ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

ОСОБЕННОСТИ ПРОИЗВОДСТВА ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПУТЕМ КИБЕРАТАК (СЕТЕВЫХ АТАК)

Учебно-практическое пособие

Воронеж
2024

ББК 67.99
УДК 343.1

Коллектив авторов: Е. А. Пидусов, В. А. Мещеряков, А. И. Гайдин, П. Г. Смагин, М. М. Жуков, А. Ю. Телков, А. Е. Васильев.

Рецензенты:

О. К. Исаева – заместитель начальника отдела экспертно-криминалистических учетов ЭКЦ ГУ МВД России по Воронежской области, кандидат юридических наук, подполковник полиции;

Н. А. Лещева – старший следователь по особо важным делам контрольно-методического отдела ГСУ ГУ МВД России по Воронежской области, подполковник юстиции.

Особенности производства предварительного следствия по уголовным делам о преступлениях, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак (сетевых атак) / Е. А. Пидусов [и др.]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2024. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

Учебно-практическое пособие предназначено для использования в практической деятельности органов предварительного следствия и дознания, а также в деятельности научных работников, профессорско-преподавательского состава, курсантов и слушателей образовательных организаций МВД России.

ISBN 978-5-00229-118-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Использование информационных технологий при совершении преступлений является наиболее ярким признаком, характеризующим качественное состояние современной преступности.

За последние 5 лет уровень криминализации в сфере информационных технологий значительно вырос. Так, в 2018 году выявлено 174,7 тыс. преступлений данной категории, в 2019 г. – 294,5 тыс., в 2020 г. – 510,4 тыс., в 2021 г. – 517,7 тыс., в 2022 г. – 522,1 тыс. Как результат, в настоящее время каждое четвертое преступление в России совершается с использованием ИТ-технологий, их доля в общей структуре преступности составляет 26,5%. При этом, нет оснований полагать, что существующая тенденция изменится в лучшую сторону.

Наиболее интенсивная динамика выявления характеризует преступления, связанные с неправомерным доступом к компьютерной информации. Только с 2020 по 2022 год рост регистрации указанных деяний составил +294% (с 3,7 до 10,9 тыс.), а за 9 месяцев 2023 года этот показатель уже достиг +224% к аналогичному периоду прошлого года, составив 19,3 тыс. преступлений (АППГ 6 тыс.).

Всего в истекшем периоде 2023 года в производстве правоохранительных органов находились уголовные дела о 22 тыс. преступлений, предусмотренных ст. 272 УК РФ, из которых предварительно расследованы только 922, в том числе следователями ОВД окончены с направлением в суд 532 уголовных дела (+6,8%, АППГ 498).

По реабилитирующим основаниям следователями ОВД прекращены уголовные дела о 10 преступлениях (-33,3%, АППГ 15). Предварительное следствие по п.п.1, 2 ч.1 ст. 208 УПК РФ следователями ОВД приостановлено по уголовным делам о 13 812 преступлениях (+221,1%, АППГ 4 301).

При этом следует учитывать, что статистические данные не в полной мере отражают складывающуюся криминогенную обстановку, диссонируют с числом компьютерных атак, возникших в результате компьютерных инцидентов, повлекших нарушение и (или) прекращение функционирования информационных ресурсов. Во многих случаях эти инциденты связаны с внедрением вредоносного программного обеспечения.

Организация работы по предотвращению, раскрытию и расследованию преступлений, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак, является одним из приоритетных направлений в области борьбы с преступностью. Для реализации эффективных алгоритмов деятельности следователей по раскрытию и расследованию преступлений, связанных с неправомерным доступом к компьютерной информации, необходима разработка соответствующего методического пособия.

Основной целью данной работы является формирование обоснованных практических рекомендаций для их использования следователями при производстве предварительного расследования по уголовным делам о преступлениях, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак.

Разработанные рекомендации предназначены для использования в практической деятельности органов предварительного следствия и дознания, в деятельности научных работников, профессорско-преподавательского состава, курсантов и слушателей образовательных организаций МВД России.

1. Криминалистически значимые признаки механизма неправомерного доступа к компьютерной информации

Неправомерный доступ к компьютерной информации – уголовно наказуемое деяние, предусмотренное ст. 272 УК РФ. Диспозиция данной статьи закрепляет юридически значимые признаки деяния. Рассмотрим некоторые из них.

Понятие «неправомерность доступа к компьютерной информации» является сложносоставным. Для его понимания необходимо проанализировать такие правовые категории, как «информация», «компьютерная информация», «охраняемая законом компьютерная информация», «доступ к компьютерной информации», «неправомерный доступ к компьютерной информации» и некоторые другие.

В основе понятия компьютерной информации лежит категория «информация» (сведения, изложение, разъяснения), под которой понимаются сведения, воспринимаемые информационными системами и относящиеся
к окружающим явлениям и объектам, их свойствам, характеристикам и состояниям.

Легальное определение дефиниции «информация» дано в положениях ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] как сведения (сообщения, данные) независимо от формы представления.

В последнее время все чаще употребляется термин «цифровая информация» как более широкое, чем понятие «компьютерная информация».

Следует учитывать, что в диспозиции ст. 272 УК РФ говорится именно об охраняемой законом компьютерной информации, к которой относят информацию ограниченного доступа, включая сведения, составляющие государственную, коммерческую, служебную и иную тайну, а также конфиденциальную информацию. Это информация, для которой законодателем установлен специальный режим правовой защиты.

Перечень сведений, составляющих государственную тайну, установлен Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»[2], и включает сведения из военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности государства.

Перечень конфиденциальных сведений утвержден Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня

---

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс». (Далее – Закон об информации).

[2] О государственной тайне : закон РФ от 21.07.1993 № 5485-1 // СПС «КонсультантПлюс».

сведений конфиденциального характера»[1]. К категории конфиденциальных сведений отнесены, в частности, персональные данные, сведения, составляющие тайну следствия и судопроизводства, сведения о мерах государственной защитыи защищаемых лицах. Иной тайной признаются сведения ограниченного доступа: налоговая, банковская, нотариальная, адвокатская, врачебная и некоторые другие виды тайн.

Применяя данный признак, необходимо руководствоваться и положениями постановления Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». В частности, Верховный Суд РФ указал, что по смыслу ч. 1 ст. 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения её к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за её разглашение, *так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение её целостности и (или) доступности*[2].

Следующим, представляющим интерес, является термин «доступ к компьютерной информации». Официальное определение данного понятия содержится в положениях п. 6 ст. 2 Закона об информации как «возможность получения информации, и её использования». При этом здесь предполагается применение любой формы проникновения в источник информации с помощью средств, в виде электрических сигналов, в результате чего становится возможным выполнение манипуляций с полученной информацией (ее копирование, модифицирование, блокировка или уничтожение)[3].

Важно отметить, что принципиальным является доступ именно к компьютерной информации, а не только к её носителю.

---

[1] Об утверждении Перечня сведений конфиденциального характера : указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) // СПС «КонсультантПлюс».

2 О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «КонсультантПлюс».

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова. М. : Проспект, 2022. Т. 2. С. 643.

Особое значение представляет понятие «неправомерный доступ к компьютерной информации», четкая трактовка которого необходима для анализа способов совершения и сокрытия данного преступления в механизме его совершения. Неправомерность доступа предполагает отсутствие у лица права на получение и использование информации.

Она всегда выражается в совершении тех или иных действий, в частности:

− применение специальных технических или программных средств, позволяющих преодолеть установленные системы защиты компьютерной информации;

− незаконное использование действующих паролей законного пользователя или маскировка под его видом для проникновения в компьютер, его систему;

− хищение носителей компьютерной информации, если пользователем были приняты меры по охране этих носителей, а преступные действия повлекли уничтожение или блокирование данной компьютерной информации;

− нарушение установленного порядка правил доступа к информации или действий с ней с применением штатных средств информационной системы (ИС) или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

Так, по одному из уголовных дел заключением эксперта установлено, что программное обеспечение «Intercepter-NG», использовавшееся для неправомерного доступа к охраняемой законом компьютерной информации, имеет возможности перехвата трафика, его анализа, а также включает различные методы организации MITM-атак[1].

Наиболее ёмкой и обширной представляется позиция И. Н. Васильева, которым заключено, что доступ к компьютерной информации будет неправомерным, когда лицо не наделено правом на доступ к этой информации либо вправе осуществлять доступ к компьютерной информации, но делает это с нарушением установленного порядка и правил её защиты (имеет место использование лицом своего служебного положения)[2].

Далее следует обратить внимание, что неправомерность доступа к компьютерной информации будет иметь уголовно наказуемый характер, если это деяние повлекло наступление последствий, указанных в диспозиции ч. 1 ст. 272 УК РФ (уничтожение данной информации, её блокирование, модификацию или копирование).

Одним из основных элементов механизма неправомерного доступа к компьютерной информации является личность преступника

---

[1] Определение Первого кассационного суда общей юрисдикции от 21.04.2020 № 77-530/2020 // СПС «КонсультантПлюс».

[2] Васильева И. Н. Расследование инцидентов информационной безопасности : учебное пособие. СПб. : Изд-во СПбГЭУ, 2019. С. 7.

как индивидуальное выражение его социально-значимых свойств.

В большинстве случаев они оказываются учащимися высших учебных заведений или занимают должности технических специалистов (например, программисты)[1]. Могут быть охарактеризованы как лица с высоким профессионализмом, нестандартным мышлением, изобретательностью[2].

Основной чертой таких лиц являются глубокие познания в области компьютерных и информационных технологий. Однако среди них есть и дилетанты. Исследователями отмечается, что многие раскрытые компьютерные преступления, включая неправомерный доступ к компьютерной информации, совершаются специалистами низкой квалификации, не имеющими достаточных знаний для сокрытия следов своих противоправных действий.

Мотивы и цели при совершении рассматриваемого преступления достаточно разнообразны. Это могут быть корысть, хулиганские побуждения, желание скрыть факт совершения другого (более тяжкого) преступления, отмщение, не исключаются и политические мотивы[3].

Например, Ч. С. Л. совершил неправомерный доступ к компьютерной информации путем уничтожения электронных файлов базы данных 1С «…» с целью причинения ущерба ООО «С» и по мотиву мести, что было вызвано имеющимся между ним и его бывшим работодателем конфликтом[4].

И все же самым распространенным является корыстный мотив. Так, Н. из корыстной заинтересованности реализовал смарт-карту «Триколор ТВ», установку и настройку через приемник спутникового сигнала к системе спутникового телевидения НАО «НСК» за вознаграждение в размере 2 000 рублей, чем совершил неправомерный доступ к компьютерной информации, повлекший её копирование. Преступными действиями Н. причинен материальный ущерб на сумму 11 688 рублей НАО «НСК»[5].

Нельзя не отметить, что развитие и повсеместное использование социальных сетей обусловливает активное размещение в них

---

[1] Жоров Е. Д., Тепляшин П. В. Особенности криминалистической характеристики личности лица, совершающего неправомерный доступ к компьютерной информации // Эпоха науки. 2018. № 14. С. 71.

[2] Захарова А. В. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации // Бюллетень магистранта. 2019. № 5. URL: https://bm.muh.ru/wp-content/mags/bm052019/ 54bm (дата обращения: 04.05.2023).

[3] Ловцов Д. А. Информационное право: учебное пособие. − М.: РАП, 2019. − С. 165.

[4] Приговор Бабушкинского районного суда г. Москвы от 20.09.2016 по делу № 01-0313/2016. URL: https://sud-praktika.ru/precedent/97705.html (дата обращения: 06.05.2023).

[5] Приговор Хасавюртовского городского суда Республики Дагестан № 1-261/2020 от 20.07.2020 по делу № 1-261/2020. URL: https://sudact.ru/regular/doc/SlYwK6TxKKNT/ (дата обращения: 06.05.2023).

пользователями информации о своей частной жизни, на которую злоумышленники и совершают посягательства. В таких случаях нередко ведущим становится мотив ревности со стороны близких (знакомых) жертв неправомерного доступа.

Важнейшим элементом механизма неправомерного доступа к компьютерной информации является способ совершения преступления. Он имеет не только криминалистическое, но и уголовно-процессуальное значение, вследствие чего отнесен законодателем к предмету доказывания по уголовному делу (пп. 1 п. 1 ст. 73 Уголовно-процессуального кодекса Российской Федерации[1] (далее − УПК РФ)).

Неправомерный доступ к компьютерной информации совершается следующими способами:

– непосредственный доступ;

– удаленный доступ;

– комплексно (удаленно и непосредственно одновременно).

Способы первой группы включают, например, ввод известных злоумышленнику логина и пароля непосредственно через компьютер жертвы[2].

В случаях непосредственного доступа компьютерная информация копируется, блокируется, модифицируется, уничтожается; происходит нарушение работы компьютера, компьютерных систем или сетей. Для этого даются соответствующие команды непосредственно с компьютера, где содержится информация (предмет посягательства).

Вторая группа охватывает способы удаленного доступа, совершаемого посредством использования ресурсов сети Интернет или локальной компьютерной сети. Соответствующая совокупность способов может быть обозначена как способы кибератак или сетевые атаки.

Третья группа включает способы неправомерного доступа, совершаемого как непосредственно, так и опосредованно. Здесь можно выделить следующие способы: внедрение в компьютерные программы набора команд, приводимых в действие по определенному сигналу; использование вредоносной компьютерной программы (например, сетевые черви, «троянский конь», хакерские утилиты); использование уязвимостей в компьютерной системе (брешей, дыр, люков).

Самыми распространенными являются способы неправомерного удаленного доступа к компьютерной информации. Данные способы связаны с использованием программы удаленного управления компьютерным устройством (например, TeamViewer, Real VNC, AnyDesk, Ammyy Admin,

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс»

[2] Савельева А. А. О способах совершения неправомерного доступа к компьютерной информации // Молодой ученый. 2020. № 48 (338). С. 328.

Radmin, RMS)[1].

Получение удаленного доступа к компьютерному устройству позволяет управлять им: запускать установленные приложения, менять настройки, просматривать, редактировать и копировать файлы.

Способы удаленного доступа можно сгруппировать в две основные группы:

1) преодоление парольной, программной, технической защиты с последующим подключением к чужой компьютерной системе;

2) перехват информации.

Первая выделенная группа включает:

а) подключение к линии связи законного пользователя;

б) использование чужих реквизитов идентификации под видом законного пользователя;

в) использование вредоносных компьютерных программ.

Так, К. Г. С., путем подбора и ввода ответа на секретный вопрос («Девичья фамилия мамы») совершила неправомерный доступ к компьютерной информации, содержащейся в электронном почтовом ящике потерпевшей, после чего блокировала доступ к компьютерной информации посредством изменения пароля[2].

Как представляется, главным отличием перехвата от несанкционированного доступа является то, что электромагнитный перехват совершается в отношении компьютерной (цифровой) информации, обращающейся в пространстве, а неправомерный доступ к информации обусловливает необходимость нарушения системы её защиты[3].

Далее следует отметить, что способы совершения неправомерного доступа к компьютерной информации находятся в тесной взаимосвязи со способами его сокрытия.

Совершая неправомерный доступ к компьютерной информации, преступники предпринимают активные действия по сокрытию следов преступления, совершенного как способами непосредственного доступа, так и удаленного.

В случае непосредственного доступа сокрытие преступления состоит в восстановлении предпреступной обстановки, что предполагает не только действия в цифровом пространстве (закрытие использованных документов и программ, очистка в браузере кеш-памяти и удаление файлов cookie и др.), но и физическое уничтожение оставленных следов (в частности,

---

[1] Программы для удаленного доступа к компьютеру. − URL: https://lifehacker.ru (дата обращения: 08.06.2023).

[2] Приговор Дзержинского районного суда г. Оренбурга Оренбургской области от 28.01.2019 по делу № 1-504/2018. – URL: https://sudact.ru/regular/doc/smPVc9O2vldJ/ (дата обращения: 04.05.2023).

[3] Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации : монография. Казань : Познание, 2020. С. 76.

микрочастиц, следов пальцев рук на клавиатуре, кнопках дисководов и других поверхностях, к которым прикасался преступник, следов обуви, оставленных на месте совершения преступления и вблизи него).

Специфика сокрытия удаленного (опосредованного) доступа заключена в самом способе совершения данного преступления на его начальном этапе, что достигается различными способами, которые весьма разнообразны.

К наиболее распространенным относятся:

− маскировка, сокрытие, подмена IP-адреса;

− использование Wi-Fi соединения в общественных местах;

− использование временных электронных почтовых ящиков;

− осуществление доступа с применением инструментов анонимизации (анонимных прокси-серверов, специализированных браузеров, расширений, плагинов)[1].

При совершении преступлений рассматриваемой категории применяются также следующие способы их сокрытия:

− шифрование файлов, содержащих информацию о преступном событии, шифрование электронной почты и пр.;

− удаление информации, хранящейся на электронных носителях и в памяти компьютера;

− хранение информации, связанной с совершенным преступлением, в облачном хранилище;

− установка пароля;

− установка программ, предназначенных для защиты компьютерной информации от постороннего доступа;

− использование вредоносных компьютерных программ для удаления файлов.

Структура механизма неправомерного доступа включает еще один элемент − типичную следовую картину. Данный элемент весьма специфичен, поскольку его составляют как традиционные следы, так и цифровые (электронные). При этом последние преобладают при удаленном доступе.

В случае неправомерного доступа к компьютерной информации следы в виде изменений внешней среды практически не сохраняются[2]. При совершении удаленного неправомерного доступа в памяти

---

[1] Пырьева Е. И. Способы и средства сокрытия неправомерного доступа к компьютерной информации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж : Воронежский институт МВД РФ, 2020. № 1 (6). С. 78.

[2] Ленков О. В. Производство осмотра места происшествия по делам о неправомерном доступе к компьютерной информации // Научные исследования. 2018. № 7. С. 55.

электронных устройств в большинстве случаев остаются «нетрадиционные» (электронно-цифровые) следы. Подобные следы являются типичными для рассматриваемых преступлений, как и многих других компьютерных преступлений, и носят преимущественно информационный характер, представляя собой определенные изменения в охраняемой законом компьютерной информации, наступившие в результате её уничтожения, модификации, копирования и (или) блокирования[1].

Понятие «электронно-цифровые следы неправомерного доступа» можно определить как зафиксированные в виде электронной формальной модели изменения в состоянии информации, содержащейся в памяти электронных устройств, обусловленные алгоритмом программного обеспечения
и связанные с преступным событием.

При неправомерном доступе через компьютерные сети электронно-цифровые следы остаются вследствие того, что система, через которую происходит проникновение, имеет определенную информацию, запрашиваемую этой системой у пользователя, который пытается соединиться с другим компьютерным устройством. Названная система определяет:

− IP-адрес как уникальный числовой идентификатор конкретного устройства, подключенного к интернету;

− применяемое программное обеспечение.

Поскольку в механизме неправомерного доступа задействованы компьютеры преступника и его жертвы, то следы данного деяния могут сохраняться на обоих устройствах. На компьютере преступника, с которого он совершил доступ, остаются следы в виде файлов, скопированных с компьютера жертвы, программ, используемых для неправомерного доступа, сообщений в электронной почте и другие.

По обнаруженным следам можно установить:

– время работы преступника на компьютере;

– время совершения удаленного доступа в сети Интернет;

– объем полученной информации с серверов и других компьютеров;

– содержание полученной информации в электронно-цифровой форме.

Начальный этап процесса следообразования при неправомерном доступе к компьютерной информации связан с вычислительной машиной злоумышленника, а завершающий этап – с наступлением последствий, предусмотренных ст. 272 УК РФ, на устройстве жертвы преступления. В данной цепи можно выделить промежуточные звенья, в которых остаются электронно-цифровые следы:

− сервер провайдера;

---

[1] Опшин В. В. Виртуальные следы преступлений, совершенных с помощью сети Интернет // Молодой ученый. 2019. № 24 (262). С. 235.

− компьютеры − посредники при передаче данных;

− пакеты данных (шлюзы), через которые передается электронно-цифровая информация.

В программных средствах компьютера преступника сохраняются данные о подключении к провайдеру, времени и продолжительности подключения, истории посещений, кэш-программах просмотра Интернет-ресурсов, специальном программном обеспечении, журналируемых файлах операционной системы и других программ, проведенных операциях. Кроме того, остаются данные в кэш-памяти аппаратных средств[1].

Провайдер, который предоставил преступнику выход в интернет, хранит информацию о сетевых подключениях в виде логов, в том числе совершенных с компьютера, использовавшегося в преступных целях[2].

Электронно-цифровые следы неправомерного доступа воспроизводятся в файлах журналируемой информации (log-файлах). Сервер фиксирует каждое обращение к сайту (о каждом обращении остается запись в лог-файле)[3].

В log-файлы записывается информация:

− о пользователе, обратившемся к ресурсам сервера;

− об IP-адресе компьютера пользователя;

− о MAC-адресе сетевой карты пользователя;

− с какого ресурса совершен вход, и по каким ключевым запросам;

− о посещенных пользователем страницах сервера;

− о продолжительности просмотра страниц;

− о файлах, скачанных с сервера или закачанных на него[4].

Представляет интерес рассмотрение следов с учетом отдельных видов и способов сокрытия неправомерного доступа к компьютерной информации, поскольку каждый способ сокрытия предполагает наличие определенных, типичных для него следов:

1) так, при использовании чужих регистрационных адресов в локальной сети, имеющей выход в сеть Интернет, могут быть обнаружены такие электронно-цифровые следы, как логический адрес сетевого уровня (IP-адрес) и физический адрес сетевой карты;

2) в случае применения беспроводного Wi-Fi соединения на сервере провайдера сохраняются, в частности, учетные данные преступника, настройки, которыми он пользовался;

---

[1] Колычева А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. М., 2018. С. 47.

[2] Дёмин К. Е. Об методических основах получения криминалистически значимой информации, содержащейся в электронных носителях данных // Вестник Московского университета МВД России. 2018. № 4. С. 45.

[3] Анализ и интерпретация лог-файлов. URL: https://www.web-patrol.net/ webanalytics-logfile.html (дата обращения: 10.05.2023).

[4] Доказательная сила логов. URL: https://www.securitylab.ru/contest/285274.php (дата обращения: 12.05.2023).

3) при осуществлении доступа к сети Интернет с чужого телефонного номера, следы обычно могут быть обнаружены на сервере провайдера;

4) при использовании для сокрытия преступления программ-анонимайзеров реальный IP-адрес пользователя останется на анонимном сервере, где также содержится информация о посещенных злоумышленником сайтах в сети Интернет[1].

Программное обеспечение для установки анонимных сетевых соединений через компьютерную сеть (Tor) также не гарантирует отсутствия следов преступления. Поскольку анонимность в этой сети формируется за счет луковой маршрутизации, то большинство действий, направленных на деанонимизацию пользователей сети Tor, основаны именно на её уязвимостях.

[1] Васильева Н. А. Способы сокрытия цифровых следов преступления // Наука. 2021. № 2 (17). С. 75.

2. Понятие сетевых атак, их сущность и виды

В отличие от ситуации с уязвимостями и угрозами ИБ[1], сетевым атакам не посвящен ни один нормативный или правовой акт как российский, так и зарубежный. Единственным источником информации подобного уровня может служить серия стандартов по безопасности сетей ISO/IEC 27033[2], в которой перечислены, например, возможные реализации следующих угроз ИБ:

1. Вирусные атаки и внедрение вредоносных программ, которые могут привести к потере или повреждению информации, потере контроля над инфраструктурой ИТ.
2. Загрузка пользователем файлов или программ, которые обходят защиту сети, используя такие методы, как быстрота прохождения порта и шифрование.
3. Утечка информации с использованием скрытых каналов для сетевых агентов-роботов.
4. Установка «троянских программ» (программ, приводящим к неожиданным и обычно нежелательным результатам), которые могут разрешать несанкционированный внешний доступ, приводящий к нарушению конфиденциальности.
5. Несанкционированное воздействие на меры обеспечения ИБ инфраструктуры, систем и приложений, что может привести к мошенничеству, отказу в обслуживании, а также злоупотреблению возможностями.
6. Атака с целью снижения доступности сети связи, в том числе чрезмерное использование услуг, связанных с пропускной способностью, например, потоковые мультимедийные средства или одноранговое совместное использование файлов может привести к перегрузке сети.
7. DoS- и DDoS-атаки на порталы или расширенные сети услуг «бизнес-бизнес».
8. Инсайдерские атаки с помощью авторизованных партнеров по бизнесу.
9. Фальсификация информационного наполнения транзакции (сообщения не передаются получателю или данные изменяются в процессе передачи) и ряд других.

---

[1] Здесь и далее: ИБ – информационная безопасность; ИТ – информационные технологии; ЖРС – журнал регистрации событий; АО – аппаратное обеспечение; САВЗ – средства антивирусной защиты; ЦИУСБ – центр интеллектуального управления сетевой безопасностью; ИТКС – информационно-телекоммуникационной сеть.

[2] См.: ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введ. 2012-01-01. М., Стандартинформ, 2012. 73 с.; ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. Введ. 2015-11-01. М. : Стандартинформ, 2015. 40 с.

Описанию различных видов атак и их сценариям развития посвящено множество публикаций[1]. Первый типовой сценарий сетевой атаки, состоящий из пяти этапов, часть из которых можно повторять многократно, представил в 2000 г. Р. Грэхэм (R. Graham)[2] :

1. Внешняя разведка (англ. *outside reconnaissance),* в ходе которой злоумышленник пытается выяснить как можно больше о «жертве», не представив себя, находя общедоступную информацию или появляясь в системах как обычный пользователь. На этом этапе он не может быть обнаружен, поскольку просто выполняет в интернете запросы о состоянии сети, узнает, как, где и кем зарегистрировано доменное имя, просматривает структуры для поиска имен компьютеров в домене, изучает другую открытую информацию о веб-сайте компании, анонимных FTP-серверах и т. д.

2. Внутренняя разведка (англ. *inside reconnaissance),* когда злоумышленник использует более «контактные» методы поиска информации, но все же не делает ничего плохого, например, переходит по веб-страницам, ищет уязвимые CC/-скрипты (англ. *Common Gateway Interface)* и работающие в настоящий момент компьютеры, сканирует *UDP/TCP-порты* на выбранных компьютерах для поиска доступных сервисов и т. п.

3. Применение эксплойтов (англ. *exploits)* – программ, использующих (эксплуатирующих) известные уязвимости на выбранных компьютерах. Злоумышленник начинает проверять учетные записи с легко угадываемыми или пустыми паролями, пытается скомпрометировать CGi-скрипт, отправляя команды оболочки в поле ввода, использует хорошо известные проблемы кода, приводящие к переполнению буфера, посылая большие объемы данных, и т. д.

4. Закрепление / удержание в системе (англ. *foot hold),* направленное на сокрытие следов атаки (например, за счет изменения ЖРС) и удостоверение в том, что он может вернуться в систему снова, установив средства для последующего доступа. Например, заменить существующие сервисы троянскими программами, содержащими программные закладки, или лазейки, или «люки» (англ. *backdoor/trapdoors)* (например, точки входа в программу, открывающие доступ к некоторым системным функциям, или намеренно измененный фрагмент ПО), создав новые учетные записи пользователей и т. д. Затем злоумышленник использует взломанную систему для доступа к смежным системам, поскольку большинство сетей хуже защищены от внутренних атак.

---

[1] Miloslavskaya N. Remote Attacks Taxonomy and their Key Verbal Indicators // Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA 2017) (Moscow (Russia), 1-6 August 2017) // Procedia Computer Science, 2018. Vol. 123. P. 278-284. DOI: 10.1016/j.procs.2018.01.043.

[2] Graham R. FAQ: Network Intrusion Detection Systems. 2000. [Электронный ресурс]: Веб-сайт / LINUXSECURITY / R.Graham. URL: http://www.linuxsecurity.com/ resource_files (дата обращения 16.03.2023).

5. Реализация конечных целей атаки и получение желаемой прибыли (англ. *profit),* когда злоумышленник использует свой статус нахождения в системе/сети для кражи конфиденциальных данных, злоупотребления системными ресурсами и т. д.

Самым серьезным источником информации о тактиках, методах и знаниях современных атакующих является модель ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) компании MITRE[1], в основном ориентированная на сети, использующие ОС Microsoft Windows. Каждая категория тактики из модели ATT&CK содержит список приемов, способов и порядков действий, которые может использовать злоумышленник.

Приведем несколько примеров из матрицы MITRE ATT&CK, обеспечивающей глубокий уровень детализации в описании этапов модели Lockheed-Martin в части того, что может произойти во время атаки после того, как противник получил доступ:

1) Первоначальный доступ (англ. initial access): эксплуатация открытых приложений, добавление оборудования, репликация через съемные носители, вложение/ссылка для фишинга; фишинг через услугу, компрометация цепочки поставок, использование доверительных отношений и т. д.

2) Выполнение (англ. execution): использование интерфейса командной строки, элементов панели управления или динамического обмена данными, через загрузку API/GUIIPowerShell/module, скомпилированный HTML-файл, запланированная задача, сценарии, использование сервисов, использование пространства после имени файла, удаленное управление и т. д.

3) Присутствие (англ. persistence): манипуляция учетной записью, наложение приложений, расширения к браузеру, изменение ассоциации файлов по умолчанию, внешние удаленные сервисы, скрытые файлы и каталоги, подключение, инъекция параметров выполнения файла, запуск агента/демона, элемент входа, выход из системы, новый сервис, запуск приложения, перехват пути, использование локального монитора портов, злоупотребление избыточным доступом, запланированная задача, модификация ярлыков, установка внешних удаленных сервисов и т. д.

4) Эскалация привилегий (англ. privilege escalation): манипуляция токеном доступа, наложение приложений, обход пользовательского управления приложениями, DLL-инъекция, эксплуатация для эскалации привилегий, инъекция в процесс, работа от имени суперпользователя (sudo), перехват маршрута, веб-оболочка и т. д.

[1] ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) [Электронный ресурс]: Веб-сайт / MITRE. URL: https://attack.mitre.org/ (дата обращения 16.03.2023).

5) Обход защиты (англ. defense evasion): очистка истории команд, подписывание кода, расшифровка файлов/информации, отключение СЗИ, отключение индикатора блокировки / удаления, удаление файлов, изменение разрешений для файла, логическое смещение в файловой системе, скрытые файлы/окна/пользователи, выполнение команд в фоновом режиме, установка корневого сертификата, маскарад, изменение реестра, удаление процесса, измененное время, обход управления учетными записями пользователей, удаление процесса и т. д.

6) Доступ к учетным данным (англ. credential access): сброс учетных данных, захват ввода, прослушивание сети, перехват двухфакторной аутентификации и т. д.; исследование (англ. discovery) системных сервисов/информации, приложений, реестра запросов, конфигурации сети, удаленных систем, владельца/пользователей системы, сетевых сервисов/соединений, процессов, ПО СЗИ, групп разрешений, файлов/каталогов, учетных записей, периферийных устройств, системного времени и т. д.

7) Движение «вбок», или ответвление (англ. lateral movement): использование стороннего ПО / ПО для развертывания приложений / удаленных сервисов, удаленное управление Windows/Admin shares, сценарии входа в систему, использование эксплойтов, использование протокола удаленного рабочего стола, репликация через съемный носитель, восстановление удаленной копии файла и т. д.

8) Сбор (англ. collection) данных от локальной системы/съемных носителей/сетевых устройств, захват входного сигнала/аудио/видео/экрана, пришедших данных, сбор сообщений электронной почты, автоматизированный сбор, сбор данных из буфера обмена и т. д.

9) Команды и контроль (англ. command and control): запутывание данных/кодирование, использование резервных каналов, пользовательского криптографического/командного и управляющего протоколов, многополосной связи, обычно/необычно используемый порт, стандартный протокол уровня приложения, многослойное шифрование, соединения через прокси-сервер, связь через съемные носители и т. д.

10) Эксфильтрация (англ. exfiltration): доставка информации, интересующей злоумышленника, в его зону доступа, или, когда он заставляет пользователя что-то сделать на свою пользу, эксфильтрация через другой сетевой носитель/командный и управляющий канал/альтернативный протокол/физический носитель, автоматизированная эксфильтрация, запланированная передача, сжатие/шифрование данных, ограничение размера передачи данных и т. д.

11) Воздействие (англ. impact): удаление учетной записи, разрушение данных, подмена стартовой веб-страницы, стирание данных на диске, отказ в обслуживании, перехват ресурсов, перезагрузка системы и т. д.

На основе известной информации о развитии сетевой атаки могут быть сформулированы индикаторы (IoC) – артефакты, как описанные специалистами признаки, отражающие наблюдаемые события, действия, объекты и т. п. в сети, ОС, СУБД, приложении, на рабочей станции, сервере и т. п., которые с высокой степенью вероятности указывают на предпринимаемую или уже состоявшуюся атаку. Они используются для описания того, что атака, возможно, уже произошла или может произойти прямо сейчас или в будущем, то есть для обнаружения попыток проникновения в компьютерные системы на ранних стадиях и первичной оценки возможного ущерба. Примеры IoC – это адреса командных серверов ботнетов (англ. botnet, от robot network), электронные адреса рассыльщиков фишинговых писем и спама, сигнатуры вирусов, хэш-суммы вредоносных файлов.

Данные, характеризующие стадии атаки и её типичные последствия, можно собрать из различных источников в атакованной сети, а далее извлечь и нормализовать (привести к сопоставимому виду/формату) для последующей корреляции (выявления событий ИБ, имеющих логическую связь и потенциально значимых для выявления возможных нарушений ИБ).

Некоторыми авторами были предложены вербальные описания основной части ключевых типовых признаков, характеризующих типичные действия злоумышленника и свидетельствующих об удаленных сетевых атаках, которые полностью применимы к ИТКС.

Приведем ряд примеров таких признаков (индикаторов компрометации):

– несанкционированный пользователь в сети;

– активность пользователя в нерабочее время (ночью или в выходной);

– совместно используемые учетные данные;

– доступ к учетной записи сервиса в интернете или несанкционированному устройству;

– несколько входов с одинаковым идентификатором из разных мест за короткое время;

– одна учетная запись хоста/пользователя пытается войти на несколько хостов в сети через несколько минут из/в разные регионы;

– многочисленные изменения за короткое временя от административных учетных записей;

– неавторизованное/не соответствующее политике, установке обновлений т. п. устройство в сети;

– появление нового неавторизованного хоста или сетевого сервиса во внутреннем сегменте и интранета;

– неавторизованное подключение внутреннего хоста (клиента, сервера) к интернету;

– взаимодействие внутренних узлов либо с известными ненадежными адресатами, либо с хостами, расположенными в другой стране, где нет деловых партнеров организации, или внешними хостами с использованием нестандартных портов или несоответствия протокола и порта;

– хосты, которые публично доступны или расположены в ДМЗ сети организации, обмениваются данными с некоторыми внутренними узлами, что указывает на проход извне внутрь и обратно, фильтрацию данных и удаленный доступ к сетевым ресурсам;

– многочисленные предупреждения об опасности от одного хоста или повтор событий на нескольких компьютерах в одной подсети в течение 24 часов (например, повторные попытки аутентификации);

– обнаружение связей известного вредоносного ПО, например, доступ с одного или нескольких внутренних узлов на внешний вредоносный веб-сайт (из известных «черных» списков);

– повторное заражение системы вредоносным ПО в течение короткого времени после очистки (сигнал о наличии руткита (англ. rootkit/toolkit) – набора программных средств для маскировки действий злоумышленника или APT-атаки);

– обнаружение нескольких зараженных хостов или типичных широко известных эксплойтов;

– необычные маршруты доступа (например, некоторые БД обычно доступны только определенным приложениям, а не непосредственно пользователями);

– чрезмерный исходящий (например, веб-, электронная почта) или входящий (например, потоковая передача, веб-) трафик из одного источника или в один адрес назначения. Например, необычный трафик между серверами может быть характерной чертой для необнаруженных вредоносных программ, ищущих хранилища данных;

– сканирование/зондирование сети/уязвимостей внутренними узлами, общающимися с несколькими хостами за короткое время или во время неразрешенного периода времени;

– несанкционированная загрузка драйверов;

– неожиданное завершение/создание/сетевая активность процесса;

– создание процессом именованного канала или подключение процесса к именованному каналу;

– несанкционированная модификация таблицы импорта запущенного процесса;

– прописывание исполняемого файла/команды в автозагрузку: изменение специфичных ключей реестра, создание/изменение файлов в специфичных каталогах, создание/изменение сервисов, задач планировщика и т. п.;

– обнаружение скрытого процесса или модуля;

– доступ процесса к памяти другого процесса для чтения / записи;

– неожиданная загрузка процессом DLL-библиотеки;

– неожиданное создание/изменение/переименование/удаление процессом файла, например, отсутствие или повреждение файлов, или появление новых файлов, которые не были созданы внутренними пользователями;

– имя файла с необычными символами;

– модификация атрибутов безопасности файла (скрытый, системный и т. д.) или файловой системы;

– несанкционированное создание общих сетевых каталогов, доступ к ним;

– манипуляция с объектами каталога Active Directory;

– изменения политики безопасности/аудита событий;

– исправленные или удаленные на источнике данных о событиях ЖРС или источник данных о событиях, остановивший запись;

– неавторизованное изменение конфигурации устройства (включая СЗИ);

– чрезмерный перерыв между сканированиями средствами антивирусной защиты (САВЗ);

– чрезмерные попытки блокировки портов от систем мониторинга, таких как САВЗ;

– обращения по протоколу HTTPS к фишинговым доменам, похожим на домены компании;

– повторная атака из одного источника или одного хоста;

– НСД к конфиденциальным, персональным или финансовым данным;

– скрытые каналы передачи данных (например, с использованием туннелирования);

– большое количество отклоненных писем с подозрительным контентом;

– аномалии в основных настройках доступа и аутентификации пользователей, сети, приложений, подозрительная деятельность;

– DoS, DDoS-атака и т. д.;

– другие признаки, такие как отказы/сбой ПО, повторение некоторых конкретных событий, неправильные команды, случайные атрибуты, не соответствующие параметры сетевого трафика, попытки передачи больших объемов данных;

– подозрительные события и процессы, трафик на известный уязвимый хост и т. д.;

Приведенный список не ранжирован по частоте встречаемости подобных атак, по тяжести последствий и т. п., поскольку приоритеты защиты от компьютерных атак должны расставляться в зависимости от специфики работы защищаемого объекта. Например, для многих организаций доставка вредоносного почтового сообщения менее важна, чем активное управление и контроль злоумышленником зараженной рабочей станцией.

3. Использование средств и способов обнаружения, фиксации и исследования следов неправомерного доступа к компьютерной информации

С точки зрения уголовно-процессуального законодательства, поиск, фиксация и изъятие материальных следов совершения преступления осуществляется в рамках трех основных следственных действий – **следственного осмотра, обыска и выемки**. При этом следует понимать, что компьютерную информацию нельзя изъять, её можно только скопировать, изменить или уничтожить.

Общая тактика следственного осмотра, обыска и выемки при расследовании неправомерного доступа к компьютерной информации мало чем отличается от традиционного порядка производства указанных следственных действий. Однако следует выполнять требования ст. 164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий». Электронные носители информации изымаются в ходе производства следственных действий с обязательным участием специалиста.

Выемка производится при необходимости изъятия определенных предметов и документов, имеющих значение для уголовного дела, и, если точно известно, где и у кого они находятся (ст. 183 УПК РФ). Таким образом, принудительная выемка представляет собой не что иное, как одну из разновидностей обыска, при её производстве используются те же тактические приемы обыска.

В соответствии со ст. 176 УПК РФ осмотр места происшествия, местности, жилища, иного помещения, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела.

Следственный осмотр

Задачами следственного осмотра при расследовании данных преступлений являются:

– выяснение сущности и обстоятельств деяния, свидетельствующих о нем как о преступлении;

– определение объекта и предмета преступного посягательства;

– выяснение способа совершения преступления;

– выяснение места, времени и обстоятельств совершения преступления;

– выявление размера и вида ущерба, причиненного потерпевшему;

– принятие мер к установлению лица, совершившего преступление, а также состава и роли каждого участника, в случае совершения преступления группой лиц;

– выяснение обстоятельств, способствовавших и (или) сопутствующих совершению преступления.

В ситуации осмотра вычислительных систем и электронных носителей, в качестве специалиста можно привлечь работника, непосредственно занимающегося обслуживанием и эксплуатацией средств вычислительной техники в той организации, где проводится следственное действие. В таком случае следователь должен быть уверен в том, что указанное лицо не заинтересовано в результатах расследования дела. Кроме того, следователь должен по возможности убедиться в наличии у него достаточной компетентности для решения предстоящих задач.

В беседе с таким лицом необходимо выяснить, обладает ли он знаниями и имеет ли опыт в решении следующих типичных задач:

– обнаружение средств экстренного уничтожения информации;

– определение способов нейтрализации средств экстренного уничтожения информации;

– выявление признаков, указывающих на применение «облачных» технологий хранения данных;

– обнаружение средств шифрования данных и криптографических контейнеров, фиксации их содержания;

– обнаружение систем дублирования и резервного хранения информации;

– оказание помощи следователю при составлении протокола следственного действия в описании средств вычислительной техники, их систем, носителей информации и действий, связанных с просмотром содержимого файлов, запущенных программ и страниц интернет-сайтов;

– осуществление действий по копированию данных, применяя методы создания посекторной копии, образа копируемого сектора электронного носителя, получения дампа оперативной памяти, определения хеш-суммы копированных данных;

– фиксация, с использованием технических и программных средств, информации с удалённых сетевых ресурсов, с установлением идентификационных данных (адресов) сетевых ресурсов, на конкретный момент времени;

– определение криминалистически значимых сведений об операционной системе, обстоятельствах её использования и аналогичных сведений относительно распространённых программных продуктов;

– обнаружение сведений о подключенных ранее к компьютеру внешних носителей информации (USB-накопители, мобильные телефоны, цифровые фотоаппараты и т. д.);

– поиск и извлечение конкретной значимой информации с серверов хранения и обработки данных;

– извлечение данных, обрабатываемых с применением виртуальных

машин, создаваемых пользователями на своем компьютере и функционирующих в «облаке» и др.

При осмотре компьютерной техники на месте обнаружения в протоколе следственного осмотра необходимо отразить:

– расположение отдельных экземпляров (частей, узлов) компьютерной техники относительно друг друга, вида их соединения между собой и с другим оборудованием;

– наличие и характер систем видеонаблюдения;

– наличие или отсутствие специального программного обеспечения или технических средств, предназначенных для негласного уничтожения или блокирования компьютерной техники (компьютерной информации);

– наличие материальных следов преступления на месте происшествия (дактилоскопических, трасологических, биологических и др.), на компьютерной технике, внешних накопителях и др.;

– тип, вид или назначение осматриваемого экземпляра компьютерной техники, марку (наименования) техники;

– цвет корпуса изделия, маркировочные обозначения, включая персонализированный номер (заводской, инвентарный и т. д.);

– индивидуальные особенности, имеющиеся на осматриваемой технике: повреждения; дефекты, незаводские маркировки, пометки, надписи; особенности соединительных и электропитающих проводов; пломбирующие устройства, загрязнения на корпусе и т. д.

В случае выявления представляющей интерес текстовой или графической информации целесообразно зафиксировать наименования, месторасположение и изображение выявленных файлов. Кроме того, необходимо указать размер, дату и время проводимых операций с данными файлами (создания, последнего изменения, удаления и др.). Важно помнить, что сведения о времени и дате создания файлов фиксируются операционной системой при создании или изменении содержимого файла, чего не происходит при его просмотре, а также эти параметры легко могут изменяться пользователем с помощью распространенных файловых менеджеров или путем изменения системного времени при создании или изменении файла.

Осмотр компьютерных объектов (вычислительной техники), электронных носителей информации включает в себя несколько последовательных этапов (в кабинете следователем):

– осмотр непосредственно устройства, как материального объекта;

– осмотр конфигураций и настройки устройства, установление его индивидуальных особенностей;

– осмотр информации, хранимой на различных электронных носителях, установление формата хранимых данных и их характеристики;

– установление удаленных (стертых) операционной системой, но физически еще не уничтоженных информационных файлов и их характеристик;

– осмотр доступных информационно-вычислительных ресурсов и электронной корреспонденции (в случае подключения осматриваемого устройства к какой-либо информационной сети).

Задачи осмотра:

– сбор «традиционных» следов пользования устройством (отпечатки пальцев, биологический материал, серийные номера комплектующих, характерные повреждения);

– определение комплектности и состава устройства, а также оценка их потенциальных возможностей;

– оценка состояния устройства;

– фиксация наиболее подходящим способом расположения устройства и его взаимосвязей с другими средствами вычислительной техники и материальными объектами;

– оценка потенциальных возможностей использования осматриваемого устройства для работы в информационных сетях и сбор «виртуальных» следов этой деятельности.

Документирование полученной информации осуществляется путем:

– распечатки на бумажном носителе важнейших информационных элементов или небольших файлов;

– создания полной и точной (в том числе побитовой) копии информации с изъятого носителя;

– подробного описания хода осмотра в протоколе следственного действия, с приложением скриншотов, фотоснимков и (или) видеофиксации всего следственного действия.

Обыск

Обыск по своим информационно-познавательным целям весьма близок к следственному осмотру. Основанием производства обыска, в соответствии со ст. 182 УПК РФ, является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела.

Целями (задачами) обыска при расследовании данных преступлений являются обнаружение и изъятие материальных объектов, содержащих информацию, имеющую отношение к расследуемому преступлению. К таким объектам могут быть отнесены:

– вычислительные комплексы и их компоненты (персональные компьютеры, модемы, принтеры и т. п.);

– различного рода носители информации, представленной в виде, пригодном для автоматизированной обработки;

– линии коммуникаций объектов вычислительной техники, понимаемые в широком смысле данного понятия, т. е. как наличие и размещение устройства передачи информации, среды распространения (передачи) и устройства приема информации;

– вспомогательные системы, обеспечивающие нормальное функционирование автоматизированных информационных систем (линии электропитания, заземления и т. п.).

Существенной особенностью обыска при расследовании преступлений в сфере компьютерной информации, в том числе предусмотренных
ст. 272 УК РФ, является то, что следователь, проводящий данное следственное действие, как правило, не может оценить на месте значение обнаруживаемой информации, в связи с чем, наиболее целесообразным является изъятие всех обнаруженных машинных носителей информации.

Готовясь к проведению обыска, следователь должен тщательно изучить обстоятельства дела и собрать ориентирующую информацию о предмете поиска, месте проведения следственного действия, личностных и профессиональных характеристиках лиц, в отношении которых будет проводиться следственное действие. Кроме того, следует обязательно выяснить: количество компьютерной техники, её тип и расположение; наличие автономных источников питания; используемые электронные носители информации; наличие систем экстренного уничтожения данных; используемое программное обеспечение; количество компьютеров и их точное местоположение; наличие локальной компьютерной сети.

Если на объекте эксплуатируется компьютерная сеть, необходимо установить её администраторов; количество и типы эксплуатируемых серверов и рабочих мест; типы применяемых операционных сетевых систем; специфическое прикладное программное обеспечение, используемое в сети (базы данных, система документооборота и пр.); наличие резервных копий серверных дисков, баз данных и место их хранения; подключение к другим сетям, эксплуатация распределенных сетей или почтовых программ для связи с удаленными подразделениями организации или с другими предприятиями; использование систем шифрования и защиты информации (если да,то каких); данные провайдера, предоставляющего услуги выхода в сеть Интернет; расположение систем вентиляции и кондиционирования (актуально для серверных помещении); план-схему помещений.

Получить ответы на все перечисленные вопросы не всегда представляется возможным, но выяснить расположение компьютеров, серверов и типов используемого программного обеспечения необходимо. От этого, в частности, зависит набор программных и программно-

аппаратных средств, которые понадобятся при проведении следственного действия.

Следователь должен учитывать особенности маскировки объектов поиска. Предполагая возможность изобличения, преступник может принимать меры к сокрытию мест хранения информации, содержащей следы его преступной деятельности. Маскировка может осуществляться путем изменения местоположения электронного носителя внутри системного блока или помещения носителя за пределы системного блока. Внешне электронный носитель может выглядеть как предмет, не имеющий отношения к компьютерной технике (брелок, сувенир, игрушка и т. п.).

При производстве обысков у подозреваемых следует искать тайники, где могут храниться сменные компьютерные носители информации. Необходимо вскрывать корпуса аппаратных средств компьютерной техники, чтобы обнаружить специально отключенные внутренние носители информации (например, дополнительный жесткий диск).

Нередко для хранения информации используются носители, принадлежащие другим пользователям, доступ к которым обеспечивается за счет использования сетевых возможностей. В последнее время все большее распространение получает хранение больших объемов компьютерных данных в так называемых облачных хранилищах, расположенных на удаленных сетевых серверах. Это обстоятельство должно обязательно учитываться при поиске криминалистически значимой информации. Признаки дистанционного использования носителей информации могут быть выявлены при обращении к журналам событий, формируемым операционной системой. Возможно, потребуется выполнение некоторых нехарактерных для обычного обыска и выемки мероприятий, таких как определение конфигурации вычислительной системы, топологии внутренних компьютерных сетей, используемой схемы подключения к глобальным сетям и др.

Выемка

Еще на этапе подготовки в обязательном порядке с участием специалистов необходимо проанализировать информацию о технологических особенностях функционирования компьютерных сетей, используемых средствах связи и телекоммуникации, во избежание их разрушения, нарушения технологического режима их нормального функционирования, причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств. В большинстве случаев нецелесообразно производить изъятие серверов, системных блоков, ноутбуков и иных электронных цифровых устройств целиком при имеющейся заводской возможности изъятия носителя информации. Следователь должен учитывать, что для коммерческих компаний, работающих в сфере компьютерных и информационных технологий, изъятие

сервера практически означает утрату бизнеса и рассогласование бизнес-процессов, то есть необратимые последствия для деятельности компании[1].

При изъятии работающей на момент обнаружения компьютерной техники, важно осуществить и отразить в протоколе следующие действия:

– зафиксировать и остановить выполнение программ;

– посредством гибернации или используя специальные программы, сохранить информацию, находящуюся в оперативной памяти компьютера, на специально подготовленный внешний носитель информации;

– выключить устройство;

– отключить все периферийное оборудование, соединительные провода и кабели питания[2].

Современные технологии, применяющиеся для хранения и обработки больших массивов данных, подразумевают такую архитектуру совокупности серверов, как отдельных средств компьютерной техники, в том числе находящихся на большом расстоянии друг от друга, при которой они работают как единое хранилище информации. Физическое изъятие отдельных устройств или какой-то их совокупности может фактически исключить возможность восстановления интересующих следствие данных.

Кроме того, необходимо помнить, что не всегда представляется уместным изъятие персональных компьютеров, их винчестеров, ноутбуков, планшетов, смартфонов и других «мобильных» средств компьютерной техники. Такие устройства достаточно часто изымаются с целью их исследования для обнаружения информации, имеющей значение для расследования преступления. Однако в рамках судебной компьютерной экспертизы объектом применения методов поиска информации будет выступать не представленный на исследование электронный носитель информации, а иной носитель, на который эксперт предварительно записывает информацию путем посекторного копирования данных представленного на исследование объекта[3].

Таким образом, во многих ситуациях производства следственных действий копирование информации в электронном виде, имеющей значение для расследования, является приемлемой альтернативой изъятию электронных носителей этой информации, а в ряде случаев, единственно возможной формой фиксации.

Существующие программные средства и оборудование, позволяющие при производстве следственного действия осуществлять посекторное

---

[1] См.: Гаврилов М. В., Иванов А. Н. Осмотр при расследовании преступлений в сфере компьютерной информации. М., 2007. С. 45.

[2] См.: Саенко Г. В., Тушканова О. В. Компьютерная экспертиза. Исследование компьютерной информации // Практическое руководство по производству судебных экспертиз для экспертов и специалистов: науч.-практич. пособие / под ред. Т. В. Аверьяновой, В. Ф. Статкуса. М.: Юрайт, 2011. С. 189–190.

[3] См.: Саенко Г. В., Тушканова О. В. Указ. соч. С. 189–190.

копирование, копирование с созданием образа файлов, каталогов, разделов, диапазона секторов и вычисления их хеш-функции, обеспечивают достоверность получаемых данных и возможность проверки их подлинности на всех этапах уголовного судопроизводства.

Закон определяет, что копирование информации не допускается, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Однако четкие критерии, подтверждающие возможность наступления при копировании указанных последствий, отсутствуют.

Во многих следственных ситуациях от специалиста требуется наличие глубоких знаний в сфере функционирования программного и аппаратного обеспечения обследуемых электронных устройств, а в отдельных случаях он должен разбираться в более сложных специфических вопросах (особенностях эксплуатации сетевого оборудования, процедурах шифрования информации и т. п.), иметь достаточные навыки их практического решения (например, владеть методикой применения криминалистических средст ввыявления и фиксации доказательств).

Упаковка изымаемых объектов должна исключать возможность непроцессуальной работы с ними, разукомплектовки и физического повреждения. Важно правильно опечатывать упаковку с изымаемыми объектами так, чтобы из неё было невозможно извлечь объект без повреждения опечатывающих наклеек.

Все обнаруженные в ходе обыска, выемки или осмотра предметы и документы, которые могут иметь значение для следствия, должны быть изъяты в строгом соответствии с требованиями закона, чтобы впоследствии они могли иметь доказательственное значение. В связи с этим в протоколе обязательно должны быть точно отражены место, время производства следственного действия и внешний вид изымаемых предметов и документов.

Основные возможности судебных компьютерно-технических экспертиз и тактические рекомендации по их назначению

Общей рекомендацией при назначении судебных компьютерно-технических экспертиз является обязательное предварительное согласование всех выносимых следователем на экспертизу вопросов (редакция вопросов, перечень необходимых для исследования объектов и материалов, сроки производства исследований) с экспертом. Следователь должен четко представлять возможность и ограничения судебной компьютерно-технической экспертизы и не ставить перед экспертами задач и вопросов, выходящих за рамки их компетенции.

При этом можно выделить следующие разновидности объектов судебной компьютерно-технической экспертизы:

– текстовые и графические документы (традиционные и электронные), изготовленные с использованием средств автоматизации (вычислительных систем, передачи данных и копирования информации);

– компьютерные программы и вспомогательная компьютерная информация, необходимая для их функционирования;

– видео- и звукозаписи, визуальная и аудиальная информация, представленная в формате мультимедиа;

– компьютерные данные и сведения, представленные в форматах, обеспечивающих их автоматизированное хранение, поиск, обработку и передачу (базы данных);

– вычислительные системы и сети, множительная техника, средства связи и другие технические средства;

– физические носители информации различной природы.

При раскрытии и расследовании преступлений, в сфере высоких технологий наиболее востребовано исследование компьютерной информации, содержащейся в современных высокотехнологичных устройствах. Данный факт обусловлен необходимостью, как на стадии возбуждения уголовного дела, так и в ходе предварительного следствия устанавливать наличие в деянии юридически значимых технических и программных процессов, предусмотренных уголовной нормой, таких как «уничтожение, блокирование, модификация либо копирование компьютерной информации»[1].

Однако также важно понимать, что юридически значимый факт, например, «уничтожения» или «модификации» устанавливает не эксперт или специалист при проведении исследования, а именно субъект, проводящий расследование, путем обнаружения и закрепления совокупности доказательств интересующего события. Одним из таких доказательств является заключение судебной компьютерно-технической экспертизы[2].

Основная цель СКТЭ состоит в изучении закономерностей функционирования информации в средствах вычислительной техники[3]. Задачи СКТЭ:

– установление фактических обстоятельств на основе изучения закономерностей функционирования информации в СВТ;

– поиск на машинном носителе (в СВТ) информации, созданной с помощью прикладных программ, информации о действиях пользователя

[1] Ст. 272 УК РФ.
[2] Далее СКТЭ.
[3] Далее СВТ.

(процессах обработки файлов, ведении баз данных, работе в сетях передачи данных и др.);

– определение свойств программ и программных продуктов, принадлежности программ и данных к конкретным классам;

– установление материальных объектов по имеющейся компьютерной информации (проводится в комплексе с другими видами экспертиз);

– определение возможности совершения каких-либо действий с помощью СВТ;

– установление фактических обстоятельств совершения преступления (проводится при наличии информации об интересующем событии, полученной из различных источников).

Объект СКТЭ – компьютерная информация, имеющаяся:

– на машинных носителях;

– отдельных технических средствах и функциональных устройствах систем обработки информации и в системах обработки информации в целом.

После доэкспертной оценки рекомендуется провести рабочую встречу с экспертами в целях согласования текста постановления о назначении судебной экспертизы, формулировок вопросов, достаточности представляемых материалов. Консультативное взаимодействие с экспертами на стадии назначения экспертиз, формулирования экспертного задания (вопросов) в большинстве случаев определяет оперативность, качество и результативность применения специальных знаний при расследовании и раскрытии преступлений.

Важно отметить, что оговоренная рабочая встреча может быть эффективна только в случае, если следователь владеет информацией по расследуемому делу, разобрался в особенностях квалификации исследуемого события.

Рекомендации по отбору объектов исследования СКТЭ и порядок их предоставления

Объекты исследования должны быть представлены в работоспособном состоянии, позволяющем производить поиск и считывание хранящейся на них информации. Предоставление заведомо неисправных устройств допускается при обязательной предварительной консультации с экспертом и в рамках назначения комплексной компьютерно-радиотехнической экспертизы.

Объекты исследования, содержащие зашифрованную информацию или заблокированные какой-либо пользовательской защитой, представляются с ключом разблокировки (паролем, пин-кодом, графическим рисунком). Представление их без ключа разблокировки

допускается после обязательного предварительного согласования с экспертом.

Объекты исследования должны соответствовать фабуле преступления.

Рекомендуемое количество объектов, представляемых на исследование в рамках одной экспертизы, – не более пяти. Они должны иметь непосредственное отношение к одному и тому же фигуранту дела и/или к одному объекту информатизации. Увеличение количества представляемых объектов возможно, если они содержат связанную, взаимозависимую информацию и допускается после обязательной предварительной консультации с экспертом.

Не должны представлять на СКТЭ объекты, внешне схожие с носителями информации, средствами вычислительной техники, такие как переходники, разветвители, кабели, зарядные устройства (отдельно), аппаратные ключи защиты[1].

Количество ключевых фраз для осуществления поисковых запросов должно быть оптимизировано с учетом полиморфизма и не должно превышать 100 на одну экспертизу.

Сетевое оборудование (маршрутизаторы, модемы, сетевые карты) может предоставляться только для ответов на вопросы в области информационно-телекоммуникационных технологий после обязательной предварительной консультации с экспертом.

Объекты исследования для СКТЭ в области анализа программного обеспечения представляются после обязательного предварительного ознакомления эксперта с информацией о преступлении (инциденте) и консультации с ним.

Информация должна быть представлена на подлинных носителях либо в виде посекторных копий. Информация из серверного оборудования должна быть предварительно скопирована на логическом уровне и представлена в виде копии. Программные продукты и базы данных, представляемые для сравнительного исследования, должны иметь те же наименования и версии, что и программные продукты, а также базы данных, представленные на исследование. Желательно представлять сведения о технических средствах защиты информации (от разработчика / правообладателя).

Упаковка объектов исследования должна исключать возможность физического доступа к ним. Целесообразно использовать картонные коробки, полиэтиленовые и бумажные пакеты, которые заклеиваются (завязываются), опечатываются и снабжаются пояснительными надписями. Все порты и разъемы персональных компьютеров и серверного оборудования оклеиваются и опечатываются. Мобильные телефоны

[1] Кроме СКТЭ в области анализа программного обеспечения.

упаковывают в непрозрачный материал в целях предотвращения доступа к его дисплею.

Объекты необходимо хранить в сухом помещении при комнатной температуре, исключив влияние на них электромагнитных полей.

Исследование некоторых видов объектов (мобильные телефоны, планшетные компьютеры и т. п.), поступающих с постановлениями о назначении компьютерных экспертиз, требует их включения. При проведении исследования мобильных устройств путем их включения возможно внесение изменений в содержимое их памяти по причинам, не зависящим от эксперта. Вместе с тем, в соответствии с п. 4 ст. 57 УПК РФ «Эксперт не вправе: проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств». Кроме того, для исследования некоторых типов мобильных устройств требуется их частичная разборка.

Таким образом, если следователь согласен с внесением изменений в содержимое памяти исследуемых объектов, а также применением при проведении экспертизы разрушающих методов исследования (при наличии такой необходимости), следует дать на это письменное согласие, о чем сообщить в постановлении.

Типовые вопросы, решаемые в рамках КСЭ

Компьютерная информация, представленная в виде файловых систем:

1. Имеются ли в памяти представленных на исследование электронных носителей информации … (перечислить) сведения об учетных записях пользователя (аккаунтах)?
2. Имеются ли в памяти представленных на исследование электронных носителей информации … (перечислить) файлы, содержащие электронную переписку посредством электронной почты, сервисов мгновенных сообщений (мессенджеров) и социальных сетей?
3. Имеются ли в памяти представленных на исследование электронных носителей информации …(перечислить) файлы, содержащие историю посещения интернет-ресурсов?
4. Имеются ли в памяти представленных на исследование электронных носителей информации … (перечислить) файлы, содержащие следующие ключевые слова (и выражения): «…», «…» и «…» (перечислить)?
5. Имеются ли в памяти представленных на исследование электронных носителей информации … (перечислить) созданные или полученные пользователем графические / текстовые / аудио- / видеофайлы?

6. Имеются ли в памяти представленных на исследование электронных носителей информации … (перечислить) сведения об установленном программном обеспечении (для чего / атрибутирующем себя как)?

Компьютерная информация, рассматриваемая в качестве объекта интеллектуальной собственности (программы для ЭВМ и базы данных):

1. Имеется ли на ... (перечислить объекты) ПО, (перечислить) (при наличии образцов для сравнительного исследования)?

2. Имеются ли на ... (перечислить объекты) ПО, атрибутирующее (именующее) себя как ... (перечислить наименования) (при отсутствии образцов для сравнительного исследования)?

3. Имеются ли на ... (перечислить объекты) ПО, у которого в качестве правообладателя указаны … (перечислить наименования)?

Если да, то:

– какие сведения о наименовании / правообладателях имеются в данных произведениях?

– какие сведения о дате и времени установки программных продуктов (для установленного программного обеспечения) / создания и последнего сохранения произведений имеются в представленных объектах?

– какие сведения о пользователях программных продуктов (ключах установки и др.) имеются в представленных объектах (для установленного ПО)?

4. Появляются ли при запуске ПО сообщения об ограничении его функциональных возможностей?

5. Имеется ли на ... (перечислить объекты) ПО, с помощью которого можно совершать следующие действия: ... (перечислить)?

В области исследования программного обеспечения:

1. Имеются ли на представленных носителях информации (средствах вычислительной техники) объекты компьютерной информации (программное обеспечение), с помощью которых возможно совершение описанных в постановлении о назначении экспертизы действий?

2. Как атрибутируют себя обнаруженные (представленные) объекты компьютерной информации (программное обеспечение), их основные параметры?

3. Совпадает ли следовая картина, образованная в результате исполнения кода и представленного на исследование программного обеспечения, со следовой картиной конкретного инцидента при условии создания аналогичных условий функционирования и схожего состава входящих информационных потоков?

4. К каким ресурсам глобальных и локальных информационных сетей фиксируются обращения в результате исполнения кода, представленного на исследование программного обеспечения?

5. Какая информация передается, и какая ожидается в результате обращения к ресурсам глобальных и локальных информационных сетей в результате исполнения кода, представленного на исследование программного обеспечения, какие предусмотрены варианты реагирования на полученные команды?

6. Доступ к каким информационным ресурсам заложен в алгоритме кода, представленного на исследование программного обеспечения, какая компьютерная информация и как (копирование, изменение, удаление и пр.) при этом обрабатывается?

Вопросы признания представленного на исследование программного обеспечения «вредоносным» либо определения его как заведомо предназначенного для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации могут быть решены в ходе производства СКТЭ в области исследования программного обеспечения.

Представленный перечень типовых вопросов является рекомендованным, но не исчерпывающим. При постановке вопросов необходимо следовать фабуле уголовного дела и ограничиваться актуальными, решение которых способствует раскрытию преступления.

Формулировки вопросов, отличающиеся от типовых, следует согласовывать с экспертом.

4. Организация и производство первоначальных процессуальных и организационно-тактических действий следователем по уголовным делам о неправомерном доступе к компьютерной информации

Алгоритм производства следователем первоначальных процессуальных и организационно-тактических действий напрямую зависит от родовой и видовой принадлежности совершенного преступления.

Обратим внимание, что весьма актуальной проблемой на современном этапе является неправомерный доступ к аккаунтам социальных сетей «ВКонтакте» и «Одноклассники», мессенджерам WhatsApp и Telegram, порталу «Госуслуги», приложению «Сбербанк Онлайн». Из особенностей «взлома» отметим задействование преступниками механизмов «социальной инженерии», позволяющих обойти защиту в виде двухфакторной аутентификации. На портале «Госуслуги» такой механизм стал обязательным с 28 октября 2023 г.

В подавляющем большинстве случаев заявление о преступлении, связанном с неправомерным доступом к компьютерной информации, поступает от представителя организации, пострадавшей от преступления либо иных заинтересованных физических лиц.

Важной составляющей при решении вопроса о возбуждении уголовного дела и последующем его расследовании являются объяснения (показания) сотрудников пострадавшей организации: администраторов сети; инженеров-программистов, разработавших программное обеспечение и осуществляющих его сопровождение; операторов; специалистов, занимающихся эксплуатацией и ремонтом компьютерной техники; системных программистов; инженеров по средствам связи и телекоммуникационному оборудованию; специалистов, обеспечивающих информационную безопасность; работников службы безопасности и других.

Из данных объяснений (показаний) можно выяснить обстоятельства обнаружения факта преступления (признаков его совершения, способов и средств, наступивших негативных последствий), наличие и функционирование информационной защиты, её недостатки, иные причины и условия, которые могли быть использованы для совершения противоправных действий.

Следователь в ходе проверки сообщения должен опросить указанных лиц в первоочередном порядке, чтобы решить следующие вопросы:

1) какие силы и средства необходимо привлечь для производства осмотра места происшествия;

2) сколько специалистов и в каких областях знаний целесообразно задействовать в сложившейся ситуации;

3) перечень технических средств, применяемых следователем и специалистом при производстве осмотра;

4) какие предметы необходимо осмотреть на месте, а какие изъять для последующего осмотра и назначения экспертизы;

5) какие экспертизы должны быть проведены для определения способа совершения преступления и оценки причиненного ущерба;

6) относится ли информация, к которой получен неправомерный доступ, к конфиденциальной;

7) получатель выгоды от противоправных действий (неизвестное лицо, желающее заработать, конкуренты, лица из числа работников и т. д.).

8) был ли активирован механизм двухфакторной аутентификации в сервисах социальных сетей, мессенджерах и портале «Госуслуги». Кто имел доступ к телефону пострадавшего, кому он сообщал персональные данные и информацию из СМС.

Также следует иметь в виду, что решение о возбуждении уголовного дела следователем принимается не только на основании материалов предварительных проверок заявлений пострадавших лиц, но и по материалам органов, осуществляющих оперативно-розыскную деятельность при реализации оперативных разработок, результатов ОРМ по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших.

Следователь не имеет права проводить оперативно-розыскные мероприятия, однако может быть их инициатором путем дачи поручения органу дознания, а также оценивает их результаты с точки зрения относимости, допустимости, достоверности и достаточности для принятия процессуального решения. В материалах, представленных по результатам ОРД, должны быть сопроводительные документы, ответы на запросы, рапорты, протоколы и акты проведенных ОРМ, объяснения должностных и иных лиц, справки по результатам проведенных исследований.

После выполнения первоначальных процессуальных действий следователь должен провести анализ материалов и выделить характерные элементы, свойственные для рассматриваемой категории преступлений.

Среди признаков преступлений, связанных с неправомерным доступом к компьютерной информации, которые необходимо установить на начальном этапе, можно выделить следующие.

1. **Установление неправомерности доступа к информации.** В уголовном законе законодателем не уточнено понятие доступа к информации, однако указанное определение содержится в п. 6 ст. 2 Закона об информации: «доступ к информации – возможность получения информации и её использования». Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) под неправомерным доступом понимают доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми

полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств её защиты[1].

В соответствии с Постановлением Пленума Верховного Суда Российской Федерации «неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа)»[2].

Для установления указанного признака следователю необходимо провести ряд процессуальных действий, направленных на получение следующих сведений:

– определить, что произошел доступ к информации, которая относится к государственной тайне, либо к конфиденциальной информации (налоговая, коммерческая, банковская, врачебная тайна, персональные данные и т. д.). Указанные сведения можно получить из допросов лиц, осуществляющих работу с информацией, путем направления соответствующих запросов в организацию, где произошел неправомерный доступ, проведения экспертизы информации на предмет отнесения её к соответствующей категории сведений;

– установить правообладателя информации и допросить его, отразив данные о количественных и качественных характеристиках информации, к которой произошел доступ.

2. **Установление способа совершения преступления.** Способы совершения преступления, предусмотренного ст. 272 УК РФ, можно разделить на две группы.

К первой относятся способы непосредственного воздействия лица на компьютерную информацию, когда проникновение осуществляется путем введения различных команд в компьютерную систему. В этом случае следы совершения преступления останутся только на носителе компьютерной информации, задействованном при совершении преступного посягательства.

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). URL: http://genproc.gov.ru (дата обращения: 20.08.2023).

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Российская газета. 2022. 28 дек.

Такой доступ может осуществляться как лицами, имеющими право на него, так и лицами, специально проникающими в зоны с ограничениями по допуску.

Вторая группа – это способы удаленного (опосредованного) воздействия на компьютерную информацию, например: проникновение в чужие информационные сети путем соединения с тем или иным компьютером; проникновение в компьютерную систему с использованием чужих идентификационных данных; подключение к линии связи легитимного пользователя с получением доступа к его системе; использование вредоносных программ для удаленного доступа к информации и т. п.

Наиболее распространенными являются следующие действия злоумышленников:

– подбор паролей, ключей и другой идентификационной или аутентификационной информации. Так, П. с целью продажи информации о логине и пароле доступа к интернет-сайту путем подбора логина и пароля совершил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в административной панели интернет-сайта www.serdolik-club.ru, после чего изменил их, что повлекло модификацию и блокировку содержащейся на нем компьютерной информации. Вышеописанные действия П. органом предварительного следствия квалифицированы по ч. 2 ст. 272 УК РФ[1].

Особое внимание следует уделить способам обхода механизмов двухфакторной аутентификации социальных сетей «ВКонтакте» и «Одноклассники», мессенджерам WhatsApp и Telegram, Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)»: кто связывался с пострадавшим, каким образом произошла утечка информации из СМС и др.

– подмена IP-адресов пакетов, передаваемых по сети Интернет или другой глобальной сети, так, что они выглядят поступившими изнутри сети, где каждый узел доверяет адресной информации другого; инициирование отказа в обслуживании – воздействие на сеть или отдельные её части с целью нарушения порядка штатного функционирования;

– несанкционированный доступ, в том числе и к незащищенным каналам связи, прослушивание и расшифровка трафика с целью сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации;

– сканирование с использованием программ, последовательно перебирающих возможные точки входа в систему (например, номера TCP-портов или телефонные номера) с целью установления путей и возможностей проникновения; подмена, навязывание, уничтожение,

[1] Приговор Устиновского районного суда г. Ижевска Удмуртской Республики суда №1-256/2017. – URL: https://sudact.ru/regular/doc/jBGlh8PHvnrc (дата обращения 15.09.2023).

переупорядочивание или изменение содержимого данных (сообщений), передаваемых по сети, и др.[1]

Для правильной квалификации преступления и определения предмета доказывания следователь должен:

– выяснить меры, предпринятые правообладателем информации по её защите. В случае, если речь идет о неправомерном доступе к информации в организации, необходимо опросить лиц из числа ответственных за обеспечение её защиты, системного администратора, специалиста по сетевой инфраструктуре.

3. Установление последствий преступления. Состав преступления, предусмотренный ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», как и подавляющее большинство иных составов в главе 28 УК РФ предусматривает наступление последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации.

Таким образом, в ходе проверки сообщения и последующего предварительного расследования необходимо установить, какие конкретно действия, образующие состав преступления, были выполнены правонарушителем. В ходе проведения процессуальных действий (получение объяснений, проведение осмотра, экспертизы, направление требований и запросов) документируется способ и последствия совершения преступления.

Принимая во внимание, что состав данного преступления носит материальный характер, он предполагает обязательное наступление одного из последствий:

а) *уничтожение информации* – приведение информации или её части в непригодное для использования состояние независимо от возможности её восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

б) *блокирование информации* – результат воздействия 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, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с её уничтожением. При этом нельзя признать блокированием информации последствия, которые наступили в результате действий не злоумышленника, а уполномоченного обеспечивать безопасность данных лица (например, временное блокирование службой безопасности организации доступа всех

[1] Лебедева А. А. Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6. С. 48–56.

либо отдельных пользователей к определенной информации, попытка доступа к которой была предпринята правонарушителем);

в) *модификация информации* – внесение изменений в компьютерную информацию (или её параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) *копирование информации* – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывание информации путем любого перехвата информации и т. п.

Отдельного внимания заслуживает вопрос оценки общественной опасности модификации и копирования информации, как имеющий важное значение для исключения возможной малозначительности деяния. С этой целью в каждом таком случае необходимо перед принятием решения о возбуждении уголовного дела, а также привлечении лица к уголовной ответственности выяснять, какая именно информация была подвергнута угрозе, повлияли ли совершенные действия на нормальное функционирование объекта преступного посягательства, какой вред нанесен либо мог быть нанесен вследствие изменения или утечки данных (как имущественный, так и неимущественный).

Одновременно следует отметить, что копирование, уничтожение, модификация информации могут быть вызваны не только преднамеренными неправомерными действиями, но и ошибками, неумышленным неправильным поведением персонала потерпевшей организации при профилактике, техническом обслуживании либо ремонте компьютера, компьютерной системы или сети; случайных неумышленных повреждениях аппаратуры, обрывах соединительных кабелей при нестандартном поведении в помещении, где расположены компьютеры, подключенные к ним устройства, компьютерная система или сеть; ошибочных действиях оператора в процессе работы, приведших к разрушению информационных данных; и неумышленном неправильном обращении с машинными носителями информации в ходе их использования и хранения и т. д.

Обратим внимание, что очень часто среди особенностей совершения рассматриваемой категории преступлений можно отметить то обстоятельство, что такие преступления имеют более сложную структуру, в которой выделяют совершение предикатного преступления, предусмотренного главой 28 УК РФ «Преступления в сфере компьютерной информации», и общеуголовное преступление против собственности (в основном хищения).

Алгоритм производства первоначальных процессуальных и организационно-тактических действий следователем по уголовным делам о неправомерном доступе к компьютерной информации, в зависимости от следственной ситуации и способа совершения преступления

Перед началом описания порядка действий следователя отметим, что в данной работе минимизировано дублирование наиболее «типовых» тезисов научных трудов по расследованию уголовных дел о преступлениях, совершенных путем социальной инженерии. Кроме того, в целях индивидуализации каждого из нижеприведенных алгоритмов, практически исключено повторное описание действий, которые необходимо произвести при различных способах совершения преступления. В этой связи для обеспечения полного и всестороннего расследования уголовного дела предлагаем обращать внимание на приведенные рекомендации комплексно, одновременно акцентируя свое внимание на одной из предложенных схем выполнения первоначальных процессуальных мероприятий.

1. *Неправомерный доступ к аккаунтам социальных сетей «ВКонтакте» и «Одноклассники», мессенджерам WhatsApp и Telegram, порталу «Государственные услуги», приложению «Сбербанк Онлайн».*

Сервисы социальных сетей, приложение «Сбербанк Онлайн» и в настоящий момент портал «Госуслуги» защищены системой двухфакторной аутентификации, что затрудняет «взлом» указанных сайтов и приложений.

При производстве первоначальных процессуальных действий от пострадавшего необходимо получить следующую информацию:

– с какого устройства он посещает указанные ресурсы;

– установлено ли на его телефоне соответствующее приложение (когда, через какие сервисы, какая версия приложения);

– кто имеет доступ к телефону (знает пароль или зарегистрированы биометрические данные);

– кто в последнее время звонил пострадавшему (с портала «Госуслуги», банков, правоохранительных органов);

– какой вид связи использовался при звонке (через мессенджеры или оператора сотовой связи);

– кому и какую информацию сообщал пострадавший, каким способом (голосом, через СМС и др.);

– какая персональная информация стала известна злоумышленникам по результатам разговора;

– записывался ли телефонный разговор пострадавшим;

– как был обнаружен неправомерный доступ к информации (рассылка сообщений из списка друзей, перевод денег, запрос на кредит и т. д.).

После установления способа, даты и времени неправомерного доступа к информации следователь направляет запросы в соответствующие организации с указанием перечня сведений, которые имеют криминалистическое значение для раскрытия и расследования преступления.

К таким сведениям можно отнести:

– с какого IP-адреса был произведен доступ в личный кабинет пострадавшего;

– использовался ли ранее IP-адрес для доступа к другим аккаунтам пользователей;

– имеются ли сведения о геолокации пользователя;

– какие действия производились в личном кабинете пользователя (изменение персональных данных, рассылка сообщений, связь со службой технической поддержки и т. д.);

– на какие расчетные счета переведены денежные средства, и кто их владелец;

– изменялся ли способ защиты аккаунта (номер телефона, адрес электронной почты и иное);

– кем, в результате каких действий и какая информация была заблокирована (уничтожена, модифицирована, скопирована).

При осмотре мобильного телефона или компьютера пострадавшего следователь должен сделать снимки экрана (скриншоты), чтобы точно отследить дату и время совершения преступления. Исходя из этой информации направляется запрос провайдеру сети Интернет или оператору сотовой связи с целью установить IP-адрес и местоположение лиц, которые связывались с пострадавшим.

2. *Шифрование (блокирование) данных на компьютере с целью вымогательства денежных средств.* Говоря о шифровании (блокировании) данных пользователя на компьютере, отметим, что в уголовном праве на сегодняшний день не выработан единый подход к квалификации такого рода деяний, условно называемых «кибервымогательство». Проблема в том, что преступники, выдвигая требования передачи денежных средств, угрожают уничтожением информации либо её блокированием. Таких видов угроз ст. 163 УК РФ не предусматривает. Как отмечают отдельные авторы, квалификация должна быть с вменением квалифицирующих признаков, предусмотренных в ч. 2 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ») – «корыстная цель» и, возможно, «причинение крупного ущерба», так как лицо, используя компьютерную программу и осуществляя неправомерный доступ к компьютерной информации, преследует цель – извлечение материальной выгоды[1].

[1] Стяжкина С. А. Вопросы квалификации кибервымогательства // Вестник Удмуртского университета. Экон омика и право. 2022. Т. 32. Вып. 5. С. 941–947.

С целью устранения указанного пробела на основании внесенных МВД России и иными органами исполнительной власти предложений, Генеральной прокуратурой Российской Федерации подготовлен проект федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации», предусматривающий ряд значимых изменений в ст.ст. 135, 150, 158, 159, 159.3, 159.6, 163, 272-274.1 УК РФ, которым предлагается дополнить диспозицию ч. 1 ст. 163 УК РФ словами «либо сопряженное с вмешательством в функционирование средств хранения обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, либо под угрозой такого вмешательства». В настоящее время законопроект проходит стадию согласования.

К первоначальным процессуальным действиям в данной следственной ситуации необходимо отнести:

– принятие заявления от пострадавшего лица и получение объяснения, в котором необходимо отразить ответы на следующие вопросы:

1) точное время обнаружения блокировки (шифрования) данных;

2) кто имеет физический доступ к компьютеру;

3) кто и когда устанавливал операционную систему, программы, сетевое оборудование (маршрутизатор), у кого имеются данные для управления указанными устройствами;

4) какие учетные записи пользователей имеются в операционной системе;

5) какой уровень владения и знаний пострадавшего в области информационных технологий;

6) установлен ли в системе антивирус;

7) пользуется ли пострадавший нелицензионным программным обеспечением, программами, скачанными с сомнительных ресурсов, торрентов и т. д.;

8) какие программы и файлы открывались в последнее время и были ли среди них новые программы и сомнительные ссылки (к примеру, в письме, пришедшем на электронную почту);

9) какие требования выдвигались лицом для расшифровки файлов (отключения блокировки доступа к файлам);

10) по какому каналу связи получено сообщение от вымогателя: точное время, содержание, реквизиты для оплаты и т. д.

В случае шифрования данных организации дополнительно могут быть выяснены детали настройки удаленного доступа к серверу, в том числе, какой протокол использовался (RDP или VPN) и был ли закрыт порт 3389, а также установлено ли ограничение запуска небезопасных файлов и блокирование IP-адресов при неоднократных неудачных попытках входа, как часто и каким образом осуществляется резервное копирование;

– осмотр компьютера с участием специалиста и пострадавшего. Перед началом осмотра создается побайтовая копия данных накопителя с информацией, которая впоследствии и осматривается. Изучаются логи операционной системы, история браузера, содержащаяся в электронном почтовом ящике корреспонденция, осматривается файловая система с указанием даты и времени модификации файлов, фиксируются права доступа пользователей к блокированным файлам, по возможности определяется способ заражения файловой системы;

– при получении криминалистически значимой информации о лице, совершившем преступление, следует принять меры к установлению его личности и местонахождения. Если в требовании указаны банковские реквизиты, необходимо направить запрос в банк для установления владельца счета. В случае направления сообщения посредством социальных сетей и мессенджеров необходимо направить запрос в соответствующие компании и запросить информацию о владельце аккаунта, IP-адресах, с которых он заходил, списки лиц, с которыми он активно общается, получить мультимедиа файлы, содержащие лицо предполагаемого преступника. Кроме того, необходимо направить запрос провайдеру сети Интернет и запросить информацию об удаленных IP-адресах, с которых возможно осуществлялась атака на компьютер пострадавшего. Если в требовании указан криптокошелек злоумышленника, целесообразно осуществить его поиск наодном из специализированных сайтов (например, https://www.blockchain.com/), где самостоятельно либо с привлечением специалиста отследить цепочки сделок имеющегося идентификатора. Также, мониторинг криптовалютных операций может быть произведен с помощью программы Росфинмониторинга «Прозрачный блокчейн. Государственный модуль», к которой подключены сотрудники МВД России по всей стране. В случае установления в ходе анализа финансовых потоков централизованной платформы (биржи либо обменного пункта, с помощью которых осуществлялся обмен криптовалюты на фиатные денежные средства), следует направить запрос её владельцам для получения персональных данных интересующего лица;

– в зависимости от способа получения вредоносного файла, скрипта в сети Интернет необходимо произвести осмотр соответствующего сайта, установить его IP-адрес с помощью сервиса https://whois.ru. Таким образом, можно узнать, за кем закреплена соответствующая подсеть и диапазон IP-адресов и определить хостинг сайта. Далее следует направить запрос регистратору доменного имени для установления владельца сайта. Сложность в проведении данной операции заключается в том, что на сегодняшний день отсутствует единый и систематический учет всех операторов связи. Для проверки почтового ящика также можно использовать специализированные ресурсы: hunter.io (проверка существования почтового ящика), haveibeenwned.com или dehashed.com (проверка адреса на предмет взлома), emailrep.io (проверка репутации и упоминания почтового ящика)

и специализированное программное обеспечение, позволяющее собрать информацию из общедоступных источников об IP-адресе, имени хоста, стране и др. (например, infoga);

– в дальнейшем целесообразно назначить экспертизу по созданной в ходе осмотра копии на предмет выявления закономерностей следообразования при блокировании (шифровании) информации, способов проникновения вредоносной программы в файловую систему и т. д.;

– необходимо задействовать органы, осуществляющие оперативно-розыскные мероприятия, у которых имеются возможности провести комплекс технических мероприятий по установлению лиц, причастных к совершению преступления, а также осуществить проверку информации о вирусе и имеющихся у разработчиков антивирусных программ цифровых следах, оставленных его создателями и распространителями (например, компания Dr.Web предлагает для проверки подозрительных объектов онлайн-сервис Dr.Web vxCube – анализатор, позволяющий получить отчет о том, как именно действует файл в системе, какие вносит в неё изменения, с какими ресурсами соединяется, а также создает карту его сетевой активности). С этой целью следует дать поручение органу дознания, который может оказать значимую помощь следователю в получении как ориентирующей, так и доказательственной информации;

– при установлении подозреваемого лица необходимо провести обыск по месту проживания подозреваемого с целью обнаружения и изъятия предметов, используемых для совершения преступления, средств компьютерной техники, специальной литературы. Кроме того, в зависимости от следственной ситуации может быть актуальным проведение таких процессуальных действий как «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» (ст. 185 УПК РФ), «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» (ст. 186.1 УПК РФ).

3. *Копирование конфиденциальной информации пользователя (организации) в виде логинов и паролей к различным информационным ресурсам и базам данных, а также иной охраняемой законом информации.*

При получении объяснения от пострадавшего и его допросе необходимо:

– установить способ неправомерного доступа к конфиденциальной информации. Это может быть как непосредственный доступ к компьютеру (члены семьи, знакомые и т. д.), так и удаленный доступ к рабочему столу, взлом браузера и копирование паролей, зеркалирование и синхронизация данных различных программных продуктов, получение доступа через открытые порты маршрутизатора и компьютера, использование вредоносного программного обеспечения. В случае неправомерного доступа к информации в организации необходимо опросить системных администраторов, операторов, специалистов, занимающихся эксплуатацией и ремонтом

компьютерной техники, программистов, инженеров по средствам связи, специалистов, обеспечивающих информационную безопасность, сотрудников службы безопасности и других;

– с участием специалиста и представителя организации осмотреть материально-техническую базу организации (рабочие места, сервера, коммутационное оборудование). Рекомендуется составить схему локальной сети с подробным указанием точек соединения с сетью Интернет, особенностями маршрутизации в рамках локальной подсети, наличием в сети доменов, VPN- и прокси-серверов. Особое внимание необходимо уделить проверке (сканированию) портов на предмет их открытости (доступности) из сети Интернет, зафиксировать настройки маршрутизации, параметры демилитаризованной зоны, переадресации портов. Обязательно отразить в протоколе наличие программного обеспечения, фиксирующего историю трафика в сети и выгрузить логи из программы;

– истребовать у провайдера логи подозрительных подключений к компьютеру пострадавшего и его активности. К таковым можно отнести, к примеру, использование порта 3389 (удаленный рабочий стол), переходы по фишинговым сайтам, скачивание торрентов, подозрительный трафик на заблокированные Роскомнадзором ресурсы и т. д.

– в случае атаки на сервер организации запросить у провайдера информацию по удаленному подключению к серверам организации по уязвимым портам. Одним из самых популярных портов, несомненно, является порт 21(FTP). Он позволяет передавать файлы между разными компьютерами, подключенными к сети TCP, и используется для удаленной аутентификации с сервером. Другой широко используемый порт – 22 для протокола SSH. Он предназначен для удаленного управления и изменения серверов в сети. Он имеет механизм аутентификации пользователя и был создан для безопасной замены Telnet. Сегодня это одна из основных целей киберпреступников. Telnet(23) – хотя это старый протокол, он все ещё используется злоумышленниками и позволяет удаленно подключаться к другому компьютеру. SMTP(25) и POP(110) – протоколы обмена почтовыми сообщениями (электронной почты) между различными устройствами, подключенными к сети. HTTP (80) и HTTPS(43) – базовые протоколы в сети для передачи информации (в основном для отображения сайтов);

– после установления последствий копирования информации необходимо отправить запросы провайдерам Интернет-услуг и владельцам сайтов, где был осуществлен вход по учетным данным пострадавшего с целью получения даты, времени, IP- и MAC-адресов сетевого оборудования, с помощью которого осуществлялся доступ. Если злоумышленники не использовали анонимизацию в виде VPN-, прокси-серверов и Tor-браузера, то можно установить их местонахождение;

– с участием специалиста осмотреть сервер организации с целью установления по логам необычной активности в сети, включая

несанкционированные попытки входа в систему, сканирования портов или необычную передачу данных, аномальное поведение пользователей, необычные системные события, аномальный трафик данных, необычные запросы или активность на веб-сервере;

– дать поручение органу дознания о проведении оперативно-розыскных мероприятий по выявлению причастности к совершению преступления лиц из числа сотрудников организации.

4. *Блокирование, отказ в доступе (DDoS-атаки) к инфраструктуре организации.*

Анализ судебной практики позволяет выявить определённые проблемы в квалификации совершённых деяний. При осуществлении DDoS-атаки на Интернет-ресурс неправомерного доступа к компьютерной информации по смыслу ст. 272 УК РФ не происходит. Обращение к находящейся в открытом доступе компьютерной информации является по умолчанию правомерным и не ограничено лимитированным количеством запросов к ней. Иными словами, если одно и тоже лицо открывает один и тот же сайт в сети Интернет одновременно с помощью различных устройств, когда каждый из них имеет свой IP-адрес, то с технической точки зрения ресурс открывается сразу для множества пользователей, и это не значит, что доступ к компьютерной информации неправомерен.

В настоящее время судебная практика идёт по пути вменения организаторам DDoS-атак ст. 273 УК РФ, то есть использования вредоносных компьютерных программ, – судами в основном даётся оценка именно по использованию вредоносной программы, однако никак не квалифицируются действия по «заражению» компьютеров, которые затем и отправляют сетевые запросы, устраивая DDoS-атаку[1].

В ходе предварительного следствия по уголовным делам рассматриваемой категории необходимо:

– при получении объяснения от пострадавшего и его допросе установить список недоброжелателей и конкурентов, которым выгодно по финансовым или иным причинам блокирование определенного сайта организации или его отдельных ресурсов (базы данных, корпоративного программного обеспечения);

– особое внимание следует уделить показаниям системного администратора, лиц, отвечающих за защиту информации и сотрудников безопасности организации. В протоколе допроса следует отразить алгоритмы функционирования сети в организации, список используемого программного обеспечения, аппаратные ресурсы серверов и их взаимодействие с остальной информационной инфраструктурой компании, подозрительные сетевые события на протяжении последнего времени и т. д.;

[1] Вестов Ф. А., Шамьенов Н. Р. Актуальность ответственности в уголовном праве за DoS и DDoS-атаки в сфере компьютерной информации. URL: https://cyberleninka.ru/article/n/aktualnost (дата обращения 17.09.2023).

– к осмотру рабочих мест, коммутационного оборудования и сервера целесообразно привлечь специалиста, который с использованием специализированного программного обеспечения сможет оказать помощь в получении как ориентирующей, так и доказательственной информации. Кроме того, необходимо провести осмотр и изъять логи программ-анализаторов сетевого трафика;

– дать поручение органу дознания о проведении комплекса специализированных оперативно-розыскных мероприятий с целью установления источников атаки;

– направить запрос провайдеру Интернет-услуг с требованием предоставить IP-адреса устройств, с которых осуществлялась атака на сервер организации. Впоследствии по IP-адресам можно установить физическое местонахождение устройств.

Таким образом, к первоначальным процессуальным действиям по преступлениям, связанным с неправомерным доступом к компьютерной информации, можно отнести получение показаний от пострадавших физических лиц или сотрудников организации (администраторов сети, инженеров-программистов, операторов, специалистов, занимающихся эксплуатацией и ремонтом компьютерной техники, работников службы безопасности и других). В ходе допросов необходимо уделить внимание способу обхода двухфакторной аутентификации для получения доступа к аккаунтам социальных сетей «ВКонтакте» и «Одноклассники», мессенджерам WhatsApp и Telegram, порталу «Государственные услуги». Осмотр места происшествия и изъятие электронных носителей информации следует проводить с участием специалиста, который также окажет помощь при выборе экспертного учреждения, формирования вопросов для проведения последующих экспертиз. Немаловажным элементом раскрытия преступления является грамотное привлечение к указанной деятельности сотрудников органа дознания.

ЗАКЛЮЧЕНИЕ

В данном исследовании на основе анализа теоретических положений наук уголовного процесса и криминалистики, норм уголовно-процессуального права, правоприменительной практики и опыта производства процессуальных действий предложены тактические рекомендации производства предварительного следствия по уголовным делам о преступлениях, связанных с неправомерным доступом к компьютерной информации, в том числе совершенных путем кибератак (сетевых атак).

Следует учитывать, что в диспозиции ст. 272 УК РФ говорится именно об охраняемой законом компьютерной информации, к которой относят информацию ограниченного доступа, включая сведения, составляющие государственную, коммерческую, служебную и иную тайну, а также конфиденциальную информацию. Это информация, для которой законодателем установлен специальный режим правовой защиты.

Особое значение для следователя имеет определение понятия «неправомерный доступ к компьютерной информации», как позволяющее раскрыть способы совершения и сокрытия таких преступлений. Неправомерный доступ к компьютерной информации означает получение данных сведений незаконным или несанкционированным способом. Это включает проникновение в источники информации при помощи компьютерных технологий и возможность её использования. Сам неправомерный доступ может осуществляться непосредственно, удаленно или комбинированно. В результате совершения преступления появляются электронно-цифровые следы, которые возникают в результате изменения компьютерной информации.

Общая тактика осмотра, обыска и выемки при расследовании неправомерного доступа к компьютерной информации мало чем отличается от традиционного порядка производства указанных следственных действий, однако есть свои особенности.

Так, привлекая к их производству в качестве специалиста сведущее лицо, не являющееся экспертом, следователь должен по возможности убедиться в наличии у него достаточной компетентности для решения предстоящих задач. Формирование типичного перечня задач, реализуемых специалистом при подготовке и в процессе производства следственных действий, позволило выработать представление о требуемых компетенциях привлекаемых лиц и необходимом объеме действий по обеспечению эффективности следственных действий, обнаружению и фиксации компьютерной информации, имеющей доказательственное значение.

Во многих ситуациях производства следственных действий копирование информации в электронном виде, имеющей значение для расследования, является приемлемой альтернативой изъятию электронных носителей этой информации, а в ряде случаев, единственно возможной формой фиксации.

Общей рекомендацией при назначении судебных компьютерно-технических экспертиз является обязательное предварительное согласование всех выносимых следователем на экспертизу вопросов с экспертом.

Однако также важно понимать, что юридически значимый факт, например, «уничтожения» или «модификации» устанавливает не эксперт или специалист при проведении исследования, а именно следователь, проводящий расследование, путем обнаружения и закрепления совокупности доказательств интересующего события.

Вопросы признания представленного на исследование программного обеспечения «вредоносным» либо определения его как заведомо предназначенного для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации могут быть решены в ходе производства СКТЭ в области исследования программного обеспечения.

Предложенные в данном пособии обобщения и выводы предназначены для сотрудников следственных подразделений органов внутренних дел и могут быть использованы в рамках их служебной подготовки. Кроме того, учитывая широкий ракурс рассмотрения темы исследования, рекомендации актуальны для изучения в рамках дисциплин «Методы и способы получения доказательственной информации с электронных носителей», «Расследование преступлений в сфере компьютерной информации» слушателями образовательных организаций МВД России.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ // СПС «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. №63-ФЗ // СПС «КонсультантПлюс».

3. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс».

4. О государственной тайне : закон РФ от 21.07.1993 № 5485-1 // СПС «КонсультантПлюс».

5. Об утверждении Перечня сведений конфиденциального характера : указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) // СПС «КонсультантПлюс».

6. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «КонсультантПлюс».

7. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Российская газета. – 2022. – 28 дек.

Монографии, учебники, учебные пособия

1. Miloslavskaya N. Remote Attacks Taxonomy and their Key Verbal Indicators / N. Miloslavskaya // Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA 2017) (Moscow (Russia), 1-6 August 2017) // Procedia Computer Science, 2018.

2. Бегишев И. Р. Преступления в сфере обращения цифровой информации : монография. / И. Р. Бегишев, И. И. Бикеев– Казань : Познание, 2020. – 300 с.

3. Варданян А. В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А. В. Варданян, Е. В. Никитина. – Москва, 2007. – 307 с.

4. Васильева И. Н. Расследование инцидентов информационной безопасности : учебное пособие / И. Н. Васильева. – Санкт-Петербург : изд-во СПбГЭУ, 2019. – 177 с.

5. Гаврилов М. В. Осмотр при расследовании преступлений в сфере компьютерной информации /М. В. Гаврилов, А. Н. Иванов. – Москва, 2007. – 165 с.

6. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. – Часть 1. Обзор и концепции. – Москва : Стандартинформ, 2012.

7. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. – Москва : Стандартинформ, 2015.

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

9. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова // − Т. 2. – Москва : Проспект, 2022. – 792 с.

10. Ловцов Д. А. Информационное право : учебное пособие. / Д. А. Ловцов – Москва : РАП, 2019. – 226 с.

11. Саенко Г. В. Компьютерная экспертиза. Исследование компьютерной информации / Г. В. Саенко, О. В. Тушканова // Практическое руководство по производству судебных экспертиз для экспертов и специалистов : науч.-практич. пособие / под ред. Т. В. Аверьяновой, В. Ф. Статкуса. – Москва : Юрайт, 2011. – 724 с.

Научные статьи, публикации, диссертации

1. Kostina A. Information Security Incident Management / A. Kostina, N. Miloslavskaya, A. Tolstoy // Proceedings of the 3rd International Conference on Internet Technologies and Applica-tions (Wrexham (UK), 8-11 September 2009). – 2009. – P. 27–34;

2. Malyuk A. Information Security Theory Development / A. Malyuk, N. Miloslavskaya // Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014) (Glasgow (UK), 9-11 September 2014). – ACM New York, 2014. – P. 52–55.

3. Miloslavskaya N. Information Visualisation in Information Security Management for En-terprises's Information Infrastructure / N. Miloslavskaya, A. Tolstoy, A. Birjukov // Scientific Visualisa-tion. – Moscow, MEPhI, 2014. – Vol. 6. – № 2. – P. 74–91.

4. Miloslavskaya N. Taxonomy for Unsecure Big Data Processing in Security Operations Centers / N. Miloslavskaya, A. Tolstoy, S. Zapechnikov // Proceedings of 2016 4th International Confer-ence on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016) (Vienna (Austria). 22-24 August 2016). – 2016. – P. 154–159.

5. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09 / В. Ю. Агибалов. – Воронеж, 2010. – 198 с.

6. Васильева Н. А. Способы сокрытия цифровых следов преступления / Н. А. Васильев // Наука. − 2021. − № 2 (17). − С. 75.

7. Давыдов В. О. О некоторых аспектах криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации / В. О. Давыдов, Е. Д. Малахвей // Известия Тульского государственного университета. Экономические и юридические науки. − 2019. − № 2. − С. 98.

8. Дёмин К. Е. Об методических основах получения криминалистически значимой информации, содержащейся в электронных носителях данных / К. Е. Демин // Вестник Московского университета МВД России. − 2018. − № 4. − С. 45.

9. Жоров Е. Д. Особенности криминалистической характеристики личности лица, совершающего неправомерный доступ к компьютерной информации / Е. Д. Жоров, П. В. Тепляшин // Эпоха науки. − 2018. − № 14. − С. 71.

10. Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовным делам : дис.... канд. юрид. наук : 12.00.09 / А. И. Зазулин. − Екатеринбург, 2018.

11. Захарова А. В. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации / А. В. Захарова // Бюллетень магистранта. − 2019. − № 5.

12. Колычева А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук : 12.00.12 / А. Н. Колычева. − Москва, 2018. − С. 47.

13. Лебедева А. А. Особенности расследования киберпреступлений / А. А. Лебедева // Безопасность бизнеса. – 2021. – № 6. – С. 48–56.

14. Ленков О. В. Производство осмотра места происшествия по делам о неправомерном доступе к компьютерной информации / О. В. Леонков // Научные исследования. − 2018. − № 7. − С. 55.

15. Малышкин П. В. Особенности сокрытия следов совершенных преступлений, совершаемых с применением информационных компьютерных технологий / П. В. Малышкин // Мир науки и образования. − 2016. − № 4 (8). − С. 43.

16. Мурузиди А. В. Методика расследования преступлений в сфере компьютерной информации / А. В. Мурузиди, Е. Г. Рыжков // Современная наука : актуальные вопросы, достижения и инновации : сборник статей VI Международной научно-практической конференции. – Пенза : Наука и Просвещение, 2019.

17. Пырьева Е. И. Способы и средства сокрытия неправомерного доступа к компьютерной информации / Е. И. Пырьева // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – Воронеж : Воронежский институт МВД РФ, 2020. − № 1 (6). − С. 78.

18. Россинская Е. Р. Современные способы компьютерных преступлений и закономерности их реализации / Е. Р. Россинская, И. А. Рядовский // Lex russica (Русский закон). − 2019. − № 3. − С. 89−90.

19. Савельева А. А. О способах совершения неправомерного доступа к компьютерной информации / А. А. Савельева // Молодой ученый. − 2020. − № 48 (338). − С. 328.

20. Симонян А. А. Уголовно-правовая юрисдикция в отношении преступлений в сфере компьютерной информации / А. А. Симонян // Молодой ученый. – 2020. – № 23 (313). – С. 288–291.

21. Стяжкина С. А. Вопросы квалификации кибервымогательства / С. А. Стяжкина // Вестник Удмуртского университета. Экономика и право. – 2022. – Т. 32. – Вып. 5. – С. 941–947.

22. Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук : 12.00.12 / Е. С. Шевченко. – Москва, 2016. – С. 63.

Материалы практики

1. Определение Первого кассационного суда общей юрисдикции от 16.04.2020 № 77-357/2020 // СПС «КонсультантПлюс» (дата обращения 15.09.2023).

2. Определение Первого кассационного суда общей юрисдикции от 21.04.2020 № 77-530/2020 СПС «КонсультантПлюс» (дата обращения 15.09.2023).

3. Приговор Бабушкинского районного суда г. Москвы от 20.09.2016 по делу № 01-0313/2016. − URL: https://sud-praktika.ru/precedent/97705.html (дата обращения: 06.05.2023).

4. Приговор Хасавюртовского городского суда Республики Дагестан № 1-261/2020 от 20.07.2020 по делу № 1-261/2020. – URL: https://sudact.ru/regular/doc/SlYwK6TxKKNT/ (дата обращения: 06.05.2023).

5. Приговор Дзержинского районного суда г. Оренбурга Оренбургской области от 28.01.2019 по делу № 1-504/2018. – URL: https://sudact.ru/regular/doc/smPVc9O2vldJ/ (дата обращения: 04.05.2023).

6. Приговор Петушинского районного суда Владимирской области от 02.07.2020 по делу № 1-85/2020. – URL: https://sudact.ru/regular/doc/EOr66Jg (дата обращения: 04.05.2023).

7. Приговор Дзержинского районного суда г. Оренбурга Оренбургской области от 28.01.2019 по делу № 1-504/2018. – URL: https://sudact.ru/regular/doc/smPVc9O2vldJ/ (дата обращения: 04.05.2023).

8. Постановление Калужского районного суда №1-31/2019 1-986/2018 от 21 января 2019 г. по делу №1-31/2019. – URL: https://sudact.ru/regular/doc/fxZzClQ44blJ. (дата обращения 15.09.2023).

9. Приговор Устиновского районного суда г. Ижевска Удмуртской Республики суда №1-256/2017. URL: https://sudact.ru/regular/doc/jBGlh8PHvnrc (дата обращения 15.09.2023).

Ресурсы сети Интернет

1. ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) [Электронный ресурс]: Веб-сайт / MITRE. – MITRE. – URL: https://attack.mitre.org/ (дата обращения 16.03.2023).

2. Common Attack Pattern Enumeration and Classification [Электронный ресурс]: Веб-сайт / MITRE. – MITRE. – URL: https://capec.mitre.org/ (дата обращения 16.03.2023).

3. Graham R. FAQ: Network Intrusion Detection Systems. 2000. [Электронный ресурс]: Веб-сайт / LINUXSECURITY / R. Graham. – URL: – http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion.

4. Hutchins E. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [Электронный ресурс]: Веб-сайт / LOCKHEEDMARTIN / E. M. Hutchins, M. J. Cloppert, R. M. Amin. – Lockheed Martin, 2010. – URL: http://www.lockheedmartin.com/content/dam/lockheed/data/ corporate/doc.

5. Olzak T. The five phases of a successful network penetration. 2008. [Электронный ресурс]: Веб-сайт / TECHREPUBLIC / T. Olzak. – URL: http://www.techrepublic.com/blog/ it-security/the-five-phases-of-a-successful-network-penetration.

6. Актуальные способы взлома паролей. − URL: https://spy-soft.net/password-cracking-methods/ (дата обращения: 08.06.2023).

7. Анализ и интерпретация лог-файлов. – URL: https://www.web-patrol.net/webanalytics-logfile.html (дата обращения: 10.05.2023).

8. Вестов Ф. А. Актуальность ответственности в уголовном праве за DoS и DDoS-атаки в сфере компьютерной информации / Ф. А. Вестов, Н. Р. Шамьенов. – URL: https://cyberleninka.ru/article/n/aktualnost-otvetstvennosti-v-ugolovnom-prave-za-dos-i-ddos-ataki-v-sfere-kompyuternoy-informatsii (дата обращения 17.09.2023).

9. Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (Версия 2.3). – Банк России. – URL: http://cbr.ru/StaticHtml/File/14408/ inforegl_23.pdf (дата обращения 16.03.2023).

10. Доказательная сила логов. – URL: https://www.securitylab.ru/contest (дата обращения: 12.05.2023).

11. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения 15.09.2023).

12. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) – URL: http://genproc.gov.ru (дата обращения: 20.08.2023).

13. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) – URL: http://genproc.gov.ru (дата обращения: 20.08.2023).

14. Программы для удаленного доступа к компьютеру. − URL: https://lifehacker.ru/udalyonnyj-dostup-k-kompyuteru/ (дата обращения: 08.06.2023).

15. Руководство по реагированию на инциденты информационной безопасности. [Электронный ресурс]: – URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2017/08/ 12170645/Incident_Response_Guide_rus_2021.pdf. (дата обращения: 08.06.2023).

Учебное издание

Евгений Александрович Пидусов
Владимир Алексеевич Мещеряков
Александр Иванович Гайдин
Павел Геннадьевич Смагин
Михаил Михайлович Жуков
Александр Юрьевич Телков
Алексей Евгеньевич Васильев

ОСОБЕННОСТИ ПРОИЗВОДСТВА ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПУТЕМ КИБЕРАТАК (СЕТЕВЫХ АТАК)

Учебно-практическое пособие

В авторской редакции.

Компьютерный набор Е. А. Пидусова.
Объем 0,87 МБ.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53