучить личность подозреваемого либо иного лица, в отношении которого будут проводиться следственные действия, в том числе его профессиональные навыки пользования компьютером, а также средствами шифрования;

– определить круг лиц, которые будут участвовать в следственном действии, в том числе специалистов в области информационной безопасности, проинструктировать их о порядке проведения следственных действий, а также характере предметов и информации, которые подлежат обнаружению и изъятию;

– подготовить необходимые технические и программные средства, позволяющие осуществлять просмотр, поиск, изъятие и последующее хранение компьютерной информации;

– определить дату, время и место следственного действия, а также предпринять меры по обеспечению конфиденциальности действий[23].

Перед началом следственного действия следователь должен четко представлять, что надо искать и где, а также принять решение о способе изъятия компьютерной информации, так как от этого будет зависеть тактика следственного действия.

По прибытии к месту проведения следственного действия необходимо выполнить следующие мероприятия:

– по возможности максимально быстро войти в помещение, подлежащее осмотру;

– при оказании сопротивления со стороны лиц, находящихся в помещении, принять действенные меры по нейтрализации противодействия и скорейшему проникновению в помещение;

– организовать охрану места следственного действия и наблюдение за ним в целях противодействия возможному уничтожению информации, а также попыткам экстренного выключения средств компьютерной техники, в том числе путем обесточивания электропитания, применения специальных средств защиты (шифрования, уничтожения информации).

В связи с этим все электроприборы, расположенные на месте проведения следственного действия, должны быть в исправном состоянии, в котором они были в момент начала следственного действия. Для этого необходимо:

– пресечь нахождение посторонних (лиц, не участвующих в проведении следственного действия) на месте следственного действия;

– запретить каким-либо лицам без разрешения следователя или специалиста включать или выключать электроснабжение;

– запретить каким-либо лицам прикасаться к средствам компьютерной техники и иным техническим средствам, а также источникам питания электрооборудования с любой целью, даже в случае согласия лица, в отношении которою проводится следственное действие, добровольно выдать требуемый предмет или информацию.

На обзорной стадии следственного действия необходимо установить:

---

[23] Россинская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. М.: Проспект, 2010. С. 259-268.

– наличие систем защиты информации, их типы;

– наличие локальной сети и места расположения серверов (на которых могут храниться различные образы памяти) и выхода в другие сети с помощью модема или выделенных линий;

– используемое системное и прикладное программное обеспечение;

– количество и места расположения средств компьютерной техники и их типы;

– возможность использования средств экстренного уничтожения компьютерной информации.

В протоколе осмотра места происшествия необходимо отразить следующие фактические данные:

– наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации (посты охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещение, металлические решетки, шторы, жалюзи, замки и запорные механизмы, экраны, заземление, специальные стекла и пленки, генераторы шума, фильтры и т.д.);

– наименование и назначение объекта, где совершено преступление; его территориальное расположение (на улице, в помещении, банке, магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т.д.) и его ориентация относительно сторон света;

– технические и конструктивные особенности объекта, связанные с установкой и эксплуатацией средств компьютерной техники (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и фактическое состояние устройств электропитания и т.д.);

– ближайшее окружение объекта и подступы к нему (здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в том числе водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцы, концентраторы, короба и т.д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло-, водо- и газоснабжения, вентиляции и т.д.);

– расположение средств компьютерной техники относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если их несколько в одном помещении);

– расположение в одном помещении вместе со средствами компьютерной техники других электрических устройств и приборов (телефонные и иные аппараты электросвязи, оргтехника (копировальные аппараты, автоответчики и т.д.), приборы электроосвещения (настольные, напольные,

настенные, потолочные, подвесные и т.д.), абонентские громкоговорители, телевизоры и мониторы, чайники, кондиционеры и т.д.);

– наличие в одном помещении со средствами компьютерной техники линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (системы электросвязи, электропередачи, тепло-, водо- и газоснабжения, антенны-провода);

– наличие или отсутствие соединений средств компьютерной техники с оборудованием или вычислительной техникой, находящимися вне территории (помещения) осмотра (на это могут указывать кабели и провода, идущие от осматриваемого средства компьютерной техники за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется);

– наличие или отсутствие технических средств сопряжения компьютерной техники с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми они соединены между собой, а также с аппаратами или линией электросвязи);

– наличие или отсутствие учетно-справочной документации к средствам компьютерной техники (технический паспорт и подобный ему документ; журнал оператора или протокол автоматической фиксации расчетно-кассовых и иных операций; журнал учета машинных носителей информации, машинных документов, заказов (заданий или запросов); журнал (карточка) учета выдачи машинных носителей информации и машинных документов; журнал (карточка) учета массивов (участков, зон), программ, записанных на машинные носители информации; журнал учета уничтожения брака бумажных носителей информации и машинных документов; акты на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов);

– наличие на объекте, путях подхода и отхода следов преступления и подозреваемого (обвиняемого) (следы орудий взлома, повреждения, уничтожения и (или) модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на средствах компьютерной техники, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих средства компьютерной техники и электрооборудование; остатки соединительных проводов средств компьютерной техники, наличие участков механического сдавливания и приклеивания посторонних предметов).

Таким образом, осмотр места происшествия, наряду с осмотром средств компьютерной техники, является наиболее распространенным и одновременно наиболее важным следственным действием при расследовании

преступлений, совершённых с использованием современных информационно-коммуникационных технологий. При проведении осмотров указанных видов устанавливается большинство доказательств как наличия самого общественно опасного деяния, так и вины подозреваемого.

При наличии вычислительной (локальной) сети в первую очередь необходимо осмотреть сетевое оборудование, а именно сетевой сервер, т.к. в его оперативной и постоянной памяти хранится большая часть цифровой информации, с его помощью осуществляется управление другими устройствами, имеющими с ним прямое подключение.

Необходимо учитывать, что, если имеются соединительные средства компьютера с другими приборами и оборудованием за пределами территории, на которой проводится следственное действие, у подозреваемого (обвиняемого) будет возможность прямого доступа к цифровой информации и выполнения каких-либо манипуляций с ней. С целью предупреждения такого вмешательства следует отключить все приборы за периметром осматриваемой территории. Не исключено отключение как на аппаратном, так и на программном уровне.

В ходе следственного действия при установлении факта уничтожения либо искажения информации, а также цифровых носителей информации следует доступными и законными способами пресечь эту процедуру и продолжить осмотр с детального изучения данного места.

Кроме того, в ходе осмотра нужно определить технические приборы и сетевое оборудование, находящиеся во включенном состоянии, а также установить характер выполняемых ими процессов и программ. **Необходимо:**

– с участием специалиста определить и отключить специальные средства защиты информации от несанкционированного доступа, принять меры к установлению пароля для шифрования-дешифрования информации либо к получению защищенной информации;

– установить перечень выполняемых программ и процессов, а также определить наличие информации, к потере которой может привести некорректное выключение компьютера.

Для получения всей возможной доказательственной информации необходимо знать перечень компьютерной техники, которая обладает свойствами хранения информации и в связи с этим имеет наибольший интерес для расследования уголовного дела, поскольку посредством данной техники можно установить основные доказательства преступной деятельности подозреваемого (обвиняемого).

Свойством хранения компьютерной информации обладают следующие средства компьютерной техники: устройство HDD (Hard Disk Drive, накопитель на жестких магнитных дисках, жесткий магнитный диск, винчестер), устройство внешний HDD, устройство Flash USB Drive (флэш-накопитель, устройство Flash-memory (флэш-память, карта памяти, USB флэш-

накопитель), оптический (лазерный) диск, планшетный компьютер (электронный планшет), мобильный телефон или смартфон; электронная книга (цифровая книга), цифровые фото- и видеокамеры; MP3-плеер; игровая приставка, GPS-навигатор. В связи с постоянным развитием сферы высоких технологий данный перечень не является исчерпывающим.

Одним из наиболее важных следственных действий при осмотре места происшествия в ходе расследования уголовных дел рассматриваемой категории является изъятие средств компьютерной техники.

Существует два основных способа изъятия компьютерной информации:

– изъятие обнаруженных средств компьютерной техники с последующим детальным изучением имеющейся на них компьютерной информации вне места изъятия (например, в служебном кабинете или в экспертном учреждении);

– изучение всех средств компьютерной техники (содержащейся на них компьютерной информации) непосредственно во время следственного действия с последующим изъятием только той ее (компьютерной информации) части, которая представляет оперативный интерес для дела.

Каждый способ имеет свои преимущества. Изъятие всех технических приборов ускоряет сам процесс осмотра (обыска, выемки), что позволяет осуществлять поиск иных материальных и цифровых следов, имеющих отношение к расследованию преступления.

Главным преимуществом подобного подхода является способность в дальнейшем детально изучить всю имеющуюся на компьютере информацию с привлечением специалистов. Применяя специальные и профессиональные познания, можно избежать потери информации, в том числе и скрытой.

Следовательно, по возможности необходимо всегда изымать машинный носитель информации для дальнейшего его детального осмотра. При этом достаточно ограничиться описанием в протоколе следственного действия внешних отличительных признаков носителя (тип, модель, серийный номер, имеющиеся надписи). Изымать целиком системный блок компьютера и тем более периферийное оборудование не нужно, поскольку они, как правило, не содержат интересующей следствие компьютерной информации.

В конкретной следственной ситуации (уголовные дела по факту использования реквизитов доступа в сеть «Интернет», несанкционированного доступа к различным ресурсам и т.д.) возможно изъятие системного блока компьютера или модема, которые содержат сведения о MAC-адресе (MAC – Media Access Control – адрес единицы оборудования в сети).

Однако иногда существуют технические и психологические проблемы изъятия всех средств компьютерной техники или такое изъятие нецелесообразно.

Если изъять сам носитель информации не представляется возможным, но возможно выключение компьютера на некоторое время, то при проведении следственных действий необходимо создать точную копию носителя

(так называемого образа памяти или побитовой копии, которые создаются специальными программами, например EnCase[24]), с которой впоследствии возможно работать так же, как с оригинальным носителем.

Кроме того, необходимо учитывать, что выход из строя компьютерных систем компаний и организаций (отсутствие в них отдельных компьютеров) может стать причиной полной дезорганизации их работы, что в свою очередь может привести к значительным материальным убыткам, которые повлекут за собой выставление претензий пострадавшими организациями.

Вследствие этого в отдельных случаях может быть применен второй способ: изъятие необходимой информации из средств компьютерной техники, непосредственно в ходе следственного действия. В таких случаях в обязательном порядке необходимо привлекать специалистов (программиста, системного администратора, специалиста по сетевому оборудованию и др.) в целях снижения объективной возможности необнаружения скрытой информации или ошибок в процессе изъятия информации.

Важным моментом в данном случае будет наличие в распоряжении следователя или специалиста необходимых для изъятия информации технических устройств (например, портативного компьютера, внешних носителей информации и т.д.). Очевидно, что каждая следственная ситуация уникальна, в связи с этим на выбор определенного способа изъятия машинных носителей информации и средств компьютерной техники могут влиять различные обстоятельства. Окончательное решение по данному вопросу должен принимать следователь, исходя из складывающейся обстановки.

В протоколе следственного действия должно быть указано, в каком месте и при каких обстоятельствах были обнаружены изымаемые предметы, выданы они добровольно или изъяты принудительно. Все изымаемые предметы должны быть перечислены в протоколе с точным указанием количества, индивидуальных признаков, в том числе с описанием повреждений. В отношении средств компьютерной техники в протоколе также должно быть указано (при наличии соответствующей информации): полное заводское название, серийный номер устройства, дата производства, нахождение устройства во включенном или выключенном состоянии. Если машинный носитель информации изымается без устройства, в котором он находился, например извлеченный из системного блока накопитель на жестких магнитных дисках, то это также должно быть отражено в протоколе с описанием как изымаемого машинного носителя информации, так и устройства, из которого он был извлечен и которое непосредственно не изымается.

Если при проведении осмотра, обыска, выемки были предприняты попытки уничтожить или скрыть подлежащие изъятию предметы, выключить

[24] С помощью специальной программы EnCase, используемой при производстве компьютерных экспертиз, создается файл, в котором дублируется вся информация с исходного носителя. Этот файл можно передавать другим экспертам, а оригинал (обычно жесткий магнитный диск) оформляется на хранение в соответствующем порядке. Данная программа может работать практически с любыми видами носителей (например, с флэш-карт для цифровых камер можно восстановить фотографии).

компьютерные устройства, удалить компьютерную информацию с машинных носителей информации, это должно быть отражено в протоколе следственного действия с указанием принятых мер.

Порядок проведения следственных действий по изъятию средств компьютерной техники, как и любых иных вещественных доказательств, порядок процессуального оформления их поиска, изъятия и упаковки регулируется соответствующими нормами УПК РФ. При проведении перечисленных следственных действий нормы УПК РФ должны неукоснительно соблюдаться. При их нарушении полученные доказательства могут быть признаны недопустимыми на стадии предварительного расследования или судебного разбирательства. Следовательно, необходимо участие соответствующих специалистов при изъятии указанных средств, машинных носителей информации.

Для соблюдения законности и требований уголовно-процессуального законодательства следует придерживаться следующих рекомендаций:

1) в ходе проведения следственного действия необходимо постоянно акцентировать внимание понятых на всех производимых специалистами манипуляциях и их результатах;

2) фактическое изъятие средств компьютерной техники, находящихся на момент их осмотра во включенном состоянии, производится только после того, как будут выполнены и отражены в протоколе следующие действия:

– информация, находящаяся в оперативной памяти средств компьютерной техники, записана на его постоянный машинный носитель информации либо на специально подготовленный и тестированный для этих целей внешний машинный носитель информации;

– выключено электропитание средства компьютерной техники и всех его периферийных устройств;

– определены и корректно закрыты все выполняемые программы (в некоторых случаях некорректное отключение средства компьютерной техники путем его перезагрузки или выключения электропитания без предварительного выхода из выполняемой программы приводит к потере информации, нарушению конфигурации вычислительной системы, стиранию всех информационных ресурсов на данном средстве компьютерной техники);

– определено и корректно приостановлено выполнение вычислительной операции;

– все электропитающие и соединительные провода и кабели, имеющие разъемное соединение, отсоединены от средства компьютерной техники, источника питания и периферийного оборудования с обязательным указанием в протоколе порядка их соединения (принципиальной схемы), отсоединения и индивидуальных признаков каждого элемента.

С целью предотвращения неправомерной и непроцессуальной работы, физического повреждения и разукомплектования изымаемые объекты необходимо опечатать. Для этого:

– средства компьютерной техники могут быть запакованы в картонные коробки, ящики, бумажные мешки или большие конверты, при этом соединительные швы должны быть опломбированы и сделана опись содержимого;

– отдельно друг от друга упаковываются технические устройства и документы, соединительные провода вместе с разъемными устройствами также должны быть упакованы отдельно, в протоколе делается точное описание индивидуальных признаков, составляется опись для каждой упаковки;

– на листах пломбируемой бумаги, пломбах или упаковке должны быть подписи следователя, понятых и специалиста, участвующего в изъятии, указанный лист накладывается на все разъемные детали корпуса устройства.

В случае невозможности изъятия и приобщения к материалам уголовного дела в качестве вещественных доказательств технических устройств (если оно включено в состав сети или дистанционной системы обработки информации) устройство может быть заменено на аналогичное по характеристикам, или изымается копия образа памяти устройства на соответствующем носителе.

При возникновении необходимости изъятия информации из оперативной памяти технического устройства может быть изъята копия нужной информации на машинный носитель информации. Процедура изъятия фиксируется с использованием видеозаписи[25].

Для того чтобы проводить осмотр средств компьютерной техники, следователь должен обладать практическими навыками, техническими знаниями для проведения осмотра того или иного носителя компьютерной информации и поиска доказательств, поскольку это трудоемкий процессе, требующий обладания специальными знаниями в области компьютерной техники, программного обеспечения. При отсутствии у следователя достаточных знаний, практического опыта он должен привлечь к участию в осмотре специалиста в данной области, чтобы вся имеющая доказательственное значение информация была обнаружена и зафиксирована. При этом следует учитывать, что осмотр средств компьютерной техники в процессе расследования уголовных дел о преступлениях в сфере высоких технологий является одним из основных следственных действий и его производство не терпит отлагательства. Для оперативного проведения процессуальных действий осмотр средств компьютерной техники должен осуществлять сам следователь, который, в отличие, например, от привлекаемого специалиста, детально знает материалы уголовного дела (следственную картину), в связи с чем может определить, относится либо не относится к делу (предмету доказывания) та или иная обнаруженная информация. При этом в ходе осмотра

[25] Мазуров И.В., Казанцев С.Я. Особенности изъятия компьютерной информации при расследовании хищений денежных средств, совершённых с использованием интернет-технологий // Закон и право. 2014. № 5. С. 119.

в случае недостаточности практического опыта и технических знаний следователь должен в полной мере использовать иные источники: знания более опытных коллег, ресурсы сети «Интернет», различную методическую литературу по данной тематике.

Согласно ст. 58 УПК РФ специалистом является лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном настоящим Кодексом, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Привлекая лицо в качестве специалиста для участия в осмотре средств компьютерной техники, следователь должен убедиться в специальной квалификации и профессиональном опыте лица путем проверки подтверждающих документов (например, диплома об окончании профильной организации профессионально-технического или высшего образования, трудовой книжки). Заверенные следователем копии таких документов необходимо приобщить к протоколу осмотра.

Кроме того, в качестве специалистов могут быть привлечены иные лица, образование, квалификация и опыт работы которых соответствуют требованиям ст. 58 УПК РФ (например, сотрудники экспертных учреждений, учащиеся или выпускники профильных организаций профессионально-технического или высшего образования).

В условиях недостаточности имеющихся в распоряжении следователя средств и методов для осмотра того или иного устройства необходимо назначать компьютерно-техническую экспертизу для проведения исследований с применением специальных знаний и специальной техники (например, для установления вредоносных функций программы, восстановления удаленной информации, расшифровки зашифрованных файлов и т.д.). При этом для эксперта следует правильно формулировать вопросы и предоставлять необходимые материалы уголовного дела с целью проведения быстрого и эффективного исследования.

В начале протокола осмотра средств компьютерной техники указываются общие сведения:

– о месте, времени составления протокола;

– об участвующих в ходе осмотра участниках административного процесса (например, специалист);

– краткие сведения о конфигурации служебного компьютера, который будет использоваться в ходе осмотра изъятых средств компьютерной техники;

– сведения о компьютерных программах (название, версия, краткое описание основных возможностей), которые будут использоваться в ходе осмотра;

– краткие сведения об осматриваемом предмете (название, серийный номер) и месте его изъятия. Далее проводится визуальный осмотр устройства, в ходе которого фиксируются: форма (квадратная, прямоугольная, круглая, овальная и т.д.), размер (ширина, длина, толщина), материал корпуса (металл, пластик и т.д.), цвет;

– название устройства, фирма-изготовитель, серийный номер, объем памяти и другие технические данные (если такие отражены на поверхности корпуса или на фабричных ярлыках осматриваемого устройства);

– способ подключения к компьютеру.

Затем проводится детальный осмотр содержащейся на осматриваемом носителе информации; указываются распечатанные приложения к протоколу осмотра (если имеются). В конце протокола осмотра рекомендуется изложить выводы о результатах его проведения, поскольку осмотр средств компьютерной техники, как правило, имеет детальное описание произведенных действий по достижении конечного искомого результата. Кроме того, в конце протокола осмотра описывается способ упаковки осмотренного устройства (устройств).

После проведения осмотра средств компьютерной техники и составления протокола он предъявляется для ознакомления всем участникам, которые после ознакомления подписывают его. Замечания участников следственного действия подлежат внесению в протокол.

Если внешний вид устройства можно осмотреть визуально без применения специальной техники, то для осмотра информации, записанной на носителе, необходимо подключение к компьютеру.

В целях исключения возможности повреждения компьютерной информации при ее исследовании необходимо создать точную (побитовую) копию содержания машинного носителя информации, которая в последующем будет использоваться при осмотре (исследовании), т.е. в дальнейшем сам машинный носитель с оригинальной информацией не используется, он может быть упакован и сдан на хранение, что позволит сохранить и защитить от случайного повреждения или удаления как сам носитель, так и информацию, которые часто являются основными доказательствами по уголовному делу.

В большинстве случаев изъятые носители машинной информации осматриваются с использованием доступного программного обеспечения (например, программы Acronis True Image[26], которая предназначена для резервного копирования, восстановления данных, создания и управления образами логических дисков машинного носителя) и аппаратных средств (например, многофункциональный кабель IDE/SATA-to-USB, предназна-

[26] Программа Acronis True Image предназначена для резервного копирования и восстановления данных. Программное обеспечение позволяет пользователю создавать образ с диска во время работы Microsoft Windows/macOS или в автономном режиме посредством загрузки с CD, DVD, USB флэш-накопителя или с другого загрузочного носителя.

ченный для синхронизации с компьютером осматриваемых носителей информации (в частности, накопителей на жестких магнитных дисках) с распространенными интерфейсами подключения – IDE (Integrated Drive Electronics – параллельный интерфейс подключения накопителей), SATA (Serial Advanced Technology Attachment – последовательный интерфейс обмена данными).

При синхронизации осматриваемого машинного носителя информации со служебным компьютером следует учитывать основное правило: необходимо обеспечить сохранность исследуемой компьютерной информации, заблокировать любую возможность изменения (удаления) изначального состояния такой информации. На практике в следственных подразделениях для указанных целей используется программа WriteBlocker XP[27] (предназначена для работы с операционной системой Windows XP, на операционной системе Windows-7 используется практически аналогичная программа Innovision-Forensics USB WriteBlocker). WriteBlocker XP предотвращает все намеренные, неумышленные и системно инициированные попытки записи на подключенные машинные носители информации, включая жесткие магнитные диски и сменные диски, за исключением системного загрузочного диска, при этом позволяет просматривать и копировать информацию с таких носителей. WriteBlocker XP сохраняет блокированное (открытое) состояние на каждое присоединенное устройство после перезапуска системы. Достаточно установить данную программу на служебный компьютер, после чего она будет работать автоматически без каких-либо дополнительных настроек. Интерфейс программы WriteBlocker XP англоязычный, однако простой и удобный в использовании.

При проведении осмотра изъятого носителя компьютерной информации следует обеспечить безопасность не только вещественного доказательства, но также используемого для осмотра служебного компьютера и хранящейся на нем служебной информации, поскольку осматриваемые устройства хранения информации ввиду специфики данного вида преступлений часто содержат различные вредоносные программы (компьютерные вирусы, троянские программы и т.д.), которые при проведении осмотра могут «заразить» служебный компьютер и в зависимости от вредоносной функции программы повлечь различного рода негативные последствия, вплоть до вывода из строя, блокирования или уничтожения служебного компьютерного оборудования либо удаления, изменения хранящейся на компьютере слу-

[27] Программа WriteBlocker XP не позволяет записывать что-либо на исследуемый накопитель, предназначена для проведения криминалистических исследований при расследовании инцидентов информационной безопасности, производстве судебных экспертиз, требующих максимально возможного сохранения целостности исследуемых данных. Необходимость применения таких средств определяется требованиями процессуального законодательства (например, УПК РФ) и различными рекомендациями методического и иного характера, а также стандартами (например, СТО БР ИББС-1.3-2016).

жебной информации. Для минимизации возможных негативных последствий на служебном компьютере должно быть установлено актуальное надежное антивирусное программное обеспечение с постоянным обновлением антивирусных баз.

После обеспечения сохранности осматриваемой информации, а также безопасности служебного компьютера и служебной информации можно осуществлять подключение изъятого по уголовному делу машинного носителя информации к служебному компьютеру для проведения осмотра его содержимого. Разные устройства хранения информации имеют различные способы синхронизации с компьютером. В практической деятельности используются следующие способы подключения носителей информации к компьютеру и специальные устройства:

– основным устройством хранения компьютерной информации является накопитель на жестких магнитных дисках. Его важным параметром служит используемая система обмена информацией между ним и материнской платой компьютера – так называемый интерфейс жесткого магнитного диска. Наиболее часто используемые интерфейсы – IDE.

– устройство внешний HDD синхронизируется с компьютером при помощи входящего в комплект поставки USB-кабеля;

– устройство Flash USB Drive не требует дополнительных средств для синхронизации с компьютером, поскольку само обладает разъемом USB (Universal Serial Bus – последовательный интерфейс передачи данных);

– для синхронизации с компьютером карты памяти Flash-memory необходимо специальное устройство чтения Card Reader;

– для чтения оптических (лазерных) дисков компьютер должен быть оборудован устройством чтения (записи) компакт-дисков (CD/DVD – дисководом);

– для синхронизации с компьютером карманных переносных компьютеров, мобильных телефонов, смартфонов, электронных книг, MP3-плееров, цифровых фото- и видеокамер, GPS-навигаторов, игровых приставок и т.д. используются входящие в комплект поставки data-кабели или USB-кабели с соответствующим программным обеспечением (драйверами).

При производстве предварительного расследования следователь должен знать, что осмотр машинных носителей компьютерной информации является основополагающим следственным действием по расследованию преступлений в сфере высоких технологий, требующим применения актуальных практических навыков работы с современными техническими и программными средствами. В связи с этим следователю необходимо постоянно совершенствовать свои знания в сфере высоких технологий, программного обеспечения, способов совершения компьютерных преступлений, поскольку лица, совершающие преступления с использованием современных информационно-коммуникационных технологий, обладают обширными знаниями в данной сфере.

Показания заявителя о совершённом преступлении, дополненные результатами проведенных осмотров, обысков и выемок, будут являться главным источником информации, имеющей значение для уголовного дела. Лицам, которым в результате противоправных действий причинен какой-либо вред, присваивается процессуальный статус – потерпевший. При производстве допроса потерпевших требуется установить следующие обстоятельства:

– наличие программных и аппаратных средств защиты информации;

– организация доступа к техническим средствам обработки информации, а также наличие локальных сетей и беспроводных соединений;

– обстоятельства выявления противоправного деяния;

– последствия выявленного посягательства;

– предварительная оценка понесенного вреда.

Если лицо, совершившее преступление, не установлено, то в ходе допроса потерпевшего необходимо уточнить криминалистические признаки, которые позволят получить некоторые сведения о правонарушителе, а именно:

– частота смены паролей и кодов доступа к информации и носителям информации;

– лица, ответственные за смену кодов и паролей (при их наличии);

– третьи лица, имевшие доступ к средствам компьютерной техники и сетям (техники, системные администраторы, программисты и др.).

При выявлении таких преступных деяний в организациях необходимо установить, имеются ли случаи нетипичного поведения персонала и сотрудников:

– выполнение сотрудниками сверхурочных работ без явной или острой служебной необходимости;

– отказ от очередных отпусков;

– «тяжелое» материальное положение;

– проявление интереса к работе сопряженных отделов;

– обнаружение нештатных устройств хранения информации (оптические диски, usb-накопители и пр.);

– недавнее посещение организации посторонними лицами, проявлявшими интерес или имевшими доступ к электротехническим приборам, аппаратному и программному обеспечению и т.д.

В результате проведения допросов потерпевших формируется свидетельская база. Следующий этап расследования включает установление очевидцев преступления и последующий их допрос, то есть тех лиц, которые непосредственно могут свидетельствовать о противоправном деянии.

Свидетелями обстоятельств произошедшего могут быть допрошены родственники потерпевшего или сотрудники организации, в отношении которой совершено преступное посягательство.

Допросы свидетелей и потерпевших проводятся с целью получения подробной информации о ситуации, складывающейся перед совершением

преступления для дальнейшего установления круга потенциальных подозреваемых. Большое количество свидетелей позволяет получить более точную картину обстоятельств совершённого противоправного действия.

На лицо, совершившее данное преступление, чаще указывает местонахождение электронно-вычислительной техники, которая в данном случае выступает орудием преступления.

В случаях хищения денежных средств или приобретения права на иные материальные ценности с применением дистанционных систем подозреваемым (обвиняемым) могла предварительно производиться переписка с потерпевшим. При указанных обстоятельствах для установления личности правонарушителя необходимо[28]:

– направить запросы в кредитные организации или операторам платежных систем о предоставлении информации о движении денежных средств по расчетным счетам потерпевшего на основании требований 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»;

– в соответствии с запросами следуют истребовать сведения, указанные держателем счета при его открытии, а также сведения об IP-адресах, посредством которых осуществлялась регистрация держателя счета в системе дистанционного банковского обслуживания, и сведения об IP-адресах, с которых осуществлялись последние 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 международной правовой помощи;

– полученные ответы на указанные запросы, сведения об IP-адресах можно проверить с помощью открытого интернет-сервиса, расположенного по адресу: https://www.ripe.net/, или любого другого схожего с ним сервиса, который даст возможность получить данные провайдера, которому принадлежит интересующий адрес. Следующие действия будут определены в зависимости от типа IP-адреса (статический или динамический).

При использовании статического IP-адреса необходимо получить судебное решение на производство выемки сведений об абонентах в организации-провайдере, которой принадлежит интересующий IP-адрес, либо в порядке п. 4. ч. 2 ст. 38 УПК РФ дать поручение органам дознания на получение данной информации. Ответ на указанный запрос может содержать сведения о состоянии устройств по конкретному адресу, которые подключались к сети и с которых производились переписка или переводы и т.д.

[28] Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие / Ю.В. Гаврилин [и др.]. М.: Акад. управления МВД России, 2019. С. 179.

С целью установления лица, осуществившего размещение в социальной сети какой-либо противозаконной информации, следует направить соответствующий запрос техническому специалисту интересующей социальной сети, содержащий следующие вопросы[29]:

– дата и время создания группы или размещения противозаконных материалов по конкретному электронному адресу (электронный адрес содержит адресная строка);

– установочные данные пользователя (информация, содержащая сведения о логине и данных, указанных при создании ресурса), создавшего группу или разместившего противозаконные материалы;

– дата и время входа и выхода пользователя на ресурс при создании группы (размещении противозаконных материалов);

– какие персональные данные были указаны пользователем при регистрации в сети;

– IP-адрес устройства, с которого был осуществлен выход в сеть пользователя, создавшего группу или разместившего противозаконные материалы, с указанием даты и временем доступа;

– вид и название операционной системы, а также название браузера, которые установлены и используются на устройстве указанного пользователя.

Используя открытые онлайн-сервисы (www.whois-service.ru, https://www.ripe.net/), можно получить сведения об операторах-провайдерах по закрепленным за ними IP-адресам и приобщить полученные сведения к материалам в виде справки. После получения данных об операторе-провайдере необходимо направить ему запрос для установления следующих сведений:

– какого типа интересующий IP-адрес – статический или динамический;

– в случае использования статического IP-адреса необходимо истребовать имеющиеся данные о лице, с которым был заключен договор о предоставлении услуг связи, а также MAC-адрес (Media Access Control address – установленный производителем аппаратный адрес устройства, присоединенного к сетевой среде, необходимый для системы управления доступом к ней) устройства, посредством которого осуществлен доступ к сети «Интернет», физический адрес подключения; сведения об операционной системе и браузере указанного 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,

[29] Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. С. 179.

по какому адресу был осуществлен доступ в Интернет и какие 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).

В последующем необходимо направить запросы всем представленным в населенном пункте провайдерам с целью получения ответов на следующие вопросы:

– заключался ли договор на предоставление услуг связи и доступа в сеть «Интернет» с кем-либо использующим MAC- адрес устройства;

– каким пользователям выделялся IP-адрес для использования устройства с интересующим MAC-адресом (дата, время, адрес доступа в сеть «Интернет» и какие ресурсы сети посещал пользователь).

Кроме того, дополнительные сведения, представляющие интерес для уголовного дела, можно получить от банков и операторов платежных систем. Для этого в адрес указанных организаций необходимо направить запрос и судебное решение с требованием о предоставлении идентификационных данных лиц, счета которых были использованы для пополнения баланса абонентского номера интересующей SIM-карты.

Дополнительные сведения посредством запроса и на основании соответствующего судебного решения можно истребовать в организации – администраторе сервиса электронной почты, ящик электронной почты которой был указан при регистрации пользователя в сети. В запросе должны содержаться следующие вопросы:

– предоставление сведений лица-пользователя, указанных им при регистрации ящика электронной почты, с указанием даты и времени регистрации ящика;

– информация об активности пользователя (датах и времени посещения сервиса за интересующий период времени);

– IP-адреса и MAC-адреса устройства, с которого была произведена регистрация ящика электронной почты и с которого осуществлялся доступ к указанному ящику электронной почты за необходимый период времени, а также сведения об абонентском номере, с использованием которого проводилась активация и, возможно, процедура восстановлении пароля пользователя электронного почтового ящика.

В случае если представленные IP-адреса отличаются от полученных ранее, то целесообразно вновь направить запрос провайдеру для получения актуальных данных, которые помогут установить пользователя интересующего ящика электронной почты.

Если при совершении преступления использовались электронные кошельки электронных платежных систем, то для установления их владельцев необходимо:

– посредством направления запроса истребовать у администратора платежной системы сведения о регистрационных данных держателя кошелька, зарегистрировавшего электронный кошелек с интересующим идентификационным номером (указывается имеющийся идентификационный номер кошелька);

– истребовать сведения о всех кошельках, зарегистрированных на вышеуказанного пользователя, а также историю произведенных по ним операций с указанием IP-адресов, с которых происходила авторизация пользователя за весь имеющийся период;

– при переводе (перечислении, выводе) средств с интересующих кошельков данного пользователя истребовать сведения о держателях кошельков, на которые были переведены средства.

В случаях выявления фактов использования сетевого оборудования при совершении противоправных деяний местонахождение указанного оборудования может быть установлено по MAC-адресам. Для этого следует:

– направить запрос интернет-провайдеру, через которого осуществлялся выход в Интернет, о предоставлении MAC-адреса оборудования соответствующего абонента, подключенного по IP-адресу;

– направить запросы операторам связи для поиска оборудования с определенным MAC-адресом в их сети и предоставления регистрационных данных абонента, его использующего[30].

Допрос фигурантов выступает одним из основных следственных действий при расследовании всех видов преступлений.

Поскольку дополнительным объектом преступлений в сфере высоких технологий выступают правоотношения по поводу владения, пользования и распоряжения компьютерной информацией, при проведении допросов должна быть получена специфическая информация, касающаяся предмета доказывания.

Перед производством допроса рекомендуется собрать сведения и провести анализ личности допрашиваемого лица. Полученные выводы позволят расширить круг лиц, которые могут иметь отношение к расследуемому деянию, что сделает допрос более результативным.

Важным аспектом выступает информация о наличии у допрашиваемого лица специальных и квалифицированных навыков и умений владения компьютерной техникой. Представление о специализации подозреваемого (обвиняемого) способствует правильной оценке его показаний и в дальнейшем решению вопроса о возможности совершения тех или иных действий с компьютерной техникой.

[30] Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. С. 185.

При расследовании преступлений, совершённых в сфере использования компьютерной информации, допросы осуществляются с применением тактических рекомендаций, разработанных в криминалистике[31].

Основными тактическими задачами допроса при расследовании дел рассматриваемой категории являются:

– выявление элементов состава преступления;

– установление обстоятельства, места и времени совершения значимых для расследования действий, способа и мотивов их совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем;

– определение предмета преступного посягательства;

– определение размера причиненного ущерба;

– установление иных свидетелей и лиц, причастных к совершению преступления[32].

Первичное обнаружение признаков неправомерных действий с компьютерной информацией посторонних лиц осуществляется, как правило, сотрудниками собственника информационной системы и ее пользователями. Описание этих признаков может найти отражение в показаниях очевидцев.

Следует учесть, что свидетелями по данной категории дел чаще всего выступают лица с высшим образованием, обладающие высоким интеллектом, в совершенстве владеющие специальной терминологией, зачатую неизвестной следователю. В связи с этим следователю необходимо детализировать показания допрашиваемого посредством постановки уточняющих вопросов, раскрывающих содержание тех или иных терминов и определений, используемых допрашиваемым. При описании конфигураций систем или схем движения информации крайне полезными могут оказаться рукописные схемы, составляемые допрашиваемым к протоколу допроса[33]. Для участия в допросе может быть приглашен специалист в области компьютерных технологий (в данном случае следует предварительно согласовать с ним формулировки задаваемых вопросов).

Для решения указанных задач в процессе допроса свидетелей необходимо выяснить:

– не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании;

– не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции;

---

[31] Шепитько В.Ю. Теоретические проблемы систематизации тактических приемов в криминалистике: дис. ... д-ра юрид. наук. Харьков, 1995. С. 118.

[32] Криминалистика: учебник / отв. ред. Н.П. Яблоков. М.: Юристъ, 2001. С. 629.

[33] Криминалистика: учебник для вузов / А.Ф. Волынский [и др.]; под ред. проф. А.Ф. Волынского. М.: Закон и право, ЮНИТИ-ДАНА, 1999. С. 604.

– не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;

– зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации;

– как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;

– как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается;

– каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

– каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи;

– кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия;

– как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.

– имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то как часто;

– могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы компьютера, компьютерной системы, сбоев программного обеспечения и т.п.;

– каков характер изменения информации;

– кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.

При расследовании неправомерного доступа к компьютерной информации на первоначальном этапе возникает необходимость допрашивать в качестве свидетелей граждан различных категорий (операторы ЭВМ; программисты; сотрудник, отвечающий за информационную безопасность, или администратор; сотрудник, занимающийся техническим обслуживанием; начальник вычислительного центра или руководитель предприятия (организации), для каждой из которых существует свой предмет допроса[34].

При подготовке, планировании и в ходе проведения допросов подозреваемых (обвиняемых) по уголовным делам о компьютерных преступлениях следует учитывать особенности составов преступлений данного вида, и прежде всего субъективную сторону и криминалистическую характеристику личности предполагаемого преступника. При первоначальном допросе необходимо, побуждая лицо к деятельному раскаянию, выяснить, какие изменения в работу компьютерных систем были внесены, какие вирусы

[34] Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнова. М., 2001. С. 57.

использовались, есть ли, с точки зрения подозреваемого (обвиняемого), возможность быстро устранить или уменьшить вред, причиненный несанкционированным проникновением в систему. Какие сведения и кому передавались[35].

На начальной стадии допроса выясняются обстоятельства общего характера, интересующие следствие и касающиеся:

– навыков и опыта работы с компьютерной техникой и конкретным программным обеспечением;

– использования на компьютере по месту работы правомерного доступа к компьютерной технике и конкретным видам программного обеспечения;

– конкретных операций с компьютерной информацией, которые подозреваемый (обвиняемый) выполняет на своем рабочем месте либо (если не работает) на своем персональном компьютере или компьютерах своих знакомых;

– правомерного доступа к сети «Интернет» и работы в Интернете;

– закрепления за ним по месту работы идентификационных кодов и паролей для пользования компьютерной сетью и др.

Немаловажное значение имеет выяснение обстоятельств, предшествовавших совершению преступления:

– когда возникло намерение совершить преступление, кто (или что) повлиял на это решение;

– почему выбран именно данный объект для преступного посягательства (организация, структура, в которой работал подозреваемый, или стороннее учреждение, предприятие);

– каковы мотивы совершения преступления (подавляющее большинство преступлений данного вида (более 70 %) совершаются по корыстным мотивам);

– какова цель совершения компьютерного преступления: только ли его совершение, либо компьютерная техника являлась лишь средством, способом совершения иных, традиционных преступлений: хищения, уклонения от уплаты налогов, промышленного шпионажа и т.д. На первоначальных допросах подозреваемые (обвиняемые) нередко называют «безобидные» цели: любопытство, проверить свои способности и т.п., чтобы смягчить свою вину либо избежать уголовной ответственности за содеянное. Особенно в случаях, когда преступный замысел еще не доведен до конца (скопированная информация еще не продана, приготовленные к хищению деньги еще не получены и т.д.)[36].

---

[35] Криминалистика: учебник для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская; под ред. Р.С. Белкина. М.: НОРМА (Издательская группа НОРМА-ИНФРА М), 2002. С. 960.

[36] Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2001. С. 70.

Преступления, которые носят серийный, многоэпизодный характер, обязательно сопровождаются действиями по их сокрытию, которые осуществляют, как правило, высококвалифицированные специалисты, входящие в организованные преступные группы и сообщества, оснащенные технически (нередко специальной оперативной техникой).

С учетом имеющихся данных о том, что преступление совершено группой лиц, в ходе допроса необходимо выяснить:

– наличие сговора с другими лицами и кем являются эти лица;

– кто инициатор;

– время, место и иные детали состоявшейся преступной договоренности;

– распределение ролей между участниками преступления;

– каковы конкретные действия по подготовке преступления: предварительное изучение объекта преступного посягательства, подтверждение наличия интересующей соучастников информации, принятие мер для нелегального получения идентификационных кодов, паролей с целью доступа в сеть, открытие лжепредприятий либо счетов в несуществующих банках, получение кредитных карт (для перевода похищенных денежных средств и т.д.); и т.п.

Вторжения в компьютерные сети потерпевших организаций извне составляют половину компьютерных преступлений. В связи с этим при допросах подозреваемых (обвиняемых) очень важно уточнить «технологию» совершения преступления, получить сведения о том, какие имеются или могли сохраниться электронные и материальные следы содеянного, где можно обнаружить интересующую следствие информацию.

При неправомерном доступе к компьютерной информации подозреваемому (обвиняемому) необходимо задать следующие вопросы:

– о месте неправомерного проникновения в компьютерную систему (сеть): внутри потерпевшей организации (путем выдачи соответствующих команд с компьютера, на котором находится информация, и т.д.) или извне;

– способах проникновения в помещение, где установлена компьютерная техника (если подозреваемый, обвиняемый не имел к ней доступа и не работал в данной организации), и осуществления неправомерного доступа в компьютерную систему, сеть;

– приемах преодоления информационной защиты: подбор ключей и паролей (вход в систему, сеть под именем и паролем одного из легальных пользователей, присвоение имени другого пользователя с помощью программы, которая изменяет данные, и пользователь получает другое имя и т.д.); хищение ключей и паролей (визуальный перехват информации, выводимой на экран дисплея или вводимой с клавиатуры, о паролях, идентификаторах и процедурах доступа; перехват паролей при подключении к каналу во время сеанса связи; электронный перехват в результате электромагнитного излучения; сбор и анализ использованных распечаток документов и других материалов, содержащих сведения о паролях и процедурах доступа

и т.д.); отключение средств защиты; разрушение средств защиты; использование несовершенства защиты;

– от кого подозреваемый (обвиняемый) получил данные об используемых в потерпевшей организации мерах защиты информации и способах ее преодоления;

– какие средства использованы при совершении преступления: технические, программные, носители информации, комбинированные (с использованием двух или трех из указанных выше);

– об иных технических уловках и ухищрениях, используемых для неправомерного доступа: считывание информации при подключении к кабелю локальной сети при приеме электромагнитного излучения сетевого адаптера; перехват электромагнитного излучения от дисплеев серверов или рабочих станций локальной сети для считывания и копирования информации; копирование данных с машинных носителей информации, оставленных без присмотра или похищенных из мест их хранения; считывание информации с жестких магнитных дисков и гибких дискет (в том числе остатков стертых и временных файлов), магнитных лент при копировании данных с оборудования потерпевшей организации; хищение портативного компьютера, машинных носителей с целью получения доступа к содержащейся в них информации и т.д.;

– о способах сокрытия неправомерного доступа (программных, об указании ложных данных о лице, совершившем неправомерный доступ);

– количестве фактов незаконного вторжения в информационные базы данных;

– об использовании для неправомерного доступа своего служебного, должностного положения, и в чем это конкретно выразилось, и т.д.[37]

Анализ уголовных дел показывает, что при расследовании незаконного вмешательства в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей в зависимости от того, насколько обвиняемый признает собственную вину, могут складываться следующие следственные ситуации[38]:

1. Обвиняемый признает собственную вину и дает развернутые правдивые свидетельские показания.

2. Обвиняемый частично признает собственную вину, но отрицает участие в основных эпизодах преступной деятельности.

3. Обвиняемый признает собственную вину, но установлены не все эпизоды преступной деятельности.

4. Обвиняемые (при совершении преступления группой лиц по предварительному сговору либо организованной группой) отрицают свою причастность к преступлению, дают противоречивые свидетельские показания.

[37] Андреев Б.В., Пак П.Н., Хорст В.П. Указ. соч. С. 70.

[38] Поливанюк В. Особенности проведения допросов при расследовании преступлений, совершённых в сфере использования компьютерной информации. Ростов н/Д.: Феникс, 2016. С. 14.

5. Обвиняемый признает собственную вину, но не называет соучастников преступления.

При учете следовой картины и по результатам допросов свидетелей из круга лиц, осуществляющих облуживание системы, а также ее разработчиков можно установить способ несанкционированного доступа к информации. При производстве предварительного следствия по уголовным делам указанной категории необходимо учитывать возможную причастность к их совершению штатных сотрудников и обслуживающего персонала организации. Процессуальная оценка действиям указанных лиц должна даваться своевременно при наличии оснований, с целью предотвращения их противоправных действий, а также исключения возможности сокрытия ими следов преступления.

Организация оперативно-розыскных мероприятий в рамках расследования уголовного дела о преступлениях, совершённых с использованием информационно-коммуникационных технологий.

Наряду с решением следственных задач, немаловажной, а порой определяющей при расследовании уголовного дела является работа оперативных подразделений.

Положительные результаты расследования преступлений в сфере информационно-коммуникационных технологий в рамках возбужденного уголовного дела зачастую зависят от правильной организации оперативно-розыскных мероприятий, а также взаимодействия следственно-оперативных групп с другими ведомственными подразделениями Министерства внутренних дел Российской Федерации.

МВД России в борьбе с преступностью в области высоких технологий задействует как подразделения уголовного розыска, так и специальные оперативные подразделения, в частности Управление «К» МВД России, как на федеральном, так и региональном уровнях.

Основными задачами Управления «К» МВД России в борьбе с преступлениями в области информационных технологий являются предупреждение, выявление и раскрытие таких преступлений, как:

– в сфере *компьютерной информации:* мошенничество в сфере компьютерной информации; хищения в банковском секторе, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей; создание, использование и распространение вредоносных компьютерных программ; неправомерный доступ к охраняемой законом компьютерной информации;

– *преступления, совершаемые с использование информационно-коммуникационных технологий, включая сеть «Интернет»:* незаконный оборот специальных технических средств, предназначенных для негласного получения информации; использование несовершеннолетнего в целях изготовления порнографических материалов и другие преступления, направленные против здоровья несовершеннолетних и общественной нравственности.

Для эффективной борьбы с преступлениями в сфере информационных технологий должны быть задействованы оперативные подразделения специальных технических мероприятий органов внутренних дел, обеспечивающих возможность проведения технических оперативно-розыскных мероприятий:

– снятие информации с технических каналов связи (заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами работы соответствующих систем и устройств, в том числе излучаемых ими электромагнитных и других полей);

– получение компьютерной информации (получение оперативно-розыскным подразделением сведений, функционирующих на машинных носителях компьютерной информации, в том числе извлеченных из сети «Интернет», и их фиксация путем съема техническими специальными средствами характеристик электромагнитных полей, возникающих при обороте компьютерной информации в сети электрической связи);

– прослушивание телефонных переговоров (мероприятие, которое заключается в получении и фиксации с помощью технических средств акустической информации, передаваемой по линиям телефонной связи, или односторонних сообщений в целях обнаружения сведений о преступной деятельности изучаемого лица, выявления его связей и получения иной информации, способствующей решению конкретных задач оперативно-розыскной деятельности). Данное мероприятие является весьма важным в борьбе с преступлениями в сфере высоких технологий, поскольку информация, полученная в результате проведенного мероприятия, не только может иметь доказательственное значение для уголовного дела, но и может способствовать:

1) установлению связей «разрабатываемого» лица, способов передачи информации между фигурантами, места хранения информационных носителей, информации о наличии автотранспорта и т.д.;

2) подготовке обысков (знание места нахождения орудий совершения преступлений) в сфере высоких технологий, что в свою очередь дает возможность предотвратить уничтожение следов преступления.

Таким образом, применение различных технических мероприятий в комплексе с мероприятиями, предусмотренными ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», имеет существенное значение для установления обстоятельств, подлежащих доказыванию по уголовному делу.

Одним из заключительных этапов расследования преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, является назначение и производство судебной компьютерно-технической экспертизы.

Следует отметить, что в связи с широким распространением криминализированных бесконтактных способов совершения преступлений в сфере

информационно-коммуникационных технологий номенклатура объектов исследования в ходе повседневной экспертной деятельности в области компьютерной экспертизы претерпевает существенные изменения. Например, в настоящее время основным объектом экспертного исследования выступает мобильная связь и аппараты мобильной связи, что составляет 90 % от всех расследуемых уголовных дел в сфере информационно-коммуникационных технологий.

Руководствуясь действующим уголовно-процессуальным законодательством Российской Федерации, дознаватель, орган дознания, следователь, руководитель следственного органа вправе назначать судебную экспертизу, принимать участие в ее производстве и получать заключение эксперта в разумные сроки (ч. 1 ст. 144 УПК РФ).

При назначении экспертизы уполномоченное лицо должно руководствоваться гл. 27 УПК РФ «Производство судебной экспертизы» (порядком, условиями и требованиями к назначению судебных экспертиз), при этом суд также инициативно либо по ходатайству сторон может назначить судебную экспертизу, руководствуясь ст. 283 УПК РФ.

В ходе анализа судебной практики по уголовным делам о преступлениях в сфере информационно-коммуникационных технологий установлено, что наибольшее распространение при расследовании уголовных дел указанной категории получило применение именно компьютерных экспертиз, объектами исследования которых являлись именно компьютеры, телефоны и иные компьютерные устройства.

Согласно ст. 9 Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» судебная экспертиза – это «предусмотренное законодательством Российской Федерации о судопроизводстве процессуальное действие, включающее в себя проведение исследований и дачу заключения экспертом по вопросам, требующим специальных знаний в области науки, техники, искусства или ремесла»[39].

В соответствии с приложением № 2 к приказу МВД России от 29 июня 2005 г. № 511[40] и перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, выделяют «компьютерную экспертизу» и «исследование компьютерной информации».

---

[39] Абз. 7 ст. 9 Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

[40] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации): приказ МВД России от 29 июня 2005 г. № 511. Доступ из справ.-правовой системы «КонсультантПлюс».

При этом на основании приказа Минюста России от 27 декабря 2012 г. № 237[41] федеральные бюджетные судебно-экспертные учреждения Минюста России также имеют право проводить «компьютерно-технические экспертизы», которые заключаются в исследовании информационных компьютерных средств.

При назначении и проведении судебных экспертиз в ходе расследования преступлений, совершённых в сфере информационно-коммуникационных технологий, эксперт должен руководствоваться следующими нормативными правовыми актами:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[42] (регламентирует вопросы регулирования общественных отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации).

2. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»[43] (целью закона является создание условий для оказания услуг связи на всей территории Российской Федерации).

3. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[44] (регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам).

4. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[45] (действие федерального закона распространяется на отношения, связанные с обеспечением доступа пользователями информации к информации о деятельности государственных органов и органов местного самоуправления).

5. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[46] (определяет основные принципы и содержание деятельности по обеспечению национальной безопасности).

6. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ.

---

[41] Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России: приказ Минюста России от 27 декабря 2012 г. № 237. Доступ из справ.-правовой системы «КонсультантПлюс».

[42] Рос. газ. 2006. 29 июля.

[43] Рос. газ. 2003. 10 июля.

[44] Рос. газ. 2004. 5 авг.

[45] Рос. газ. 2009. 13 февр.

[46] Рос. газ. 2010. 29 дек.

7. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (определяет правовую основу, принципы организации и основные направления государственной судебно-экспертной деятельности в гражданском, административном и уголовном судопроизводстве).

8. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (регламентирует условия и порядок производства судебных экспертиз по уголовным делам, проверке сообщений о преступлениях, а также экспертиз по делам об административных правонарушениях).

9. Инструкция по организации производства судебных экспертиз в судебно-экспертных учреждениях системы Министерства юстиции Российской Федерации, утвержденная приказом Минюста России от 20 декабря 2002 г. № 347 (определяет условия и порядок организации производства судебных экспертиз в государственных судебно-экспертных учреждениях системы Министерства юстиции Российской Федерации).

10. Методические рекомендации по производству судебных экспертиз в государственных судебно-экспертных учреждениях системы Министерства юстиции Российской Федерации, утвержденные Приказом Минюста России от 20 декабря 2002 г. № 346 (рекомендации используются при определении возможных сроков производства судебных экспертиз и составлении заключений).

Соответственно, деятельность ведомственных экспертных учреждений в целом урегулирована законодательством, однако деятельность иных экспертных учреждений, по мнению ряда исследователей-криминалистов[47], имеет проблемы законодательного регулирования, в частности, связанные с назначением и проведением судебных компьютерных экспертиз в экспертных учреждениях вне системы правоохранительных органов, а именно отсутствие:

– нормативных требований к квалификации эксперта, которому поручается производство судебной компьютерно-технической экспертизы;

– четких требований к экспертным учреждениям, которым поручается производство судебной компьютерно-технической экспертизы;

– руководящих инструкций, методик о порядке производства судебной компьютерно-технической экспертизы экспертными учреждениями.

При этом как в ведомственных, так и в негосударственных экспертных учреждениях доктринально, в соответствии с положениями общей теории су-

[47] Алиев Т.Т. Судебная экспертиза: проблемы и перспективы развития // Современное право. 2022. № 1. С. 79-83; См. также: Сысенко А.Р. Проблемы назначения и производства судебной компьютерно-технической экспертизы / А.Р. Сысенко, И.С. Смирнова, С.Е. Тимошенко // Сибирское юридическое обозрение. 2020. Т. 17. № 4. С. 523-533.

дебной экспертизы, процесс экспертного исследования состоит из нескольких последовательных и взаимосвязанных стадий: предварительное исследование, раздельное исследование, сравнительное исследование, стадия обобщения результатов исследования и формулирования выводов[48].

Следовательно, в заключении эксперта по результатам проводимой компьютерной экспертизы на основании существующих и апробированных в течение многих лет методик и правил можно выделить вводную часть, исследовательскую часть и выводы.

В настоящее время согласно п. 11 приложения № 2 к приказу МВД России от 29 июня 2005 г. № 511 компьютерную экспертизу составляет класс судебных экспертиз, фактически включающих ряд направлений (родов), которые нормативно не регламентированы:

– аппаратно-компьютерная;

– программно-компьютерная;

– информационно-компьютерная (данных);

– компьютерно-сетевая экспертизы[49].

Отметим также, что формируется новый род судебных компьютерно-технических экспертиз, а именно экспертиза устройств сотовой связи[50].

Для экспертизы компьютерной информации большое теоретическое и практическое значение имеет также существующая классификация типов объектов, которые исследуются экспертами:

1. Аппаратные средства[51] – персональные компьютеры, периферийные устройства, сетевые аппаратные средства, пейджеры, мобильные телефоны, встроенные системы на основе микропроцессорных контроллеров, иные комплектующие и микросхемы.

2. Информационно-компьютерные объекты – аудиофайлы (waw, mid, mp3 и др.), текстовые файлы (doc, xlsx, txt и др.), видеофайлы (mpg, mpeg и др.), графические файлы (bmp, gif, jpeg и др.), исполняемые файлы (com, exe, и др.) и др. файлы.

3. Программно-компьютерные объекты – системное программное обеспечение (операционные системы на базе Windows, Linux, IOS, Android и др.), вспомогательные программы (утилиты), средства разработки и отладки программ, служебная системная информация, прикладное программное обеспечение (текстовые и графические редакторы).

---

[48] Козменкова С.В., Тренина А.Ю. Признаки «финансовых пирамид» и значение роли эксперта-экономиста при их выявлении // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2019. № 17. С. 21-29.

[49] Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. 4-е изд., перераб. и доп. М.: Норма, ИНФРА-М, 2018. 576 с.

[50] Сергеева К.А. Значение классификации судебных экспертиз для судопроизводства // Материалы 4-й Междунар. науч.-практ. конф. «Теория и практика судебной экспертизы в современных условиях», г. Москва, 30-31 января 2013 г. М., 2013. С. 253-256.

[51] См.: ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования».

4. Сетевые информационные технологии, сети связи (технологическая система, включающая средства и линии связи, предназначенная для передачи всевозможной информации) – телефонные устройства (смартфоны, планшеты и др.), персональный компьютер (с доступом в Интернет), «смарт-телевизор» (с доступом в Интернет) и др.

Все задачи, которые ставятся эксперту лицом, осуществляющим предварительное расследование, определяются исходя из конкретного перечня вопросов в соответствующем документе – постановлении следователя о назначении судебной экспертизы либо определении суда в ходе проводимого судебного заседания.

На сегодняшний день не существует общепринятой, непротиворечивой и достаточно полной классификации методов проведения компьютерных экспертиз. Например, при производстве компьютерных экспертиз используется широкий диапазон общенаучных методов: эксперимент, измерение, описание, моделирование, метод аналогий и пр.

К настоящему времени практика использования определенных методов в ходе проведения компьютерных экспертиз в ведомственных организациях уже сложилась и наиболее важными из них при проведении компьютерных экспертиз являются следующие:

– визуальный метод исследования;

– метод тестирования компьютерных средств;

– метод замены комплектующих деталей.

Задачами проведения компьютерной экспертизы, назначаемой при расследовании преступлений в сфере информационно-коммуникационных технологий, как правило, являются:

– установление тождества или его отсутствия между идентифицирующим и идентифицируемым объектом;

– диагностика представленного объекта в ходе производства компьютерной экспертизы;

– поиск на электронном носителе информации цифровых следов преступной деятельности.

При этом вопросы, выносимые на разрешение компьютерной экспертизы, должны соответствовать общим требованиям, предъявляемым к вопросам, выносимым на судебную компьютерную экспертизу:

1. При постановке вопроса необходимо использовать устоявшийся понятийный аппарат, исключающий жаргонные и полупрофессиональные термины («винчестер», «логи», «взлом» и т.п.). В случае отсутствия терминов, определенных законодательными или нормативными актами, необходимо использовать те термины, которые употребляют разработчики технических средств, программных продуктов в документации, описаниях, справках и т.п.[52]

2. Вопрос должен быть четким и однозначным.

[52] Саенко Г.В, Тушканова О.В. Компьютерная экспертиза. Исследование компьютерной информации. М.: ЭКЦ МВД России, 2010. С. 15.

3. Формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов является обязательным этапом исследования информации).

4. Вопросы не должны носить справочный характер.

5. Вопросы не должны носить правовой характер и выходить за пределы компетенции эксперта.

6. Вопросы должны соответствовать существующей методической и технической базе.

7. Использование терминологии, определенной ГОСТ 15971-90 «Системы обработки информации. Термины и определения»[53], ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»[54], ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения»[55] и иными нормативными актами. В случае отсутствия нормативного определения того или иного термина необходимо использовать терминологию, применяемую разработчиками аппаратных средств и программных продуктов в технической документации.

8. Вопросы, определяемые для компьютерной экспертизы, не должны носить правового характера в соответствии с п. 4 Постановления Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28[56].

9. Вопросы должны соответствовать представляемым на исследование объектам.

В настоящее время при назначении компьютерных экспертиз наиболее распространенными являются информационно-поисковые задачи по исследованию компьютерной информации, содержащейся на электронных носителях и соответствующей определенным критериям.

В ходе решения экспертных задач, определенных с целью проведения компьютерных экспертиз, в данное время актуальны следующие программные устройства, используемые при исследовании компьютерной информации, аппаратных средств (компьютер, носители информации и др.) как в ведомственных организациях, так и в иных в экспертных учреждениях:

1. «Autopsy» – программа с открытым исходным кодом и графическим интерфейсом для эффективного криминалистического исследования жестких магнитных дисков и смартфонов (анализ электронных писем, определение типа файла, воспроизведение мультимедиа, анализ реестра, восстановление фотографий, находящихся на карте памяти, извлечение данных из устройств на Android: SMS, журнал звонков, контакты и др.).

---

[53] Доступ из справ.-правовой системы «КонсультантПлюс».

[54] Там же.

[55] Там же.

[56] О судебной экспертизе по уголовным делам: постановление Пленума Верховного Суда РФ от 21 декабря 2010 г. № 28: ред. от 29 июня 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».

2. «Magnet RAM Capture» – позволяет получить снимок оперативной памяти и проанализировать артефакты в памяти. Программа работает с ОС Windows.

3. «RAM Capturer by Belkasoft» – это инструмент для создания дампа[57] данных энергозависимой памяти компьютера. Программа совместима с Windows. Дамп памяти может содержать находящиеся на зашифрованных томах пароли и данные для входа в электронную почту или социальные сети.

4. «Network Miner» – инструмент сетевого криминалистического анализа для Windows, Linux и MAC OS X позволяет определить операционную систему, имя хоста, обнаружить сессии и открытые порты с помощью анализатора трафика или PCAP-файла. Network Miner отображает извлеченные артефакты в интуитивно понятном интерфейсе.

5. «FAW» (Forensics Acquisition of Websites) – используется для сбора данных о веб-странице в целях дальнейшего исследования. В инструменте реализован ряд функций: сохранение страницы частично или полностью, сохранение всех видов изображений, сохранение исходного HTML веб-страницы и др.

6. «HashMyFiles» – криминалистический инструмент вычисляет хеши MD5 и SHA1, программный продукт работает почти на всех последних версиях Windows.

7. «ExifTool» – с помощью ExifTool можно считывать, записывать и редактировать метаданные разных видов файлов, в том числе EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Photoshop IRB, FlashPix, и т.д.

8. «Мобильный криминалист» (ООО «Оксиджен Софтвер», Россия) – в настоящее время самый мощный отечественный программный комплекс, включающий в себя ряд программных продуктов по работе с извлечением данных и их анализом: мобильные устройства, облачные сервисы, персональные компьютеры, аналитический функционал.

9. «PALADIN Forensic Suite» – самый востребованный набор криминалистических инструментов на базе операционных систем «Linux» в мире, представляющий собой модифицированный дистрибутив Linux, основанный на Ubuntu и доступный в 32-разрядной и 64-разрядной версиях.

10. «FTK Imager» – программное обеспечение, используемое для создания файлов образов дисков или монтирования образов дисков или устройств хранения, выполнения анализа структуры диска, восстановления данных и др. Программное обеспечение позволяет находить потерянные файлы или искать данные путем сканирования образа диска по ключевым словам. Также программное средство позволяет работать эксперту с образом (дампом) оперативной памяти.

[57] Дамп – содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы.

Вопросы для самоконтроля

1. Перечислите типовые версии преступлений в сфере информационно-коммуникационных технологий.

2. Укажите необходимые мероприятия, проводимые на подготовительном этапе расследования преступлений, совершённых с использованием современных информационно-коммуникационных технологий.

3. Определите, какие данные должны быть отражены в протоколе осмотра места происшествия при расследовании преступлений, совершённых с использованием современных информационно-коммуникационных технологий?

4. Перечислите способы изъятия компьютерной информации.

5. Перечислите лиц, которые должны принимать участие в осмотре места происшествия в рамках расследования преступлений, совершённых с использованием современных информационно-коммуникационных технологий.

6. Укажите способы подключения носителей информации к компьютеру.

7. Укажите, какие обстоятельства необходимо установить в ходе допроса заявителя и потерпевшего.

8. Укажите, какие обстоятельства необходимо установить в ходе допроса свидетелей.

9. Определите алгоритм заключительного этапа расследования преступлений, совершённых с использованием современных информационно-коммуникационных технологий.

10. Перечислите виды судебно-компьютерных экспертиз.

11. Укажите объекты исследования при производстве судебно-компьютерных экспертиз.

12. Перечислите предметы, исследуемые при производстве информационно-технологической экспертизы.

13. Сформулируйте задачи информационно-технологической экспертизы.

14. Перечислите вопросы, решаемые в рамках судебно-компьютерной экспертизы по исследованию аппаратных средств.

15. Перечислите вопросы, решаемые в рамках судебно-компьютерной экспертизы по исследованию программных средств.

16. Перечислите вопросы, решаемые в рамках судебно-компьютерной экспертизы по исследованию информации (данных).

17. Перечислите вопросы, решаемые в рамках судебно-компьютерной экспертизы комплексного исследования компьютерной системы (при экспертизе целостной компьютерной системы).

Задания для самостоятельной работы

1. Потерпевшим Б. были предоставлены USB флеш-накопители, которые могли быть заражены вирусным программным обеспечением (рис. 1).

Составьте протокол осмотра предоставленных USB флэш-накопителей. По результатам осмотра примите процессуальное решение, касающееся указанных накопителей.

Рис. 1. USB флеш-накопители[58]

2. В ходе проведения следственных действий по уголовному делу, возбужденному в отношении неустановленного лица по признакам состава преступления, предусмотренного ч. 2 ст. 274 УК РФ, были изъяты: 1) три USB флеш-накопителя; 2) накопитель на жестких магнитных дисках; 3) мобильный телефон (рис. 2-4).

Составьте протокол осмотра изъятых объектов, вынесите постановление о назначении судебной экспертизы.

Рис. 2. USB флеш-накопители[59]

[58] Изображение получено из поисковой системы «Яндекс».
[59] Там же.

Рис. 3. Накопитель на жестких магнитных дисках[60]

Рис. 4. Мобильный телефон[61]

3. В отношении гр-на А. было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 3 ст. 274.1 УК РФ. В ходе обыска по месту жительства гр-на А. были обнаружены и изъяты: SSD накопитель, USB флеш-накопитель, мобильный телефон, ноутбук, роутер (маршрутизатор) (рис. 5-9).

Составьте протокол осмотра изъятых объектов, по результатам осмотра примите процессуальное решение, касающееся изъятых объектов.

Определите наличие (отсутствие) необходимой информации, при ее отсутствии укажите на недостающую информацию об изъятых объектах.

Будет ли достаточно изъятых объектов для установления обстоятельств совершённого гр-ном А. преступления, предусмотренного ч. 3 ст. 274.1 УК РФ? (Ответы должны быть развернутыми и обоснованными).

Рис. 5. SSD накопитель[62]

[60] Изображение получено из поисковой системы «Яндекс».
[61] Там же.
[62] Там же.

Рис. 6. USB флеш-накопитель[63]

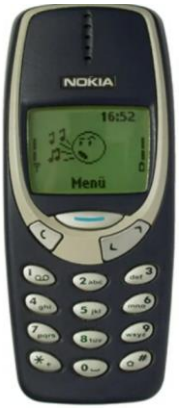

Рис. 7. Мобильный телефон[64]

Рис. 8. Ноутбук[65]

Рис. 9. Роутер (маршрутизатор)[66]

4. Гр-ну А. было предъявлено обвинение, предусмотренное ч. 2 ст. 242 УК РФ. Гр-н А. вину не признал и в ходе допроса пояснил, что в конце ноября 2020 г. его страница в социальной сети «VK» была взломана, он не имел доступа к информации на своей странице, именно в тот период на его

[63] Изображение получено из поисковой системы «Яндекс».
[64] Там же.
[65] Там же.
[66] Там же.

странице неустановленными лицами были размещены порнографические материалы.

Составьте алгоритм действий следователя, план следственно-оперативных мероприятий. Установите виновность гр-на А. в инкриминируемом ему деянии.

5. От гр-на Б., действующего в интересах ООО «Вектор», поступило заявление следующего содержания: «В период с 1 января 2021 г. по 2 января 2021 г. неизвестное лицо неустановленным способом получило неправомерный доступ к клиентской базе ООО «Вектор» и удалило все имеющиеся сведения из указанной базы. В результате действий неизвестного лица ООО «Вектор» нанесен материальный ущерб на сумму не менее 150 000 руб. Прошу установить виновное лицо и привлечь к ответственности.».

От имени следователя соберите первоначальный материал доследственной проверки. Квалифицируйте действия неизвестного лица. На основании полученных материалов примите процессуальное решение. Составьте план оперативно-следственных действий.

6. От гр-на В., действующего в интересах ООО «Плюс», поступило заявление следующего содержания: «В период времени с 00 часов 00 минут 1 марта 2021 г. до 23 часов 59 минут 2 марта 2021 г. неизвестное лицо неустановленным способом получило неправомерный доступ к локально-вычислительной сети ООО «Плюс» и внесло изменения в данные, хранящиеся на серверах компании, а также заблокировало часть из них. Прошу установить виновное лицо и привлечь к ответственности.».

От имени следователя соберите первоначальный материал доследственной проверки. Квалифицируйте действия неизвестного лица. На основании полученных материалов примите процессуальное решение. Составьте план оперативно-следственных действий.

7. От гр-на Г. поступило заявление следующего содержания: «25 апреля 2021 г. в неустановленное время неизвестное лицо получило неправомерный доступ к моей странице в социальной сети «VK», после чего, действуя от моего имени, осуществляло рассылку рекламных спам-писем по моим контактам до 15 часов 00 минут 30 апреля 2021 г. Прошу установить виновное лицо и привлечь к ответственности.».

От имени следователя соберите первоначальный материал доследственной проверки. Квалифицируйте действия неизвестного лица. На основании полученных материалов примите процессуальное решение. Составьте план оперативно-следственных действий.

ЗАКЛЮЧЕНИЕ

Информатизация органов предварительного расследования оказывает непосредственное влияние на повышение качества правоохранительной деятельности при раскрытии преступлений в сфере информационно-коммуникационных технологий.

На наш взгляд, одной из главных проблем совершенствования деятельности органов предварительного следствия и дознания является то, что созданные на сегодняшний день базы данных зачастую содержат лишь криминалистически значимую информацию. В указанных базах данных отсутствуют сведения о деятельности юридических и физических лиц. Отсутствие информации о динамике деятельности различных субъектов не позволяет проводить анализ, выявлять тенденции, сопоставлять оперативную информацию.

При расследовании преступлений необходимо применять не только криминалистически значимую информацию, но и пользоваться общегосударственными информационными ресурсами. Данный подход позволит оперативно и объективно производить анализ собранной и полученной информации, своевременно определять ее оперативную значимость и принимать верные тактические решения.

Актуальной задачей остается использование систем искусственного интеллекта при расследовании преступлений. На основе имеющихся данных интеллектуальные системы формируют и предлагают решения поставленных задач в автоматическом режиме, что позволяет сократить затрачиваемое служебное время на анализ и сопоставление имеющихся сведений.

Применение алгоритмов и систем искусственного интеллекта в базах и банках данных позволит преобразовать автоматизированное рабочее место сотрудника из «компьютера», который используется для составления и хранения документов, в современную информационную систему. Платформа используемой Единой системы информационно-аналитического обеспечения деятельности МВД Российской Федерации (ИСОД МВД России) позволяет реализовать алгоритмы систем искусственного интеллекта.

Считаем необходимым проведение анализа эффективности взаимодействия оперативных служб с центрами реагирования на инциденты в сфере информационной безопасности, что позволит проработать вопрос о возможности создания автоматизированных поисковых систем, в том числе на базе уже существующих, путем расширения функционала по предупреждению и пресечению киберпреступности, а также их интеграции с другими базами данных.

Учитывая специфику выявления преступлений, совершаемых в сфере информационно-коммуникационных технологий, стремительное распространение криминального использования виртуальных активов, компьютерных атак на критическую информационную инфраструктуру государства,

необходимо осуществлять специализацию сотрудников, их профессиональный отбор, добиваться устойчивого повышения раскрываемости преступлений.

Учитывая трансграничный характер киберпреступлений, необходимо более эффективно использовать возможности специализированных сетей правоохранительных органов, международного полицейского взаимодействия и сотрудничества в области уголовного судопроизводства.

Кроме того, необходимо совершенствовать действующее законодательство в части расширения признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия «электронного доказательства», процедур внесудебной блокировки «зеркал» ранее заблокированных сайтов, а также по ряду других вопросов.

Фактором, оказывающим влияние на качество расследования преступлений в сфере информационно-коммуникационных технологий, является подготовка компетентных кадров. На сегодняшний день отмечается недостаточный уровень квалификации сотрудников органов внутренних дел в этом направлении, что вызвано рядом особенностей расследования преступлений указанной категории, особенно технической составляющей. Подготовка в образовательных организациях системы МВД России компетентных кадров, привлекаемых к расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий, позволит разработать действенные алгоритмы предотвращения преступлений в сфере высоких технологий, а также значительно повысить качество предварительно расследования без дополнительного привлечения специалистов в данной области.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 дек. 2016 г. № 646. Доступ из справ.-правовой системы «Консультант Плюс».
2. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «ГАРАНТ».
3. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
4. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
5. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31 мая 2001 г. № 73-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
6. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ // Рос. газ. 2003. 10 июля.
7. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // Рос. газ. 2006. 29 июля.
8. О коммерческой тайне: федер. закон от 29 июля 2004 г. № 98-ФЗ // Рос. газ. 2004. 5 авг.
9. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон от 9 февр. 2009 г. № 8-ФЗ // Рос. газ. 2009. 13 февр.
10. О судебной экспертизе по уголовным делам: постановление Пленума Верховного Суда РФ от 21 дек. 2010 г. № 28. Доступ из справ.-правовой системы «КонсультантПлюс».
11. О безопасности: федер. закон от 28 дек. 2010 г. № 390-ФЗ // Рос. газ. 2010. 29 дек.
12. ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования».
13. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
14. ГОСТ Р 52292-2004. «Информационная технология. Электронный обмен информацией. Термины и определения».
15. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях ор-

ганов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России от 29 июня 2005 г. № 511. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2001. 70 с.

18. Белицкий В.Ю. Алгоритм первоначальных действий по делам о хищениях, совершённых с использованием сети «Интернет» // Вестник Барнаульского юридического института МВД России. 2017. 1(32). С. 139-141.

19. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. Москва, 2000. 72 с.

20. Гаврилин Ю.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. Москва: Акад. управления МВД России, 2019. 189 с.

21. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнова. Москва, 2001. 88 с.

22. Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие. Москва: ДГСК МВД России, 2017. 160 с.

23. Густов Г. А. Проблемы методов научного познания в организации расследования преступлений: автореф. дис. … д-ра юрид. наук. Москва, 1993. 52 с.

24. Долгова А.И. Криминология: учебник для вузов. Москва: Норма, 2005. 912 с.

25. Криминалистика: учебник для вузов / под ред. А.Ф. Волынского. Москва: Закон и право, ЮНИТИ-ДАНА,1999. 615 с.

26. Криминалистика: учебник / отв. ред. Н.П. Яблоков. Москва: Юристъ, 2001. 629 с.

27. Криминалистика: учебник для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская; под ред. Р.С. Белкина. Москва: НОРМА (Издательская группа НОРМА-ИНФРА М), 2002. 960 с.

28. Попов А.Н. Преступления в сфере компьютерной информации: учеб. пособие. Санкт-Петербург: Санкт-Петерб. юрид. ин-т (филиал) Университета прокуратуры Рос. Федерации, 2018. 67 с.

29. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования / А.Ф. Абдулвалиев, А.В. Белоусов, Ж.В. Вассалатий [и др.]: монография. Тюмень, 2021. 376 с.

30. Уголовное право. Особенная часть / под общ. ред. Л.М. Прозументова: учебник. Томск: Изд. дом Томского гос. ун-та, 2019. 480 с.

Дополнительная литература

1. Клепицкий И.А. Мошенничество и правонарушения гражданско-правового характера // Законность. 1995. № 7. С. 42.

2. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. Москва: Горячая линия – Телком, 2002. 336 с.

3. Мазуров И.В., Казанцев С.Я. Особенности изъятия компьютерной информации при расследовании хищений денежных средств, совершённых с использованием интернет-технологий // Закон и право. 2014. № 5. С. 119-121.

4. Поливанюк В. Особенности проведения допросов при расследовании преступлений, совершённых в сфере использования компьютерной информации. URL: http://nadzor.pk.ru

5. Комментарий к статье 29 УК РФ / рук. авт. коллектива С.А. Разумов // Законодательство России: [сайт]. URL: https://studopedia.ru

6. Рассолов И.М. Право и Интернет. Теоретические проблемы. Москва: Норма, 2009. 336 с.

7. Россинская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2010. 464 с.

8. Россинская Е.Р., Усов А.И. Компьютерно-техническая экспертиза. Москва: Право и закон, 2001. 414 с.

9. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук. Москва, 2015. 222 с.

10. Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. № 1 (1). С. 104-106.

11. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: дис. … канд. юрид. наук. Иркутск, 2006. 185 с.

12. Тропина Т.Л. Борьба с киберпреступностью: Возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86.

13. Хилюта В.В. Признаки мошеннического обмана в теории и практике уголовного закона // Криминологический журнал ГУЭП. 2009. № 2(8). С. 13-21.

14. Хисамова З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. … канд. юрид. наук. Краснодар, 2016. 222 с.

15. Чекунов И.Г. К вопросу о понятии и системе преступлений, совершаемых с использованием компьютерных сетей // Правовые вопросы связи. 2012. № 1. С. 18.

16. Шевко Р.Н. Проблемы подготовки специалистов по раскрытию и расследованию преступлений, совершённых с использованием современных информационных технологий, в образовательных организациях МВД России // Вестник Казанского юридического института МВД России. 2017. № 1(27). С. 87-89.

17. Шепитько В.Ю. Теоретические проблемы систематизации тактических приемов в криминалистике. Харьков, 1995. 418 с.

ПРИЛОЖЕНИЕ[67]
(к главе I)

Постановление Лефортовского районного суда города Москвы от 29.09.2016 по уголовному делу № 1-277/2016 в отношении Анисимова А.В., обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 274 Уголовного кодекса Российской Федерации (извлечение)

Лефортовский районный суд города Москвы в ходе судебного заседания по уголовному делу № 1-277/2016 в отношении Анисимова А.В., обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 274 Уголовного кодекса Российской Федерации, установил:

Настоящее уголовное дело подлежит возвращению прокурору для устранения препятствий его рассмотрения судом, так как обвинительное заключение составлено с существенными нарушениями требований уголовно-процессуального закона, что исключает возможность постановления судом приговора или вынесения иного решения на основе данного заключения.

В соответствии с п. 1 ч. 1 ст. 237 УПК РФ уголовное дело возвращается прокурору, если обвинительное заключение или обвинительный акт составлены с нарушением требований УПК РФ, что исключает возможность постановления судом приговора или вынесения иного решения на основании данного заключения или акта.

В соответствии со ст. 8 УК РФ основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного Уголовным кодексом РФ.

В силу п. 4 ч. 1 ст. 73 УПК РФ установление характера и размера вреда, причиненного преступлением, является необходимым условием вынесения законного и обоснованного решения.

Так, Анисимов А.В. обвиняется в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ, а именно в том, что совершил нарушение правил эксплуатации средств хранения и передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, причинившее крупный вред.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшем уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившие крупный ущерб, состав преступления является материальным, при этом необходимым его элементом является причинение крупного ущерба. Крупным ущербом в данном случае признается ущерб, сумма которого превышает один миллион рублей.

[67] Приложение приведено для учебных целей.

Между тем, как следует из обвинительного заключения и иных материалов уголовного дела, крупный ущерб был установлен органами предварительного расследования исходя из справки об ущербе (представленной потерпевшим ООО «Приват Трэйд»), согласно которой ущерб выразился в вынужденных действиях, а именно в восстановлении доступа к базе данных ООО «Приват Трэйд» после смены всех паролей сотрудников, проведении комплекса мероприятий, направленных на поиск лица, которое копировало информацию, покупке оборудования для сотрудников ООО «Приват Трэйд», введении дополнительных средств учета лиц, осуществляющих доступ к базе данных ООО «Приват Трэйд», всего на общую сумму 1 155 600 рублей, что противоречит требованиям закона. Фактическая стоимость скопированной компьютерной информации органами предварительного расследования не устанавливалась.

Исходя из изложенного, суд приходит к выводу, что указанные выше нарушения не могут быть устранены в ходе судебного разбирательства и препятствуют рассмотрению уголовного дела.

Суд пришел к выводу, что настоящее уголовное дело подлежит возвращению прокурору для устранения препятствий его рассмотрения судом, так как обвинительное заключение составлено с существенными нарушениями требований уголовно-процессуального закона, что исключает возможность постановления судом приговора или вынесения иного решения на основе данного заключения, поскольку органами предварительного расследования достоверно и документально не установлен размер ущерба, причиненного преступлением, что служит препятствием к рассмотрению дела по существу и является основанием к возвращению уголовного дела прокурору для принятия им решения по делу в соответствии с уголовно-процессуальным законом.

ПРИЛОЖЕНИЕ[68]
(к главе II)

Перечень вопросов, решаемых в рамках судебной компьютерно-технической экспертизы

1. Вопросы по исследованию аппаратных средств:

– Относится ли представленное устройство к аппаратным компьютерным средствам?

– К какому типу (марке, модели) аппаратов относится средство? Каковы его технические характеристики и параметры?

– Каково функциональное предназначение представленного аппаратного средства?

– Какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство?

– Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения от типовых (нормальных) параметров, в том числе физические дефекты?

– Является ли неисправность данного средства следствием нарушения определенных правил эксплуатации?

– Каковы причины изменения функциональных (потребительских) свойств в начальной конфигурации представленного аппаратного средства?

– Является ли представленное аппаратное средство носителем информации?

– Какой вид (тип, модель, марку) имеет представленный носитель информации?

– Доступен ли для чтения представленный носитель информации?

2. Вопросы по исследованию программных средств:

– Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит?

– Обладают ли программные средства признаками контрафактности?

– Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)?

– Какое общее функциональное предназначение имеет программное средство и является ли оно вредоносным?

– Какова совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы?

– Имеются ли в программном средстве отклонения от нормальных параметров (например, свойства инфицирования, недокументированных функций)?

---

[68] Приложение приведено для учебных целей (за основу взяты вопросы, приведенные в работе Россинской Е.Р., Усова А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. 414 с.).

– Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования?

– Имеются ли на носителях информации тексты (коды) с первоначальным состоянием программы?

– Подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием?

– Какой вид имело программное средство до его последней модификации?

– С какой целью было произведено изменение каких-либо функций в программном средстве?

– Направлены ли внесенные изменения в программное средство на преодоление его защиты?

– Каким способом были произведены изменения в программе (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.)?

– Имеются ли в программном средстве «враждебные» функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы?

– Правильна ли начальная настройка программы бухгалтерского учета и корректны ли действия пользователя?

3. Вопросы по исследованию информации (данных):

– Как отформатирован носитель информации, и в каком виде на него записаны данные?

– Каковы характеристики физического и логического размещения данных на носителе информации?

– Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?

– Какого вида (явный, скрытый, удаленный, архив) имеется информация на носителе?

– К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и др.) и какими программными средствами они обеспечиваются?

– Каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики?

– Какие свойства, характеристики имеют выявленные средства защиты данных и какие возможны пути ее преодоления?

– Какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации?

– Каково содержание защищенных данных?

– Какие несоответствия типовому представлению имеются в выявленных данных (нарушение целостности, несоответствие формата, вредоносные включения и пр.)?

– Каковы пользовательские (потребительские) свойства и предназначение данных на носителе информации?

– Какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа и пр.) имеются на носителях информации?

– Какие данные представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации?

– Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами находились определенные данные до их удаления или модификации)?

– Каким способом и при каких обстоятельствах произведены действия (операции) (блокирование, модификация, копирование, удаление) определенных данных на носителе информации?

– Какая причинная связь имеется между действиями (вводом, модификацией, удалением и пр.), данными и имевшим место событием (например, нарушение в работе компьютерной системы, в том числе сбои в программном и аппаратном обеспечении)?

– Какова степень соответствия (или несоответствия) действий с конкретной информацией специальному регламенту или правилам эксплуатации определенной компьютерной системы?

4. Вопросы комплексного исследования компьютерной системы (при экспертизе целостной компьютерной системы):

– Является ли представленное оборудование компьютерной системой?

– Является ли представленное оборудование целостной компьютерной системой или же ее частью?

– К какому типу (марке, модели) относится компьютерная система?

– Какой состав (конфигурацию) и технические характеристики имеет компьютерная система?

– Какое функциональное предназначение имеет компьютерная система?

– Имеет ли компьютерная система какие-либо отклонения от типовых (нормальных) параметров, в том числе физические (механические) дефекты?

– Какие эксплуатационные режимы задействованы (установлены) в компьютерной системе?

– Существуют ли в компьютерной системе недокументированные (сервисные) возможности? Какие это возможности?

– Какие носители информации имеются в представленной компьютерной системе?

– Реализована ли в компьютерной системе какая-либо система защиты информации?

– Какая система защиты информации имеется в представленной компьютерной системе? Каков тип, вид и характеристики этой системы защиты? Каковы возможности по ее преодолению?

– Какова стоимость производственных и эксплуатационных дефектов компьютерных средств?

Для заметок

Учебное издание

Коптяев Алексей Юрьевич

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Редактирование *Е.А. Пыжова*
Дизайн обложки *Е.К. Булатова*
Тиражирование *А.И. Кубрина*

Подписано в печать 24.06.2022. Формат 60х84/16.
Уч.-изд. л. 5,0. Заказ № 030.
Тираж 80 экз. Цена свободная.

Научно-исследовательский и редакционно-издательский отдел
Тюменского института повышения
квалификации сотрудников МВД России
625049, г. Тюмень, ул. Амурская, 75.

ISBN 978-5-93160-331-5