МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ПРОГРАММИРОВАНИЯ

И.Н. ВАСИЛЬЕВА

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

ИЗДАТЕЛЬСТВО САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2019

ББК 32.81
В19

Васильева И.Н.

В19 Расследование инцидентов информационной безопасности : учебное пособие / И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с.

ISBN 978-5-7310-4814-9

Учебное пособие освещает теоретические основы и методические подходы к расследованию инцидентов информационной безопасности и правонарушений в компьютерной сфере. Рассмотрены международные стандарты, базовые принципы, организационные методы управления инцидентами безопасности, а также технические приемы и программно-аппаратные средства компьютерной криминалистики. Основной целью издания является формирование представлений о способах и средствах реагирования на нарушения информационной безопасности.

Предназначено для направления подготовки бакалавров 10.03.01 «Информационная безопасность», профиль безопасность компьютерных систем (в экономике и управлении).

Vasilyeva I.N.

Investigation of information security incidents : a manual / I.N. Vasilyeva. – Saint Petersburg : Publishing house of Saint Petersburg State University of Economics, 2019. – 113 p.

The manual covers the theoretical foundations and methodological approaches to the investigation of information security incidents and cybercrimes. International standards, basic principles, organizational methods of security incident management, as well as techniques and hardware and software of computer forensics are considered.

The manual is intended for bachelors of the direction of training 10.03.01 «Information security», profile «Security of computer systems (in economics and management)».

LBC 32.81

Рецензенты: канд. экон. наук **О.Д. Мердина**
канд. техн. наук **Г.М. Чернокнижный**

ISBN 978-5-7310-4814-9

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Учебное пособие разработано в соответствии с программой дисциплины «Расследование инцидентов информационной безопасности» для направления подготовки бакалавров 10.03.01 «Информационная безопасность», специализация: безопасность компьютерных систем (в экономике и управлении).

Целью освоения дисциплины «Расследование инцидентов информационной безопасности» является получение необходимых знаний по основным принципам и методам, применяемым при расследованиях инцидентов нарушений информационной безопасности (ИБ) в общей структуре процессов управления безопасностью, а также основных аспектов практической деятельности команды по расследованию инцидентов.

Изучение дисциплины призвано решить следующие задачи:

- приобретение знаний в области ИБ в части правового обоснования, принципов и этапов проведения расследования фактов ее нарушения;
- формирование владения основными нормативно-методическими документами (стандартами) в области управления инцидентами ИБ и организации деятельности команды по расследованию инцидентов;
- ознакомление с порядком действий сотрудников организации в случае инцидента ИБ;
- получение базовых знаний об источниках информации об инцидентах ИБ, методах и средствах сбора и анализа свидетельств инцидента ИБ;
- формирование навыков владения профессиональной терминологией в сфере управления инцидентами ИБ.

Пособие освещает все темы дисциплины «Расследование инцидентов информационной безопасности» и может быть использовано обучающимися в качестве дополнения к занятиям лекционного типа для освоения теоретического материала, а также служить основой для самостоятельной работы по дисциплине.

ГЛАВА 1. ПРАВОВАЯ БАЗА РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРАВОНАРУШЕНИЙ И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятия компьютерного преступления и инцидента информационной безопасности

Понятия компьютерного правонарушения (преступления) и инцидента ИБ различаются, однако, подходы к их расследованию, применяемые методики и сопутствующие процедуры и методы криминалистического исследования компьютерных систем во многом схожи. На бытовом уровне данные понятия обычно объединяются термином «компьютерная преступность» (computer crime) или «киберпреступность» (cyber crime). Этот термин может трактоваться в более широком или более узком смысле. Например, одно общепринятое определение описывает киберпреступность как любое деяние, в котором *инструментом*, *целью* или *местом* преступных действий являются компьютерные системы.

В России первая попытка криминализации компьютерных преступлений была предпринята в 1994 году, когда был разработан проект внесения изменений и дополнений в действующий УК РСФСР, состоящий из 6 статей. Однако до их пор в отечественной юридической науке нет однозначного мнения, что следует понимать под термином «компьютерные преступления».

Российское законодательство не использует понятие «компьютерные преступления», в УК РФ введена глава 28 «Преступления в сфере компьютерной информации» (ст. 272, 273 и 274 УК РФ). При этом применен традиционный подход отграничения деяний от смежных составов по *объекту* преступных посягательств. Главным признаком данной категории является не сам компьютер как орудие преступления, а информационные отношения. Глава 28 УК РФ помещена в раздел IX «Преступления против общественной безопасности и общественного порядка». Тем самым законодатель определил их родовой объект – общественные отношения, регулирующие общественную безопасность и общественный порядок. Действительно, хотя информация и имеет конкретного обладателя, ущерб от компьютерных посягательств затрагивает, как правило, интересы неограниченного круга лиц, то есть общество.

Преступление в сфере компьютерной информации можно определить, как запрещенное УК РФ под угрозой наказания виновно совершенное общественно опасное деяние, посягающее на общественные отношения, связанные с правомерным и безопасным использованием охраняемой законом компьютерной информации [11].

Глава 28 УК РФ включает следующие 4 состава преступлений:

- ст. 272 Неправомерный доступ к компьютерной информации;
- ст. 273 создание, использование и распространение вредоносных компьютерных программ;
- ст. 274 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- ст. 274.1 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (КИИ РФ).

УК РФ статья 272. *Неправомерный доступ к компьютерной информации* – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Ч. 1 ст. 272 УК РФ использует формулировку «охраняемая законом компьютерная информация», что требует, чтобы компьютерная информация охранялась нормативным актом рангом не ниже федерального закона. Вместе с тем, круг таких законодательных актов достаточно широк. Это Конституция РФ, Уголовный, Гражданский, Налоговый, Трудовой кодексы РФ, Кодекс РФ об административных правонарушениях, Законы РФ: от 21.07.1993 № 5485-1 «О государственной тайне», от 27.12.1991 № 2124-1 «О средствах массовой информации», Федеральные законы: от 29.07.2004 № 98-ФЗ «О коммерческой тайне», от 27.07.2006 № 152-ФЗ «О персональных данных», от 07.07.2003 № 126-ФЗ «О связи», от 06.04.2011 № 63-ФЗ «Об электронной подписи», от 13.03.2006 № 38-ФЗ «О рекламе», от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», от 02.12.1990 № 395-1 «О банках и банковской деятельности» и др.

При этом информация может защищаться не только от несанкционированного ознакомления (сведения, составляющие государственную тайну, или иная конфиденциальная информация), но и от искажения или изменения ее содержания или реквизитов. Кроме того, может быть ограничен оборот информации как вредной (например, призывающая к насилию, разжигающая социальную, расовую или религиозную рознь, содержащая порнографические материалы и т.п.).

Различные виды информации ограниченного доступа и соответствующие им федеральные законы доступны в справочной информации системы Консультант Плюс «Перечень нормативных актов, относящих сведения к категории ограниченного доступа» (http://www.consultant.ru/document/cons_doc_LAW_93980/#dst0).

Согласно определениям ФСТЭК России [1], **доступ к информации** – возможность получения информации и ее использования. Стандарт ФСБ

России СТО.ФСБ.КК 1–2018 «Компьютерная экспертиза. Термины и определения» [14] определяет **доступ к компьютерной информации** как ознакомление и (или) обработка компьютерной информации. При этом под *обработкой компьютерной информации* понимаются операции сбора, накопления (хранения), ввода, вывода, приема, передачи, записи, регистрации, уничтожения, преобразования (модификации) и отображения компьютерной информации как по отдельности, так и в совокупности.

Юридическое понятие «неправомерный доступ» является эквивалентом технического термина «несанкционированный доступ», а «неправомерные воздействия» − «несанкционированные действия». Согласно определениям ФСТЭК России, **несанкционированный доступ** (**несанкционированные действия**) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы (ИС) или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам. Под **правилами разграничения доступа** понимается совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Таким образом, доступ к компьютерной информации будет считаться неправомерным, если:

- лицо не имеет права на доступ к данной информации;
- лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты.

  В последнем случае лицо использует свое служебное положение.

Следует отметить отсутствие в нормах УК РФ указания на такую операцию, как «ознакомление с компьютерной информацией». Однако в ряде случаев нарушителю достаточно увидеть и прочитать информацию (например, пароль учетной записи), чтобы в дальнейшем воспользоваться ею безо всякого копирования. В случае, если информация обладает действительной или потенциальной ценностью в силу неизвестности ее третьим лицам (например, коммерческая тайна), несанкционированное ознакомление может привести к потере ценности такой информации.

УК РФ статья 273. *Создание, использование и распространение вредоносных компьютерных программ* – создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения (ст. 1261 ГК РФ).

Вредоносность или полезность компьютерных программ определяется не их способностью уничтожать, блокировать, модифицировать или копировать информацию (что является типичными функциями компьютерных программ), а наличием следующих признаков:

1) несанкционированная работа программы, что подразумевает выполнения хотя бы одного из двух следующих условий:

- отсутствие предварительного уведомления собственника (добросовестного владельца, пользователя) компьютерной информации о характере действий программы;
- отсутствие получение согласия (санкции) собственника (добросовестного владельца, пользователя) компьютерной информации на выполнение таких действий;

2) результатом работы компьютерной программы является уничтожение, блокирование, модификация или копирование информации либо нейтрализация средств защиты компьютерной информации. Если программа не производит ни одно из вышеперечисленных действий, то ее нельзя считать вредоносной;

3) заведомая предназначенность компьютерной программы для несанкционированного выполнения перечисленных в диспозиции ст. 273 УК РФ действий.

Стандарт ФСБ России СТО.ФСБ.КК 1–2018 определяет **вредоносное программное обеспечение** как компьютерную программу, предназначенную для нанесения вреда (ущерба) владельцу (пользователю) компьютерной информации, хранящейся на средствах вычислительной техники (СВТ), путем ее несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на СВТ средств защиты, или для получения доступа к вычислительным ресурсам самого СВТ с целью их несанкционированного использования.

Несанкционированное уничтожение, блокирование, модификация или копирование информации либо нейтрализация средств защиты компьютерной информации, даже если они повлекли тяжкие последствия, но произошли из-за непредвиденных результатов действия программы либо ошибки разработчика или пользователя не должны квалифицироваться по ст. 273 УК РФ. Однако в подобных деяниях могут содержаться составы других преступлений, например, нарушение правил эксплуатации средств

хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), халатности (ст. 293 УК РФ) и др.

УК РФ Статья 274. *Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей* – нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей (ИТС) и оконечного оборудования, а также правил доступа к ИТС, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Статья 274 УК РФ является наиболее сложной для практического применения. Трудности вызваны как конструкцией статьи, так и отсутствием в законе определения используемых терминов, что приводит к проблемам квалификации конкретных деяний. Так, нет четкого определения, что понимается в законе под средствами хранения, обработки или передачи компьютерной информации, а также что считать их эксплуатацией.

Кроме того, она является бланкетной, то есть содержит отсылку к нормам, непосредственно не определенным в законе (конкретным инструкциям и правилам работы со средствами хранения, обработки или передачи компьютерной информации и ИТС). Такие инструкции и правила могут утверждаться подзаконными нормативными актами (федеральными, ведомственными, корпоративными, актами самой организации). В качестве примера можно привести Постановление Правительства РФ от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи». Сложности практического применения данной статьи демонстрирует и статистика МВД РФ.

УК РФ Статья 274.1. *Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации* (введена Федеральным законом от 26.07.2017 № 194-ФЗ):

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или ИС, ИТС, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, ИС, ИТС, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ.

26 июля 2017 года принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», согласно которому под **критической информационной инфраструктурой** понимаются объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. В свою очередь, **объекты КИИ** – это ИС, ИТС, автоматизированные системы управления субъектов КИИ. К последним относятся государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТС, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В настоящее время проводится категорирование объектов КИИ, исходя из их социальной, политической, экономической, экологической значимости и значимости для обеспечения обороны страны, безопасности государства и правопорядка, а также создание реестра значимых объектов КИИ.

Закон «О безопасности КИИ РФ» определяет и понятие **компьютерного инцидента** – это факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Таким образом, инцидент является фактом относительно состояния работоспособности информационных систем, сетей или систем защиты информации, который не обязательно является следствием противоправных деяний (либо рассматривается безотносительно квалификации таких деяний по статьям УК РФ).

Кроме того, закон утверждает наличие государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Такая система

представляет собой единый территориально распределенный комплекс, получивший название ГосСОПКА, создание которого ведется под управлением ФСБ России с 2013 года. Соответствующие изменения были внесены и в уголовное законодательство России (ст. 274.1 УК РФ).

В отечественной теории уголовного права нет единого подхода к определению терминов, используемых при квалификации компьютерных преступлений. Это относится, в частности, к базовым понятиям «компьютер», «компьютерная информация» и «информационная безопасность».

В настоящее время дать юридически значимое определение термина «компьютер» не представляется возможным в силу сложности в его уяснении, что послужило одной из причин исключения термина «ЭВМ» (как синонима термина «компьютер») из УК РФ. Поэтому при решении вопроса об отнесении устройства к компьютерным руководствуются существующей правоприменительной практикой (например, если речь идет о ноутбуке, персональном компьютере), а в сложных случаях (например, в отношении игровых автоматов, контрольно-кассовых машин, сотовых телефонов и т.п.) опираются на заключение компьютерно-технической экспертизы.

Согласно примечанию к ст. 272 УК РФ, под *компьютерной информацией* понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Многими авторами данное определение подвергается критике как по причине сложности в уяснении термина «электрический сигнал», так и по причине того, что с помощью электрических сигналов возможна передача информации, не предназначенной для обработки СВТ, то есть не являющейся компьютерной. С другой стороны, компьютерная информация может представляться не только в форме электрических сигналов (например, записанная на оптических дисках).

С другой стороны, с развитием информационных технологий грань между специальными «машинными» формами представления информации и «обычной» информацией постепенно стирается. Компьютерная техника может воспринимать и обрабатывать информацию, представленную в традиционном виде – графическом (рукописный текст, фото, видео), голосовом (голосовой ввод, голосовые команды). Это касается и носителей информации («носители компьютерной информации» или «машинные носители» или «традиционные носители» информации). Так, информация с листа бумаги или с компакт-диска одинаково легко вводится в компьютер, разница заключается лишь в используемых технических устройствах ввода (в первом случае – это сканер, во втором – CD/DVD привод).

Стандарт ФСБ России СТО.ФСБ.КК 1–2018 вводит следующие определения.

Средство вычислительной техники – совокупность программных и технических элементов систем обработки компьютерной информации, способных функционировать самостоятельно или в составе других систем.

Это определение фактически повторяет аналогичное определение ГОСТ Р 57429–2017 «Судебная компьютерно-техническая экспертиза. Термины и определения» [5].

Вычислительная машина (**компьютер**) – СВТ, выполняющее некоторые функции без участия человека и функционирующее по заданной программе.

Электронно-вычислительная машина – вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах.

Компьютерная информация – информация, представленная в форме, пригодной для обработки на вычислительной машине, независимо от средств ее хранения, обработки и передачи.

Здесь основным классифицирующим признаком является то, предназначена ли информация специально для обработки с помощью компьютерных систем или нет.

В настоящее время компьютерная информация может содержаться не только в компьютерах, но также и в мобильных телефонах, банкоматах, платежных терминалах и др. Поэтому зачастую рассматривается более широкая группа преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, которые зачастую называют *преступлениями в сфере высоких технологий* (компьютерными преступлениями, киберпреступлениями).

Наиболее близким к главе 28 УК РФ является *мошенничество в сфере компьютерной информации* – ст. 159.6 УК РФ. С точки зрения криминалистической методики расследования они во многом схожи, поскольку до 2012 (когда была введена ст. 159.6) деяния, предусмотренные ст. 159.6 УК РФ, квалифицировались по совокупности статей 159 и 272 (а иногда еще и 273) УК РФ. Иные деяния, совершенные с использованием компьютерных и телекоммуникационных технологий, обычно квалифицируются по следующим статьям УК РФ:

- ст. 146 Нарушение авторских и смежных прав,
- ст. 165 Причинение имущественного ущерба путем обмана или злоупотребления доверием,
- ст. 171 Незаконное предпринимательство,
- ст. 183 Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну и др.

Отдельно следует отметить составы преступлений, в качестве квалифицирующего признака называющие использование ИТС (включая сеть Интернет):

- ст. 137 Нарушение неприкосновенности частной жизни,
- ст. 171.2 Незаконные организация и проведение азартных игр,
- ст. 185.3 Манипулирование рынком,
- ч. 2 ст. 228.1 Сбыт наркотических средств, психотропных веществ или их аналогов,
- ст. 242 Незаконные изготовление и оборот порнографических материалов и предметов, ст. 242.1 Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, ст. 242.2 Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов,
- ст. 280 Публичные призывы к осуществлению экстремистской деятельности, ст. 280.1 Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации,
- ст. 282 Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства,

ст. 187 Неправомерный оборот средств платежей и ст. 159.3 Мошенничество с использованием электронных средств платежа.

К преступлениям в сфере высоких технологий относят и незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ), а также нарушение с их помощью неприкосновенности частной жизни (ст. 137 УК РФ), либо тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ). Однако методика расследования этих преступлений существенно отличается от таковой для компьютерных преступлений.

Кроме того, существуют ряд содержащих компьютерный аспект правонарушений, предусматривающих не уголовную, а административную или дисциплинарную ответственность в рамках КоАП РФ и ТК РФ соответственно (например, нарушение правил защиты информации или разглашение информации с ограниченным доступом). Поэтому в дальнейшем будем использовать термин «компьютерные правонарушения» (правонарушения в компьютерной сфере/ в сфере высоких технологий).

Что касается понятия информационной безопасности, то в российском уголовном законодательстве определение данного понятия отсутствует. Однако ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» вводит понятие безопасности информации (данных) как состояния защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [6] определяет **информационную безопасность** (information security) как сохранение конфиденциальности, целостности и доступности информации.

Стандарты ГОСТ Р ИСО/МЭК 27000–2012 и ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [7] приводят определения *инцидента информационной безопасности*, согласованные с ГОСТ Р 18044 ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» [10]. **Инцидент информационной безопасности** (information security incident) понимается как появление одного или нескольких нежелательных или неожиданных событий ИБ, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для ИБ.

1.2. Классификация правонарушений в компьютерной сфере

В основу классификации компьютерных правонарушений может быть положено разделение в соответствии с местом компьютерной информации и информационных технологий (ИТ) в механизме совершения правонарушения:

- компьютерная информация и ИС являются *объектом* (предметом) преступного посягательства, например, хищение информации или нанесение урона ИС;
- ИТ используются в качестве *орудий* (средства) совершения правонарушений и электронных атак;
- ИТ, ИС и ИТС являются *средой*, которая содержит объекты преступных посягательств (например, запоминающие устройства, к которым осуществляется несанкционированный доступ).

Необходимость разработки эффективных методик расследования правонарушений в компьютерной сфере требует учета *криминалистических оснований* и, в первую очередь, *способа* совершения правонарушения. Криминалистическая классификация является основой не только криминалистической характеристики, но и может служить для построения системы частных криминалистических методик расследования правонарушений. В этом смысле классификации по способу совершения правонарушения представляют наибольший практический интерес, хотя по мне-

нию многих авторов, в этом случае неизбежно происходит смешение уголовно-правовых понятий и технических особенностей реализации компьютерных систем.

Классификации, в основу которых был положен способ совершения компьютерных преступлений, были разработаны европейскими странами еще в 80-90-х годах XX века (например, кодификатор Интерпола). Более развернутую классификацию компьютерных преступлений предлагает Конвенция Совета Европы о преступности в киберпространстве, принятая 23 ноября 2001 года в Будапеште (Будапештская Конвенция), являющаяся основополагающим международным документом в сфере борьбы с киберпреступностью. На сегодняшний день Конвенцию подписали 46 стран, включая 4 страны, которые не являются членами совета Европы. Российская Федерация не присоединилась к участию в Конвенции из-за положений п. «b» ст. 32, согласно которому любая из договаривающихся сторон может без согласия другой стороны получать через компьютерные системы, находящиеся на своей территории, доступ к хранящимся на территории другой страны ресурсам. Похожей классификации правонарушений в компьютерной сфере придерживается Международный союз электросвязи (ITU), однако его классификация несколько шире.

1. **Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем**.

- *Несанкционированный доступ* к компьютерным системам (путем взлома, обмана и другими средствами).
- *Незаконное получение данных* (информационный шпионаж).
- *Незаконный перехват*.
- *Искажение информации*.
- *Искажения системы*.

К этой группе относятся вирусные заражения, атаки типа «отказ в обслуживании» (DoS, DDoS).

2. **Преступления, связанные с контентом**.

К этой категории относится распространение контента (информационных материалов), противоречащих законодательству. Распространение материалов через Интернет дает правонарушителям ряд преимуществ, включая малую стоимость распространения, отсутствие специального оборудования и глобальную аудиторию. Правовая оценка контента и законодательство сильно зависит от национальных особенностей, которые учитывают фундаментальные культурные и правовые принципы и могут существенно различаться.

Одним из методов обеспечения ограничения на распространение контента, считающегося незаконным, является создание систем фильтрации и блокирование сайтов. В России блокирование доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов осуществля-

ется операторами связи и хостинг-провайдерами на основании реестра, поддерживаемого Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором).

В Российской Федерации, согласно ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» запрещено распространение материалов с детской порнографией, информации об изготовлении и использовании наркотических средств, способах совершения самоубийства, информации о детях, пострадавших от противоправных действий, предложения о розничной продаже дистанционным способом алкогольной продукции и др. Также запрещено распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность (п. 6 ст. 10 Федерального закона «Об информации, информационных технологиях и о защите информации»). Не допускается использование СМИ в целях совершения уголовно наказуемых деяний (ст. 4 Закона Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации»).

Кроме того, блокируется информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности и др. (ст. 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации»).

- *Эротические или порнографические материалы*.
- *Детская порнография*.
- *Расизм, агрессивные высказывания, подстрекательство к насилию, пропаганда жестокости*.
- *Религиозные преступления*.
- *Незаконные азартные игры и онлайн-игры*.
- *Клевета и фальшивая информация*.
- *Спам* и связанные с ним угрозы.

Спам означает передачу незапрашиваемых сообщений. Наиболее широко используемым является спам в электронных письмах, которые могут, наряду с рекламой содержать вирусные вложения или фишинговые ссылки. Например, по данным Лаборатории Касперского, доля спама в российском интернет-трафике в 2018 году составила 53 процента (общемировые показатели − около 50 процентов).

Поставщики услуг электронной почты реагируют на растущие уровни спама применением фильтрации по ключевым словам и ведением «черных списков» IP и почтовых адресов спамеров. Обнаружение спама затрудняет использование правонарушителями сетевых роботов и зомби-сетей.

- *Вымогательство*.

Вымогательство считается обычным правонарушением, однако последнее время широко распространено вредоносное ПО, блокирующее доступ к компьютерной системе и предлагающие ее разблокировку после выплаты выкупа. При этом правонарушители могут использовать технологии анонимной связи, а также оплату с использованием виртуальных кошельков или криптовалют, что затрудняет их обнаружение.

- *Другие формы незаконного контента*.

Интернет широко используется правонарушителями не только для прямых атак, но и как площадка для подстрекательства, предложений и побуждения к совершению преступлений, незаконной продажи товаров и распространения информации и инструкций по выполнению незаконных действий (например, по изготовлению взрывных устройств и другого оружия).

3. **Преступления, связанные с правами собственности и товарными знаками**.

Компании, распространяющие продукцию через Интернет, могут столкнуться с правовыми проблемами, связанными с нарушениями авторских прав. Кроме того, актуальны проблемы пиратства для продукции, которая может быть представлена в цифровом виде (например, аудиовизуальная продукция, книги) и распространения поддельных продуктов, когда производители контрафакта копируют как логотипы, так и сами продукты успешных брендов и пытаются зарегистрировать домен, связанный с определенной компанией.

- Преступления, *связанные с нарушением авторских и смежных прав*.

Основой существующих нарушений авторских и смежных прав является возможность быстрого и точного воспроизведения цифрового произведения (компьютерных программ, аудио/видео и других видов цифровой продукции, а также баз данных и книг). До оцифровки копирование аудио и видеокассет приводило к некоторому снижению качества. В настоящее время можно скопировать цифровую продукцию без потери качества, а также делать копии с любой копии. Чаще всего встречаются правонарушения, заключающиеся в размещении нелегальных копий цифровых произведений в файлообменных сетях, а также обход систем управления цифровыми правами DRM (digital restrictions management).

- Преступления, *связанные с товарными знаками*.

Эта группа преступлений похожа на нарушения авторских и смежных прав, кроме того, товарные знаки могут использоваться для введения пользователей в заблуждение (например, в фишинговых схемах). К этому виду преступлений относится и незаконная регистрация доменных имен, идентичных или похожих на товарные знаки известной продукции или компании (киберсквотинг). Другим примером является «угон» домена или регистрация доменных имен, которые были случайно утеряны. Целью подобных действий может быть последующая перепродажа домена по завышенной цене владельцу торгового знака или использование его для продажи товаров и услуг, вводя в заблуждение пользователей за счет их предполагаемого отношения к данному товарному знаку.

4. **Преступления, связанные с применением компьютерной техники**.

В эту категорию входят преступления, средой для совершения которых является компьютерная система: связанные с применением компьютерных систем мошенничество или подлог, фишинг и кража личных данных, а также неправомерное использование компьютерных устройств.

- *Компьютерное мошенничество*.

Большинство систем уголовного права рассматривают такие правонарушения не как преступления, связанные с применением компьютеров, а как обычное мошенничество. К наиболее распространенным мошенническим действиям относятся:

- мошенничество с онлайн-аукционами: выставление на продажу несуществующих товаров, а также покупка товаров без намерения их оплаты, в том числе и с использованием счетов третьих лиц («угон» аккаунтов, «захват» счетов);
- мошенничество с предоплатой: обещание значительных бонусов (выигрыша, социальной помощи и т.п.) и просьба о предварительном переводе небольшой денежной суммы за оформление или под другим предлогом; при разглашении реквизитов банковского счета, они затем могут использоваться мошенниками для других правонарушений.

Последовательность осуществления мошеннической комбинации в сети Интернет, как правило, можно разделить на две стадии:

1. передача или навязывание ложной информации потерпевшим с целью введения их в заблуждение;
2. непосредственное завладение предметом посягательства.

Наиболее распространенными способами передачи ложной информации являются мошеннические сайты и электронная почта. Однако мошенники могут использовать мессенджеры, форумы или чаты. Веб сайт, как правило, регистрируется на бесплатном хостинге, чтобы соблюсти анонимность. Однако мошенники могут разместить сайт и на серверах хостинг-компаний, представляющих платные услуги.

Непосредственное завладение предметом посягательства может осуществляться путем ввода регистрационных данных кредитных карт, переводом средств на «электронные кошельки», номера сотовых телефонов и т.п. Перевод электронных денег (WebMoney, Яндекс деньги) наиболее характерен для схем с предоплатой (сотовое мошенничество, предложение несуществующих товаров). В отличие от традиционного мошенничества, характерной особенностью интернет-мошенничества является то обстоятельство, что при нем остается мало традиционных следов и потерпевшие не знают преступников в лицо.

- *Подлог*, совершенный с применением компьютеров.

Фальсификация электронных писем или цифровых документов (создание документа с имитацией электронного бланка организации, изменение текста подлинного документа, подделка цифровой подписи или использование «чужой» легальной цифровой подписи, подделка цифровых изображений и видео).

- *Кража идентичности*.

Понятие кражи идентичности не имеет четкого определения и четкого использования, под ним подразумевается преступное деяние по мошенническому получению и использованию «чужой» личности (персональных данных). В целом преступления этого типа проходят три различных этапа.

1. Преступник добывает информацию об идентичности с помощью вредоносного ПО, фишинг-атак, кражи носителей компьютерной информации или другими способами (например, с помощью поиска и анализа данных социальных сетей). Кроме того, чтобы убедить жертву раскрыть личную информацию, широко применяются методы социальной инженерии.

2. Второй этап характеризуется взаимодействием с персональными данными до их непосредственного использования, например, продажа информации об идентичности. Можно констатировать рост объема «черного» рынка информации, имеющей отношение к идентичности. Значительная часть персональных данных, скомпрометированных вследствие крупных утечек, впоследствии оказывается в продаже.

3. Использование информации об идентичности при совершении преступления, например, для подделки документов, удостоверяющих личность, или мошенничества с кредитными картами.

- *Злоупотребление устройствами*.

К этой группе правонарушений относится изготовление, продажа, приобретение для использования, распространения или предоставление для использования иным образом устройств, компьютерных программ, компьютерных паролей или кодов доступа с целью осуществления правонарушений. В криминальной части сети Интернет широко представлены

автоматизированные инструменты для проведения спам-рассылок, DoS атак, создания компьютерных вирусов, дешифрации зашифрованных сообщений или получения несанкционированного доступа к компьютерным системам. При этом интерфейсы многих таких программ почти не отличаются от офисных приложений и интуитивны для освоения, а внедрение вредоносного ПО осуществляется в автоматическом режиме, когда преступнику достаточно запустить программу и ждать результатов.

В настоящее время все большее развитие получает рынок аренды вредоносного ПО. Создание или модификация таких программ под специальные задачи, обозначенные заказчиком, является одним из видов такого широко распространенного явления, как «преступление как услуга». За определенную плату можно заказать совершение DDoS атаки на указанные серверы, или получить ботнет для осуществления тех же целей. Поэтому различные национальные законодательства предусматривают преследование в судебном порядке также и обладание такими инструментами.

5. **Комбинированные преступления**.

К этой группе относятся сложные преступные деяния, сочетающие в себе ряд различных правонарушений. Например, использование сети Интернет в террористических целях (кибертерроризм), отмывание денег с использованием компьютерных технологий и фишинг.

Созданная на основе сети Интернет и других сетевых ИТ трансграничная инфраструктура поставок товаров, оказания услуг, перевода средств между физическими и юридическими лицами, хранения информации и подключение к ней каждого компьютера, предоставляет широкие возможности как собственно для совершенствования компьютерных преступлений, так и для отмывания полученных денег с помощью компьютерных технологий. При этом возможности правонарушителей характеризуются следующими качествами сети Интернет, как среды совершения преступных деяний:

- скорость и невысокая стоимость преступления;
- высокая технологичность;
- сложный характер;
- анонимность;
- транснациональный характер;
- доступность широкому кругу лиц (популярность);
- организованный характер и смешанный состав участников.

Наиболее сложные уголовные дела обычно связаны с крупными преступными группами, которые занимаются целевыми атаками (APT), кражами денег через интернет-банк или мобильные приложения финансовых организаций. Злоумышленники в этих случаях уделяют большое внимание скрытности своей личности − используют несколько цепочек серверов

для доступа к ресурсам, применяют шифрование, постоянно модифицируют программные средства, используемые для атак. К сожалению, зачастую по единственному инциденту установить злоумышленников не удается. Только по нескольким эпизодам набирается материал, с которым можно работать, но даже тогда процесс поиска может затянуться.

Другую сложность представляет то, что в таких преступных группах, как правило, роли четко распределены и дробятся, поэтому правонарушение от начала до конца совершается разными людьми. Лидер группы нанимает исполнителей для выполнения определенных задач, при этом некоторые из них могут даже не подозревать, что участвуют в преступной деятельности.

- *Использование сети Интернет в террористических целях*.

Террористические группировки могут использовать компьютерные технологии, и в частности сеть Интернет, для:

- пропаганды;
- сбора информации;
- подготовки нападений в реальном мире;
- публикации обучающих материалов;
- координации и связи;
- финансирования террористических операций и групп;
- атак на объекты КИИ.

- *Кибервойны*.

Термин «кибервойна» зачастую используется для обозначения массированных атак на компьютерные системы какой-либо страны. Однако в настоящее время нет унифицированной терминологии, равно как и общепринятого определения этого понятия. В узком смысле кибервойна – это управление и использование информации всех видов и на всех уровнях для достижения явного военного преимущества, особенно в ходе объединенных и совместных военных действий. В этом смысле кибервойна не может вестись в мирное время, поэтому можно говорить лишь о кибероперациях. Более широкие толкования термина подразумевают любой электронный конфликт, в котором информация выступает как стратегическое средство, подлежащее захвату или уничтожению.

Вместе с тем, следует четко разливать понятия киберпреступления и кибервойны, поскольку если компьютерные преступления регулируются национальным законодательством, то правила и регламент относительно военных действий регулируются преимущественно нормами международного права, в частности Уставом Организации Объединенных Наций.

- *Отмывание денег с использованием компьютерных технологий*.

Распространение онлайновые финансовых услуг и электронных денег (виртуальных валют, криптовалют) дает возможность быстрого вы-

полнения многочисленных финансовых операций по всему миру и позволяет обойти жесткие ограничения и проверки, характерные для банковских безналичных расчетов. При этом выявление подозрительных сделок в области борьбы с отмыванием денег основано на обязательствах финансовых учреждений, принимающих участие в сделке.

Отмывание денег в целом подразделяется на три стадии:

1. размещение наличных средств,
2. расслоение (разбивка крупных сумм денег на более мелкие);
3. суммирование.

Интернет-сервисы особенно востребованы правонарушителями на стадии расслоения или маскировки. Особую сложность представляют расследования преступлений, когда для расслоения денежной суммы используются онлайн-казино и виртуальные валюты.

- *Фишинг*.

Цели фишинга не ограничиваются только получением паролей для проведения банковских онлайн-операций, злоумышленников могут интересовать коды доступа к компьютерам, аукционным площадкам и персональные данные, что может привести к преступлениям типа «кража идентичности». Традиционная схема фишинговой атаки включает следующие этапы.

1. На первом этапе определяются компании, предлагающие онлайн-услуги и взаимодействующие с клиентами в электронном виде, например, финансовые институты.

2. Далее правонарушители создают подложные веб сайты (фишинговые сайты), внешне напоминающие законные сайты, где от жертвы требуется выполнить обычные процедуры входа, что позволяет правонарушителям получить личную информацию, например, номера счетов и онлайновые банковские пароли.

3. Чтобы направить пользователей на подложные сайты, как правило, используются почтовые рассылки, при этом письмо уже содержит готовую ссылку, по которой жертва должна перейти на обманный сайт. Это позволяет избежать ручного ввода пользователями правильного адреса. Существуют и другие схемы фишинговых атак [13].

Как только личная информация раскрыта, правонарушители входят в учетные записи жертв и совершают преступления, такие как перевод денежных средств, заявки на паспорта или новые счета и т.д.

Отечественные исследователи относят к комбинированным преступлениям и правонарушения, *связанные с использованием электронных банковских карт*, при этом последние рассматриваются как средства компьютерной техники [11].

1.3. Криминалистическая характеристика правонарушений в компьютерной сфере

Криминалистическая характеристика – это система типичных признаков преступления того или иного вида. Криминалистическая характеристика формализует опыт и формирует систему знаний о типичном правонарушении, поэтому она полезна при рассмотрении сходных преступных деяний в рамках одного состава или даже каждого из видов правонарушений в рамках одного состава.

Наиболее значимыми криминалистическими сведениями являются:

- предмет преступного посягательства,
- личность правонарушителя,
- мотивы и цели преступного поведения,
- типичные способы подготовки, совершения и сокрытия преступления,
- время, место и обстановка преступных посягательств,
- механизм следообразования.

Криминалистическая характеристика правонарушений в компьютерной сфере обладает определенной спецификой, а именно: *техническая составляющая данного вида правонарушений – одна из главных*. Компьютерные преступления характеризуются *высокой латентностью*, это значит, что официально регистрируется лишь незначительная часть таких преступлений, а раскрывается, то есть доводится до суда – еще меньше. По мнению специалистов, от 70 до 90 процентов компьютерных преступлений остаются за пределами уголовных учетов. При этом статистические распределения для криминалистических характеристик (например, характеристики личности преступника) рассчитываются только по данным раскрытых преступлений. Поэтому приводимая в литературе статистика по криминалистическим характеристикам достаточно условна. Статистические данные свидетельствуют о неуклонном росте числа регистрируемых преступлений в сфере высоких технологий (табл. 1).

В настоящее время в РФ наиболее распространенными преступными деяниями в компьютерной сфере являются:

- правонарушения, связанные с интернет-торговлей, обслуживанием кредитных карт и дистанционным банковским обслуживанием (ДБО), в том числе с применением мобильных средств связи;
- вымогательство;
- правонарушения в сфере игорного бизнеса;
- пиратство в отношении цифрового контента и программного обеспечения;

- кибернаемничество, а также организация распространения проституции, нелегальной миграции, порнографии, незаконного оборота наркотиков и оружия.

Таблица 1. Статистика преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий

Всего	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
зарегистрировано	**10227**	**11104**	**10968**	**43816**	**65949**	**90587**	**174674**
раскрыто						20424	43362
в т.ч. гл. 28 УК РФ	**2820**	**2563**	**1734**	**2378**	**2570**	**1883**	
ст. 272 УК РФ	1930	1799	1150	1395	1443	1079	
ст. 273 УК РФ	889	764	583	970	1124	802	
ст. 274 УК РФ	1	0	1	13	3	2	
ст. 159.6		**693**	**993**	**5442**	**5380**	**2195**	

Предмет преступного посягательства. Предметом компьютерных правонарушений могут являться информационные ресурсы (собственно компьютерная информация и ИС), а также деньги, либо иные материальные ценности и связанные с ними права. Вид информационных ресурсов зависит от мотивов и цели преступника. Это может быть охраняемая законом информация (различные виды тайн, персональные данные), сведения, имеющие повышенную материальную ценность (секреты производства, «ноу-хау», инсайдерская информация, реквизиты кредитных и платежных карт, объекты авторского права), сайты органов государственной власти, политических и общественных организаций, отдельных компаний, объекты КИИ. Предмет преступного посягательства нередко указывает на определенную категорию преступников. Например, производственные секреты интересны конкурентам, а клеветническая информация о политическом деятеле распространяется в интересах его оппонентов и т.д.

Характеристика личности правонарушителя. Подавляющее большинство преступников в компьютерной сфере (свыше 80%) – мужчины. Однако с распространением «женских» профессий, связанных с ИТ (бухгалтеры, кассиры, операторы) доля женщин увеличивается.

Значительная часть компьютерных правонарушений совершается лицами, деятельность которых связана с компьютерными или телекоммуникационными технологиями. При этом у более 50% преступников была специальная подготовка в области автоматизированной обработки информации, а 30% – были непосредственно связаны с эксплуатацией ЭВМ и разработкой программного обеспечения к ней. Однако, вопреки образу «хакера», нарисованного СМИ, правонарушители не всегда являются высококвалифицированными специалистами в ИТ сфере. Действительно, со-

вершение киберпреступлений (например, организация фишинговой рассылки) не всегда требует серьезных специальных познаний. Кроме того, развитие «черного рынка» вредоносного ПО, общедоступность инструментов и методов атак приводит к снижению требовательности к уровню специальных знаний атакующих. С другой стороны, проведение сложных атак практически невозможно осуществить в одиночку. Исследователями отмечается высокая степень организованности компьютерной преступности – по некоторым данным, до 60% компьютерных правонарушений совершается в составе организованных групп и сообществ. Как правило, они имеют отдельные структурные подразделения, обособленные по признаку преступной специализации: разработчики вредоносных программ; администраторы используемой для проведения атак сетевой инфраструктуры; операторы ботсетей зараженных компьютеров; группы, обеспечивающие вывод и обналичивание похищенных денежных средств.

Характерные мотивы и цели компьютерных правонарушений. Подавляющее большинство (по некоторым данным, до 70%) компьютерных правонарушений совершаются их корыстных побуждений: получение финансовой выгоды или материальных ценностей, услуг; получение конкурентных преимуществ, привилегий, льгот; уклонение от уплаты налогов, платежей и сборов; легализация преступных доходов. По данным статистики компании GroupIB (https://ict.moscow/research/hi-tech-crime-trends-2018/), объем хищений денежных средств с использованием компьютерных технологий за вторую половину 2017 – первую половину 2018 года составил около 3 млрд. руб., доля финансово мотивированных киберпреступников составляет 94%, 6% делят проправительственные группировки и хакеры, кибертеррористы и хактивисты[1].

Таким образом, кроме финансовых соображений, действующие в компьютерной сфере правонарушители, могут руководствоваться следующими мотивами:

- политические цели: терроризм, шпионаж, подрыв финансово-экономической и политической стабильности государства, разжигание расовой, межнациональной и религиозной розни и т.п.);
- исследовательский интерес и любопытство;
- хулиганские побуждения;
- месть (конкретным лицам или организациям);
- стремление к самоутверждению и получения признания в своем кругу, желание получить известность, продемонстрировать интеллектуальное превосходство;

[1] хакеры, действующие из идейных соображений, для продвижения политических идей, защиты свободы слова и прав человека, обеспечения свободы информации, участвующие в протестном движении, акциях гражданского неповиновения.

– стремление скрыть другое преступление или облегчить его совершение.

Пострадавшая сторона. В соответствии с ч.1 ст.42 УПК РФ потерпевшим является физическое лицо, которому причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения вреда его имуществу и деловой репутации. Однако преступление может нанести вред и другим лицам, не только прямой, но и косвенный. Поэтому правильнее говорить о потерпевшей стороне, охватывающей всех лиц, чьи права и законные интересы были нарушены. Потерпевшей стороной от правонарушений в компьютерной сфере может быть:

- обладатели (владельцы) информационных ресурсов;
- владельцы средств компьютерной техники и ИТС;
- лица, сведения о которых хранятся (обрабатываются) в ИС;
- лица, пользующиеся информационными ресурсами, компьютерной техникой и ИТС;
- прочие лица, правам и законным интересам которых причинен вред.

Способ и средства совершения правонарушения. В криминалистическом понимании наибольшее значение имеет способ совершения правонарушения, так как он, во-первых, характеризуется наибольшим объемом криминалистически значимой информации, а во-вторых, все остальные элементы криминалистической характеристики так или иначе с ним связаны. В криминалистическом смысле *способ совершения преступления* характеризуется как система действий по подготовке, совершению и сокрытию правонарушения, но также имеет внешнее проявление в виде следов и различных материальных объектов.

Способы совершения правонарушений в сфере компьютерной информации достаточно разнообразны, в определенной степени они отражаются приведенной ранее классификацией.

Рассмотрим, к примеру, жизненный цикл (последовательность этапов и шагов совершения)[2] сложных целевых атак (APT-атак, Advanced Persistent Threat − Постоянно совершенствуемая угроза), которые наиболее трудны в обнаружении. Под APT понимается сложная, продолжительная, хорошо спланированная многоходовая атака, в ходе которой для достижения цели используется целый комплекс инструментов – разнообразные виды вредоносного и легального ПО, методы и приемы социальной инженерии, а также данные об информационной инфраструктуре конкретного атакуемого объекта. Объектом таких атак, как правило, являются корпоративные сетевые ресурсы. Действия, которые предпринимают правонарушители для осуществления подобных атак, могут быть квалифици-

[2] В англоязычной литературе жизненный цикл атаки получил название kill chain (цепочка атаки).

рованы по совокупности по нескольким статьям УК РФ. Можно выделить следующие этапы развития атак:

1. Проникновение во внутреннюю корпоративную сеть. Осуществляется обычно с помощью целевой либо массированной спам-рассылки фишинговых писем, содержащих в качестве вложения специальным образом сформированный документ либо вредоносную ссылку на сторонний ресурс. Открытие данного документа либо переход по ссылке приводит к инфицированию системы вредоносной программой.

2. Разведка и реализация. На скомпрометированные компьютеры устанавливаются программы удаленного администрирования и управления, используя которые, преступники пытаются завладеть учетными данными администраторов систем. Широко используются легальные программы удаленного управления и администрирования, а также штатные средства операционных систем (такие как Power Shell и WMI), функциональность которых известна многим пользователям.

3. На заключительном этапе реализуются возможности несанкционированного доступа к сетевым компьютерам и сервисам, целью которого может быть:

- выполнение незаконных финансовых транзакций и хищение денежных средств;
- завладение персональными данными пользователей;
- формирование ботнета;
- перехват контроля над АСУ ТП;
- использование информации, скопированной со внутренних корпоративных ресурсов для осуществления целевых атак на клиентов или партнеров компании и т. д.

Специалисты «Лаборатории Касперского» выделяют семь основных шагов реализации APT.

1. Разведка и сбор данных (Reconnaissance) – идентификация и отбор целей на основании данных из открытых источников. На этом шаге осуществляется сбор информации об организации, которая будет атакована, и ее информационных активах, в частности, производится попытка установить:

- организационную структуру компании;
- используемый стек технологий;
- средства обеспечения ИБ;
- возможности использования методов социальной инженерии по отношению к сотрудникам (например, выявление их аккаунтов в социальных сетях).

Разведка может быть пассивной (Passive reconnaissance) и активной (Active reconnaissance). Пассивная разведка заключается в получении ин-

формации без непосредственного воздействия на атакуемую ИС (например, просмотр DNS и Whois информации, связанной с ИС организации). Активная разведка включает в себя взаимодействие с атакуемой ИС: сканирование портов, поиск уязвимостей и другие действия.

Вся собранная информация служит отправной точкой и источником знаний для реализации последующих шагов.

2. Выбор способа атаки (Weaponization). На основе полученной на первом шаге информации определяется способ атаки. При этом может создаться новое вредоносное ПО, позволяющее эксплуатировать обнаруженные уязвимости. Создаются объекты (документы, электронные письма или съемные носители), содержащие вредоносное ПО или ссылки, которые будут использоваться при атаке. На этом шаге также определяется способ доставки созданного вредоносного ПО в атакуемую организацию: с помощью заражения публичного ресурса компании, через одного из сотрудников или через компрометацию компаний-субподрядчиков, работающих с атакуемой организацией.

3. Доставка (Delivery). Обеспечение попадания разработанного вредоносного ПО в ИС атакуемой организации. Обычно для этого используются вложения электронной почты, вредоносные и фишинговые ссылки, заражения сайтов, которые часто посещают сотрудники атакуемой организации, или зараженные USB-устройства.

4. Эксплуатация (Exploitation). После попадания в ИС атакуемой организации вредоносное ПО, используя уязвимости, распространяется по сети и закрепляется на зараженных машинах в ожидании команд, поступающих от атакующего. Непосредственно на данном шаге, как правило, вредоносное ПО использует повышение привилегий для обхода систем защиты с целью получения дополнительных данных о системе и продвижения по сети организации в поисках целевой информации или системы.

5. Закрепление (Installation). Вредоносное ПО осуществляет заражение компьютеров для того, чтобы не быть обнаруженным или удаленным после перезагрузки или установки обновления, блокирующего возможности использования определенных уязвимостей ИС. Обычно для заражения используются утилиты несанкционированного управления (backdoor), кейлоггеры и reverse shell[3] подключения для получения удаленного контроля над системой.

6. Исполнение команд (Command and Control). С помощью соединения, устанавливаемого изнутри ИС атакованной организации, вредоносное ПО реализует взаимодействие с сервером управления (C&C сервер),

---

[3] Reverse shell – тип подключения, в которой целевая машина жертвы связывается с атакующей машиной. В данном случае компьютер злоумышленника выступает в роли сервера и открывает порт связи на прослушивание, ожидая входящего соединения.

подконтрольным атакующему. Таким образом, атакующий получает управление компьютерами внутри ИС атакуемой организации. Команды от атакующего могут поступать как через Интернет (от командных центров C&C), так и с помощью доставки другого вредоносного ПО (например, если на машине отсутствует прямое подключение к Интернету).

7. Достижение цели (Actions on Objective). Получив управление, атакующий может работать с данными на скомпрометированном компьютере, не только осуществляя несанкционированный доступ, но и изменяя или удаляя их. Кроме того, атакующий может попытаться заразить другие машины в ИС, для того чтобы увеличить объем доступной информации.

От того, на каком шаге была обнаружена угроза, зависит эффективность расследования, а также размер материального и репутационного ущерба, нанесенного атакуемой организации. Позднее обнаружение (на этапе достижения цели) означает, что система защиты оказалась неспособной противостоять атаке, и нарушитель достиг своих целей. Наименьший ущерб будет нанесен в случае раннего обнаружения (на этапах доставки или закрепления).

Время, место и обстановка совершения правонарушения. Время совершения компьютерного правонарушения не всегда может быть установлено с точностью до дня, и тем более, до часов и минут. Установление точного времени возможно, когда момент подключения/отключения фиксируется в системных журналах, журналах соединений, журналах на сервере тарификации и т.п. Нередко время совершения преступных деяний, особенно многоэпизодных, определяется несколькими периодами разной продолжительности. При этом само деяние, наступившие последствия, и их обнаружение, могут быть разнесены по времени.

В соответствии с ч. 2 ст. 9 УК РФ *временем совершения преступления* признается время совершения общественно опасного деяния (т. е. окончания такого деяния) независимо от времени наступления последствий.

Использование сетевых технологий и возможностей удаленного доступа приводит к тому, что общественно опасные деяния (например, создание вредоносного ПО) могут совершаться в одном месте, а последствия (например, последствия заражения вредоносной программой) – наступать в другом месте, часто находящемся на значительном расстоянии. При этом правонарушитель не вступает в непосредственный контакт с потерпевшей стороной и может не иметь физического доступа к СВТ потерпевшей стороны. В связи с этим под *местом совершения* компьютерного правонарушения понимается место, где было совершено общественно опасное деяние, то есть там, где расположены устройства управления компьютером, которым пользовался нарушитель (клавиатура, мышь и т.п.). Данный принцип лежит в основе определения территориальной подследственности в соответствии со ст. 152 УПК РФ.

В отличие от места совершения преступления, *место происшествия* характеризуется наличием *следовой картины*, оставленной в результате реализации правонарушения. Поэтому местом происшествия в случае компьютерного правонарушения может быть место, где:

- производились преступные деяния (осуществлялся доступ в компьютерную сеть, вводились команды и информация, создавалось вредоносное ПО и т.п.);
- расположены информационные ресурсы, которым нанесен вред в результате неправомерного воздействия;
- где наступили вредные последствия, либо иные места, например, место расположения транзитных носителей информации и др.

Мест происшествия для компьютерных правонарушений может быть несколько, в том числе и значительно удаленных друг от друга, находящихся в разных юрисдикциях (например, за рубежом).

Обстановка совершения компьютерного правонарушения включает материальные и социально-психологические факторы среды, в которой происходит преступное деяние (например, установленные средства защиты информации, возможность применения методов социальной инженерии к персоналу атакуемой организации и т.п.). Важная черта обстановки проявляется в том, что она динамична.

Состояние обстановки достаточно сильно влияет на поведение участников правонарушений в компьютерной сфере. Как правило, совершению правонарушения предшествует тщательная подготовка, которая связана с изучением и приспособлением к выявленной обстановке. С этой целью в обстановку могут вноситься изменения, например, путем внедрения в атакуемую компьютерную систему вредоносного ПО. Целью таких действий является нейтрализация или изменение функций системы защиты и получении возможности осуществления неправомерного доступа.

К факторам, способствующим совершению преступления, можно отнести низкий уровень защищенности компьютерных систем и сетей, концентрация компьютерной информации различного назначения в незащищенных базах данных, ошибки в управлении доступом к компьютерной информации, широкий круг пользователей, возможность физического доступа посторонних лиц к СВТ.

На обстановку, складывающуюся после совершения преступления, накладывают отпечаток условия и обстоятельства, происходящие впоследствии. Так, следы пребывания в системе, появившиеся вследствие совершения преступления, могут целенаправленно уничтожаться правонарушителями (например, путем очистки журналов операционной системы, журналов прикладных систем и удаления системных файлов, либо шифрования носителя информации). Некоторые цифровые следы могут в процессе функционирования системы естественным путем затираться новы-

ми, вплоть до такой степени, что восстановить их окажется невозможным. Так, по данным специалистов Group-IB, уже по прошествии трех месяцев проведение полноценного расследования и восстановление картины произошедшего представляется проблематичным.

Механизм следообразования. На месте происшествия можно обнаружить как «традиционные» следы, так и виртуальные следы, остающиеся в памяти электронных устройств как потерпевших, так и правонарушителей.

Можно выделить следующие группы следов преступлений, связанных с использованием компьютерных средств:

- следы на средствах компьютерной техники, с помощью которых было совершено правонарушение: использовавшееся для неправомерного доступа ПО, журналы подключения к ИТС, сохраненные коды доступа, тексты программ, скопированная у потерпевшей стороны информация и т.п. Такие следы могут остаться в записях операционной системы, в аппаратно-программной конфигурации компьютерных средств, на электронных носителях и др.;
- следы на «транзитных» (телекоммуникационных) носителях информации, посредством которых лицо осуществляло связь с удаленными ИС или ресурсами: документированная информация о трафике через оператора телематических услуг, размещенная в сети информация, электронная переписка и т.д.;
- следы в подвергшейся воздействию компьютерной системе, в том числе, на электронных носителях: результаты неправомерного уничтожения, блокирования, модификации компьютерной информации, воздействия на средства защиты информации и несанкционированного доступа к компьютерной системе. Местоположение этих следов сходно со следами в компьютерной системе нарушителя;
- следы на иных компьютерных средствах (компьютерах, органайзерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах, диктофонах, других носителях информации), непосредственно не участвовавших в совершении преступления, но содержащие имеющие значение для уголовного дела сведения;
- документы, изготовленные с использованием средств компьютерной техники;
- традиционные следы, как материальные – рук, обуви, орудий, инструментов и др., так и идеальные. Под идеальными следами понимается отображение события в сознании человека, в этом случае криминалистически значимая информация может быть воспроизведена в вербальной или иной форме (например, в качестве свидетельских показаний).

Так, автор [15] приводит пример из практики, когда обладающий высокой ИТ-квалификацией правонарушитель довольно чисто уничтожил виртуальные следы (всевозможные компьютерные журналы, временные файлы, информацию в файле подкачки и т.д.) и считал, что его преступление «абсолютно недоказуемо». Однако он совершенно забыл про существование пяти свидетелей, которым сам все подробно описывал и показывал.

Отличительными чертами информации, хранящейся в цифровом виде, в том числе и виртуальных следов, являются:

- неявный вид и необходимость использования специальных средств (программных, аппаратных) для обеспечения ее восприятия;
- возможность уничтожения или модификации в кратчайшие сроки и удаленно;
- наличие специальных средств, ограничивающих доступ к данной информации;
- постоянное изменение информации в ходе работы пользователя и выполнения различных операций;
- формирование взаимосвязанной информации на различных устройствах одновременно при передаче данных по каналам связи.

Перечисленные свойства цифровых данных обусловливают необходимость соблюдения определенных правил при фиксации и изъятии цифровых доказательств, а также их судебно-экспертном исследовании.

ГЛАВА 2. ОСНОВНЫЕ МЕРОПРИЯТИЯ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРАВОНАРУШЕНИЙ И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Возбуждение уголовных дел по преступлениям в сфере высоких технологий

Поводом для возбуждения уголовных дел по преступлениям в сфере высоких технологий, в соответствии со ст. 140 УПК РФ, может быть:

- заявления граждан или юридических лиц, которым в результате противоправных действий причинен вред или возникла угроза его причинения;
- явка с повинной лица, совершившего преступление;
- сообщения о совершенном или готовящемся преступлении, полученном из разных источников (в основном, такая информация может быть получена по материалам контрольно-ревизионных и иных документальных проверок, по публикациям в СМИ, из оперативных источников, в ходе проведения оперативно-розыскных мероприятий специализированными подразделениями МВД и ФСБ России, при задержании лица с поличным. Признаки компьютерного преступления могут быть обнаружены и при расследовании других преступлений, не обязательно компьютерных);
- постановление прокурора о направлении материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

Важно, что квалифицировать действия, вызвавшие компьютерные инциденты, как преступления могут только представители правоохранительных органов (следователь), а в дальнейшем – суд. Для установления оснований для возбуждения уголовного дела (за исключения задержания правонарушителей с поличным), требуется тщательная проверка и оценка имеющихся данных (ст. 144 УПК РФ). В ходе предварительной проверки должны быть подтверждены факты:

- нарушения целостности, доступности или конфиденциальности информации, нарушение нормального функционирования или работоспособности компьютерной системы;
- наступления вредных последствий;
- наличие причинно-следственной связи между неправомерными действиями и наступившими последствиями;
- а также определен размер ущерба, который может быть использован при квалификации преступных деяний − причинение значительного ущерба гражданину, крупного ущерба, тяжких последствий или создание угрозы их наступления.

Размер ущерба в денежном выражении определяется ст. 158 УК РФ. Так, на 2019 год крупным размером ущерба признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным − один миллион рублей. Значительный ущерб гражданину (используется, например, в ст. 159.3 и ст. 159.6) определяется с учетом его имущественного положения, но не менее 5 тысяч рублей.

В ходе решения вопроса о возбуждении уголовного дела членами следственной группы обычно проводятся следующие действия: получение объяснений (опрос) заявителя, производство осмотра места происшествия, истребование необходимых материалов, осуществление других оперативно-розыскных мероприятий (например, задержание подозреваемых), назначение и производство судебных экспертиз (исследований), консультации со специалистами. По результатам предварительной проверки может быть возбуждено уголовное дело с квалификацией по составам статей УК РФ, либо может быть отказано в возбуждении уголовного дела.

Алгоритм расследования компьютерных преступлений складывается в зависимости от состава совершенного преступления и исходной следственной ситуации. Планирование расследования компьютерных преступлений на начальном этапе характеризуется, как правило, высокой информационной неопределенностью, личность преступника не установлена. В таких случаях обычно планируют следующие первоначальные следственные действия, оперативно-розыскные и организационные мероприятия:

- опрос заявителя и лиц, на которых указано в исходной информации как на возможных свидетелей;
- привлечение специалистов, обладающих специальными познаниями, для консультаций и участия в следственных мероприятиях;
- решение вопроса о возможности задержания подозреваемого с поличным и о необходимых в связи с этим мероприятиях;
- осмотр места происшествия;
- проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления виновных лиц, обнаружения следов и других вещественных доказательств;
- выемка и последующий осмотр средств компьютерной техники, предметов, материалов и документов, характеризующих информационный процесс, с которым предположительно связаны преступные деяния;
- допросы свидетелей (очевидцев);
- допросы подозреваемых (свидетелей), чья деятельность непосредственно связана с информационной системой, обеспечением ИБ и подвергшейся преступному посягательству информацией;

- обыски на рабочих местах и по месту проживания подозреваемых;
- назначение компьютерной (технико-компьютерной) экспертизы, технико-криминалистической экспертизы документов, бухгалтерской и иных экспертиз.

2.2. Привлечение к расследованию специалистов

На успех расследования правонарушений в компьютерной сфере в значительной мере влияет привлечение специалистов, обладающих специальными познаниями в области ИТ, телекоммуникаций, программирования и защиты информации. Помощь таких специалистов требуется буквально на каждом этапе – от обнаружения признаков правонарушения до поддержания обвинения в суде. Специальные знания нужны уже на самой ранней стадии расследования – при первичной проверке материала дела, а также при проведении оперативно-розыскных мероприятий. Специалист может привлекаться также в качестве эксперта для проведения исследования компьютерной информации и дачи заключения в ходе компьютерно-технической экспертизы.

Согласно ст. 58 УПК РФ, **специалист** – лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном УПК РФ, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию.

В соответствии с ч.2 ст. 168 УПК РФ перед началом следственного действия, в котором принимает участие специалист, следователь обязан удостовериться в его компетентности. В качестве подтверждения могут быть предъявлены дипломы о высшем или среднем профессиональном образовании по специальности, дополнительные квалификационные документы (свидетельства о повышении квалификации, присвоении научной степени), документы, подтверждающие значительный стаж работы по специальности. Если специалист не может подтвердить свой профессиональный уровень документально, его квалификация может быть подвергнута сомнению со стороны защиты. Такие специалисты не могут привлекаться к следственным действиям, но могут оказывать консультирование неофициально. Справочно-консультационная деятельность является непроцессуальной формой использования специальных познаний. В этой форме специалист может оказывать помощь следователю в подготовке

следственных действий, материалов для экспертизы, формировании вопросов эксперту и т.д.

Справочно-консультационная деятельность может осуществляться как до, так и в процессе производства по делу. Чаще всего она необходима следователю до возбуждения уголовного дела (до начала производства по делу) или на начальном этапе и касается получения общих сведений о компьютерных системах. Если факты, полученные в результате консультации, могут иметь доказательственное значение, то после начала официального производства по делу консультация может быть оформлена справкой или ответом на официальный запрос следствия. Полученный в итоге документ рассматривается в качестве источника доказательств, и будет являться, в соответствии с п. 6 ч. 2 ст. 74 УПК РФ, иным документом.

Специалист может участвовать в любых следственных действиях. На начальных стадиях расследования он, как правило, привлекается для участия в таких следственных действиях как:

- осмотр места происшествия;
- обыск и выемка;
- допрос подозреваемого (обвиняемого), потерпевшего, свидетеля, а также для участия в оперативно-розыскных мероприятиях.

На последующих этапах следствия по делам о компьютерных правонарушениях могут проводиться такие следственные действия с привлечением специалиста, как следственный эксперимент (ст. 181 УПК РФ). В частности, могут производиться следственные эксперименты по проверке возможности:

- проникновения в помещение (с отключением и без отключения систем охранной сигнализации и видеонаблюдения);
- перехвата информации с помощью специальных технических средств, а также визуального наблюдения за действиями оператора;
- подключения конкретных средств компьютерной техники и осуществления непосредственного доступа к компьютерной информации;
- подключения к ИТС;
- нейтрализации средств защиты информации;
- совершения определенных операций с компьютерной информацией в одиночку;
- совершения определенных операций с помощью конкретных СВТ за определенное время, а также по установлению временного промежутка, необходимого для производства таких действий.

2.3. Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации

По делам о правонарушениях в компьютерной сфере могут производиться осмотры:

- места происшествия;
- средств вычислительной техники;
- электронных носителей информации;
- электронных документов.

Обыск – это принудительное обследование, он проводится на основании постановления следователя (а обыск жилища – по постановлению суда) в рамках возбужденного уголовного дела с целью обнаружения предметов, вещей, ценностей, имеющих значение для уголовного дела (ст. 182 УПК РФ). *Осмотр* же места происшествия, документов и предметов может быть произведен до возбуждения уголовного дела (ст. 176 УПК РФ). В отличие от осмотра, обыск носит принудительный характер, поэтому при его проведении членам следственной группы следует предусмотреть возможность оказания сопротивления со стороны лиц, находящихся на объекте обыска, а также попыток изменения или уничтожения криминалистически значимой компьютерной информации.

Осмотр производится следственной группой с возможностью привлечения необходимых специалистов. Осмотр помещения организации производится в присутствии представителя администрации соответствующей организации (ст. 177 УПК РФ). Осмотр жилища производится только с согласия проживающих в нем лиц, либо по решению суда.

При проведении специальных мероприятий с участием специалиста основной задачей является обеспечение сохранности информации, имеющейся в компьютерных системах и на электронных носителях информации. Для этого, в зависимости от обстоятельств дела, необходимо [3]:

- предотвратить отключение энергоснабжения для обеспечения сохранности энергозависимых данных (может потребоваться охрана распределительного щита);
- запретить производить какие-либо манипуляции с компьютерами и носителями информации даже членам следственной группы, все действия выполнят специалист, в случае невозможности специалиста провести действие собственноручно, оно выполняется под его контролем;
- оградить работающие компьютеры от случайных или преднамеренных нажатий на клавиши клавиатуры, кнопки системных блоков и устройств;

- предупредить всех сотрудников о недопустимости самостоятельной манипуляции с компьютерной техникой и носителями информации;
- удалить из помещений, в которых находятся компьютеры и носители информации, все взрывчатые, едкие и легковоспламеняющиеся материалы;
- обеспечить отключение беспроводных систем передачи данных.

При соблюдении последнего пункта следует иметь в виду, что некоторая информация может обрабатываться на удаленном сетевом ресурсе, в этом случае следует принять меры к сохранению такой информации с фиксацией данных сетевого ресурса, на конкретный момент времени.

Целями осмотра СВТ и электронных носителей является, прежде всего, обнаружение следов, образовавшихся в результате происшествия или совершения преступления, а также установления технического состояния СВТ и электронных носителей. Поиск и фиксация компьютерной информации осуществляются, как правило, в местах:

- непосредственной обработки и постоянного хранения информации;
- непосредственного использования компьютерного оборудования;
- непосредственного нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС;
- наступления вредных последствий.

В отличие от многих иных видов свидетельств, компьютерная информация не может восприниматься человеком непосредственно. Для ее восприятия необходимо посредство технических аппаратных и программных средств, причем количество и сложность этих технических посредников настолько велики, что связь между исходной информацией и воспринимаемом человеком образом, далеко не всегда очевидна. Таким образом, в случае компьютерных правонарушений осмотр – это не визуальный осмотр, а скорее инструментальная проверка, требующая определенных знаний об используемых технических средствах и принципах их действия. Поэтому осмотр компьютерной техники, электронных носителей информации и электронных документов производится с привлечением *специалиста*.

При проведении осмотра места происшествия первоначально выясняется *общая информация о происшествии* (инциденте):

- дата и время обнаружения инцидента (признаков правонарушения);
- контактные данные лица, обнаружившего инцидент;
- тип инцидента;
- средства обнаружения признаков компрометации задействованной компьютерной системы;
- предпринятые действия по восстановлению системы;
- продолжается ли инцидент в настоящее время;

– информация об устройстве обнаружения.

Относительно *помещения*, в котором расположены задействованные в происшествии устройства, выясняется:

– кто имеет доступ в помещение в рабочее/ нерабочее время;
– наличие системы контроля и управления доступом (СКУД);
– наличие видеонаблюдения;
– наличие охраны.

Кроме того, выясняются данные об *организации ИТ-инфраструктуры* организации:

– расположение устройств, топология сети;
– наличие беспроводных сетей;
– данные о системном администрировании (контактные данные системного администратора);
– домен, права пользователей на рабочих станциях, политики;
– каким образом осуществляется доступ в Интернет (технология, схема подключения);
– провайдер услуг, хостинг-провайдер, регистратор доменного имени;
– данные о межсетевых экранах/ прокси-серверах;
– внешние IP адреса организации;
– случались ли в последнее время штатные/ внештатные выходы из строя оборудования.

Опрос *системного администратора* позволит выяснить следующие вопросы:

– количество и типы используемых серверов;
– количество и типы рабочих мест;
– типы используемых операционных систем;
– используемое прикладное ПО (базы данных, системы документооборота и пр.);
– используемые средства защиты информации и шифрования;
– наличие и места хранения общих файлов данных, резервных копий серверных дисков и баз данных;
– пароли администраторов системы;
– имена и пароли пользователей.

Для *задействованных компьютерных устройств* определяется:

– имя устройства (компьютера) и его IP адрес в локальной сети;
– ФИО пользователя;
– тип операционной системы;
– версия MS Office;
– наличие антивирусного ПО и актуальность антивирусных баз данных;

- запущенные процессы;
- сетевые соединения и службы;
- обновления операционной системы;
- используемый браузер, версия;
- настроено ли журналирование, журналы операционной системы;
- выключается ли устройство на ночь.

Осмотр следов правонарушения и иных обнаруженных предметов обычно *производится на месте*. Если для производства осмотра требуется продолжительное время или осмотр на месте затруднен, то предметы должны быть изъяты, упакованы, опечатаны, заверены подписью следователя на месте осмотра. Изъятию подлежат только те предметы, которые могут иметь отношение к уголовному делу. При этом в протоколе осмотра по возможности указываются индивидуальные признаки и особенности изымаемых предметов. Все обнаруженное и изъятое при осмотре должно быть предъявлено участникам осмотра.

Все производимые действия в ходе осмотра *протоколируются*. Допускается производство осмотра без участия понятых при условии применения технических средств фиксации хода и результатов следственного действия (обычно, видеозапись). Однако если в ходе осмотра возникает *необходимость снятия копии с электронных носителей информации, участие понятых обязательно* (ч. 2.1 ст. 82 УПК РФ). Участие при производстве следственного действия понятых является гарантом достоверности происхождения скопированной информации.

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). Выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, производится на основании судебного решения (ст. 182 УПК РФ).

По финансовым преступлениям (мошенничество, присвоение или растрата, причинение имущественного вреда путем обмана или злоупотребления доверием – в сфере предпринимательской деятельности, а также разглашение коммерческой, банковской и налоговой тайн, злоупотребления при эмиссии ценных бумаг и др. преступления, указанные в ч. 4 ст. 164 УПК РФ) не допускается необоснованное применение мер, которые могут привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, в том числе не допускается необоснованное изъятие электронных носителей информации (ч. 4.1 ст. 164 УПК РФ). По этим делам изъятие электронных носителей информации допускается лишь в случаях, когда:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации (ст. 164.1 УПК РФ).

Копирование информации осуществляется на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Копирование информации не осуществляется, если копирование может повлечь ее утрату или изменение. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации.

Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись.

Изъятые электронные носители информации хранятся в уголовном деле *в опечатанном виде* в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации (ч. 2 п. 5 ст. 82 УПК РФ).

Следователь в ходе производства следственного действия вправе осуществить *копирование информации*, содержащейся на электронном носителе информации (ч. 3 ст. 164.1 УПК РФ). В *протоколе* следственного действия должны быть *указаны технические средства*, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носите-

ли информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия (ч. 3 ст. 164.1 УПК РФ). Это позволяет получить процессуальное удостоверение факта появления копии информации, имеющее доказательственное значение.

Процедура *копирования информации* в процессе следственного действия должна позволять решать задачи обеспечения достоверности и неизменности сведений. То есть, при копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. Ошибки в выборе метода копирования, объеме копируемой информации лицом, не имеющем специальных знаний в этой области, могут вообще исключить возможность использования полученных данных в качестве доказательств или снизить возможность их дальнейшего экспертного исследования. Поэтому копирование электронных носителей и фиксация другой компьютерной информации обычно *выполняется специалистом*.

В ряде случаев с учетом закономерностей механизма следообразования изъятие носителей оказывается неприемлемым для целей фиксации доказательной информации. В частности, достаточно сложно зафиксировать сведения, хранящиеся на массивах жестких дисках серверов, путем изъятия этих дисков. Современные технологии 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 привести к невозможности восстановления интересующих данных.

Согласно сложившейся криминалистической практике, если носитель следовой информации невозможно изъять в натуре, с него снимают копию, отражающую значимые признаки. Фактически в отношении данных, размещенных в облачных хранилищах или на серверах компаний, предоставляющих услуги хостинга и размещения медиаконтента (YouTube, Вконтакте и т.п.), единственным приемлемым способом фиксации доказательственной информации является ее копирование. При изъятии информации с серверов передачи и хранения данных изымается только необходимая информация, а не весь дисковый массив, при этом по возможности производится фиксация (копирование) информации без изъятия электронных носителей и компьютерной техники.

Согласно ч. 2 ст. 86 УПК РФ, потерпевший, гражданский истец и их представители вправе собирать и представлять письменные документы и предметы для приобщения их к уголовному делу в качестве доказательств. Поэтому зачастую организации сами привлекают специалистов для сбора

свидетельств происшествия (инцидента). Задача специалиста в этом случае – обеспечить доказательную силу собранных свидетельств для того, чтобы представленные потерпевшей стороной доказательства не были признаны недопустимыми в соответствии со ст. 88 УПК РФ. При проведении осмотра компьютерной техники, изъятия электронных носителей информации и копирования информации с них специалист придерживается вышеизложенных требований УПК РФ к соответствующим процедурам:

- осмотр СВТ, носителей информации, их изъятие и копирование информации производится независимым специалистом в присутствии двух понятых (как правило, привлекаются сотрудники организации, они же выступают и в роли представителей организации);
- все предпринимаемые специалистом действия протоколируются, и кроме того, как правило, фиксируются с помощью фото/ видеосъемки;
- изымаемые носители информации опечатываются и хранятся в надежном месте (например, в сейфе), чтобы исключить повреждение и доступ к содержащейся на них информации;
- составляются акты о копировании информации, выгрузке/ снятии данных, изъятии носителей информации, их опечатывании, передачи материалов на исследование, заверенные всеми участвующими сторонами.

Указанные акты должны содержать детальную опись объектов с информацией и их источников. То есть должны указываться реквизиты, позволяющие однозначно идентифицировать объект (например, серийные номера рабочих станций и накопителей на жестких магнитных дисках, а также их тип). Опечатанные носители информации хранятся вместе с соответствующим актом до передачи их на исследование (экспертизу) или в правоохранительные органы.

2.4. Осмотр электронных документов

Осмотр документа на электронном носителе обычно производится следователем или дознавателем с участием предметного специалиста. Целями такого осмотра является выявление и анализ внешних признаков и реквизитов документа, анализ его содержания, обнаружение возможных признаков его подделки (фальсификации).

При осмотре документов, содержащихся в ИТС, в частности, в Интернет, осмотр происходит опосредованно (через ИТС). Осмотр может быть проведен с помощью рабочего оборудования (компьютера), подклю-

ченного к этой сети и размещенного в подразделении органа предварительного расследования.

При этом ссылки на ресурсы, содержащие автоматический переход, с технической точки зрения аналогичны самому ресурсу (на ресурсах социальных сетей могут быть расположены, например, ссылки на видео экстремистской направленности, а не само видео).

В *протоколе* осмотра интернет-ресурса описывается его внешний вид и все действия, выполняемые следователем, начиная от загрузки операционной системы и браузера до последовательного перехода по ссылкам и пунктам меню [2]. Так как размещенная в сети информация не статична, и впоследствии она может быть изменена или удалена, необходимо указывать время осмотра, т.е. каждое действие по фиксации информации обязательно должно иметь привязку ко времени. Необходимо зафиксировать и указать в протоколе часовой пояс или время UTC Всемирное координированное время (UTC), а также адрес каждой копируемой страницы сайта. Содержимое страниц сайта может быть скопировано как с помощью штатных средств браузера, так и с помощью специализированного ПО для копирования всего содержимого сайта. В ряде случаев достаточно сделать скриншот страницы. Для копирования видеороликов с YouTube могут применяться специальные программы, свободно распространяемые в сети Интернет.

Использование свободных программных продуктов, не сертифицированных ФСТЭК России, не противоречит нормам УПК РФ. Возникновение возможных сомнений в том, что такая программа может скрытно для пользователя реализовать вредоносные функции, в том числе изменить копируемые данные, устраняется путем приложения к протоколу следственного действия неперезаписываемого оптического диска или иного носителя, на которых записаны portable версии использованных свободных программ, с которых они запускались. Если в процессе дальнейшего производства по делу будет установлено противоречие доказательств, его всегда можно будет устранить путем экспертизы вызвавших сомнение программ.

Скопированные файлы сохраняют на неперезаписываемый носитель информации (CD, DVD), что исключает их дальнейшую модификацию. В протоколе осмотра указываются технические средства (компьютер) и программное обеспечение, которые применялись при осмотре и копировании файлов, сами файлы оформляются как приложение к протоколу осмотра.

Если фиксация размещенной в сети информации производится представителем организации или физическим лицом, то используется *нотариальное заверение* содержимого веб страниц.

Если содержащаяся в сети информация представляет общественную опасность, то согласно ст. 15.1, 15.1-1 и 15.3 Федерального закона

«Об информации, информационных технологиях и о защите информации», после снятия копии она должна быть заблокирована до вступления решения суда по уголовному делу в законную силу, а при невозможности блокирования – удалена. Представление правоохранительного органа о блокировании информации направляется в Роскомнадзор или непосредственно компании – владельцу сервера. Предварительно с удаляемой (блокируемой) информации должна быть снята копия в установленном процессуальном порядке. Невыполнение этого условия может привести к потере доказательной базы вплоть до прекращения уголовного дела. Снятие копии компьютерной информации позволяет не только проводить дополнительные (повторные) экспертные исследования, но и обеспечивает сохранность доказательств и их защиту от возможных попыток противодействия расследованию.

2.5. Оперативно-розыскные мероприятия

Перехват и исследование сетевого трафика

Перечень видов оперативно-розыскной деятельности согласно ст. 6 Федерального закона «Об оперативно-розыскной деятельности» включает «снятие информации с технических каналов связи» и «получение компьютерной информации». Указанные оперативно-розыскные мероприятия проводятся с использованием оперативно-технических сил и средств *органов федеральной службы безопасности*, *органов внутренних дел*. Эти универсальные формулировки применительно к компьютерным системам подразумевают *перехват сетевого трафика*.

Сниффинг (перехват и анализ трафика) широко используется для совершения компьютерных преступлений. С другой стороны, в работе ИТ-специалистов анализ сетевого трафика – один из основных методов диагностики и поиска неисправностей и уязвимостей сети.

На основе анализа содержимого и статистики сетевого трафика можно определить и доказать совершение пользователем многих действий в сети, а также получить информацию об устройстве программ, информационных систем и сетей. Сбор и анализ сетевого трафика определенного компьютера может заменить физическое изъятие и экспертизу этого компьютера, поскольку даст такую же информацию, а именно: содержимое электронной почты, свидетельства о просмотре веб сайтов, размещении информации в сети Интернет, несанкционированном доступе к удаленным узлам, использовании контрафактных программ. В то же время осуществить перехват трафика в ряде случаев бывает проще, чем найти и изъять в исправном состоянии компьютер.

Существует достаточно много различных мест и методов перехвата сетевого трафика. С точки зрения организации этого процесса, перехват трафика может быть осуществлен:

- с помощью аппаратуры СОРМ;
- средствами оператора связи;
- собственными средствами.

СОРМ (Система технических средств для обеспечения функций оперативно-розыскных мероприятий) − комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи (за исключением телеграфных каналов). С помощью разных видов СОРМ может осуществляться прослушивание телефонных переговоров, протоколирование обращений к сети Интернет, сбор информации с различных видов связи (с дополнительным контролем части VPN серверов, прямого прослушивания Skype, ICQ, спутниковой связи). Система СОРМ управляется дистанционно и позволяет передавать информацию о наблюдаемых соединениях или сообщениях в автоматическом режиме. Сбор информации может осуществляться в одном из двух основных режимах: *полный перехват* информации (фазы установления соединений, данные о контролируемых вызовах, информация, передаваемая в разговорном тракте) или *статистический контроль* (только информация о фазах установления соединений и данные о контролируемых вызовах).

Согласно ст. 64 федерального закона «О связи» и ряду приказов Минкомсвязи и ФСБ России, на всех операторов связи возложена обязанность по внедрению СОРМ. Оператор должен за собственный счет закупить и установить соответствующее оборудование, через которое будет проходить весь трафик, а также обеспечить каналы связи этого оборудования с пунктом управления, установленном у правоохранительных органов.

Системы законного перехвата сообщений LI (Lawful Interception) есть и в других странах, например, основанные на европейском стандарте ETSI (European Telecommunications Standards Institute), североамериканском CALEA (Communications Assistance for Law Enforcement Act).

В отличие от европейских и американских моделей законного перехвата, функционирование СОРМ полностью контролируется спецслужбами. Спецслужба самостоятельно, без обращения в суд, определяет пользователя, которого необходимо поставить на контроль, и управляет процессом получения информации, роль оператора связи незначительна и заключается только в покупке и установке оборудования СОРМ. ETSI и CALEA предусматривают наличие административной функции оператора, которому высылается судебное решение. С точки зрения спецслужбы непосредственное управление СОРМ значительно повышает ее оперативность и возможности по установлению и контролю законного перехвата, так как

нет необходимости дополнительно запрашивать через суд любое изменение в параметрах СОРМ для определенного абонента, что позволяет экономить административные и временные ресурсы. С другой стороны, данная особенность не гарантирует отсутствия возможности злоупотреблений со стороны самих спецслужб, что послужило поводом признания законодательства о СОРМ нарушающим ст. 8 Европейской конвенции по правам человека, ратифицированной Россией в 1998 году (решение принято Европейским судом по правам человека в декабре 2015 года).

Поскольку в перехватываемом трафике может содержаться тайна переписки (тайна связи) или личная тайна, защищаемые ст. 23 Конституции РФ, ст. 63 ФЗ «О связи», для осуществления такого перехвата средствами оператора связи требуется получение судебного решения. Без судебной санкции возможен перехват своего собственного трафика потерпевшим либо с его письменного разрешения.

Организация может осуществлять контроль трафика в своей сети и осуществлять снятие дампа сетевых подключений, что может быть реализовано на разных уровнях сетевой архитектуры [15].

На *физическом* уровне – с помощью:

- электрических и оптических ответвителей (сплиттеров, Test Access Point, TAP);
- бесконтактных датчиков;
- перехвата радиосигнала (для беспроводных соединений);
- подключения к концентратору (хабу).

На *канальном* уровне – с помощью:

- функции зеркалирования порта на коммутаторе (свиче);
- ARP-атак и проксирования трафика;
- установки снифера на целевом или транзитном узле.

На *сетевом* уровне – с помощью:

- изменения маршрутизации и проксирования трафика;
- встроенных функций межсетевого экрана или системы обнаружения вторжений (IDS).

На *прикладном* уровне – с помощью анализа трафика:

- на прокси-сервере (для HTTP-трафика);
- на сервере электронной почты (для SMTP-трафика);
- с помощью функций DLP-системы.

Если при мониторинге помимо технической информации может быть перехвачено содержимое передаваемых сообщений, согласно действующему законодательству это может быть расценено как нарушение тайны связи/ переписки. Для того, чтобы полученная таким образом информация имела доказательную силу, необходимо соответствующее правовое обоснование ее получения (уведомление сотрудников о контроле),

что требует от организации разработки ряда нормативно-правовых актов и ознакомление с ними сотрудников под роспись. Подробнее эти вопросы будут рассмотрены в параграфе 3.3.

Объем перехватываемого трафика может быть столь велик, что его последующий анализ будет существенно затруднен, поэтому требуется как можно более четко и узко сформулировать критерии фильтрации трафика. Возможно также сокращение объема информации за счет использования таких усеченных вариантов, как перехват сведений о сетевых соединениях (сессиях) или перехват трафика на основе сигнатур.

При перехвате *сведений о сетевых соединениях* содержимое пакетов не сохраняется, ограничиваются информацией лишь об их заголовках.

Перехват *по сигнатурам* реализуется в таком средстве защиты информации, как система обнаружения вторжений. В передаваемых пакетах ищутся заранее предопределенные последовательности байтов, характеризующие некоторые неразрешенные или подозрительные действия, например, попытки несанкционированного доступа, активность вредоносных программ и т.п. Аналогично можно определить характерные последовательности байтов (сигнатуры) для автоматического контроля трафика подозреваемого. Организация избирательного перехвата может быть реализована с помощью практически любой IDS, большинство из которых поддерживает довольно сложные сигнатуры со многими условиями. Тогда будут отслеживаться лишь те сессии, в которых встречаются эти сигнатуры.

Анализ и интерпретация перехваченного трафика должны производиться экспертом в ходе *компьютерной экспертизы*. Для анализа перехваченного трафика необходима также информация о конфигурации и состоянии коммуникационного оборудования (например, данные о конфигурации коммутатора сети и устройства, производящего трансляцию адресов (NAT), а также MAC-таблицу на соответствующем порту), чтобы в ходе КЭ содержимое трафика можно было интерпретировать уверенно, без предположений.

При использовании защищенных протоколов передачи данных (HTTPS, SSH, SMTP/TLS, IPSec и др.), весь трафик или его часть может оказаться зашифрованной. Перехват зашифрованного трафика мало информативен, в этом случае возможно лишь установить сам факт сетевой активности, ее приблизительный объем, а также установить IP адреса взаимодействующих сторон (кроме случая VPN-туннелирования). В этом случае целесообразно перехватывать трафик в том месте, где он идет открытым (например, перехватывать его до входа в туннель или после выхода из него), для чего следует установить, где именно производится шифрование. Поэтому для эффективно решения задачи перехвата сетевого трафика необходимо знать сопутствующую конфигурацию оборудования и интерфейсов.

Использование кейлогеров

Кейлогерами (keyloggers) называют программные или аппаратные устройства для перехвата сигналов с клавиатуры, то есть для записи последовательности нажатых пользователем клавиш. Сбор информации о нажатых клавишах позволяет узнать вводимые пользователем пароли, содержание сообщений, персональные данные и реквизиты платежных средств, и иную информацию.

Кейлогер можно отнести к устройствам двойного назначения, основной функцией которого является скрытное (негласное) получение информации. Вопрос заключается в том, кем осуществляется такой сбор информации – нарушителем или оперативным сотрудником. Кейлогеры могут также использоваться самим владельцем компьютерной системы для обнаружения попыток несанкционированного доступа, а кроме того − для родительского контроля или контроля за сотрудниками (на территории России – с их уведомления).

Аппаратные кейлогеры выполнены в виде переходника, который вставляется в разрыв между клавиатурой и системным блоком. Они не зависимы от используемой операционной системы, не могут быть детектированы программным способом, зато легко обнаруживаются визуально. Существуют аппаратные кейлогеры, которые встраиваются непосредственно в клавиатуру или в USB-кабель, что повышает их скрытность. Аппаратные кейлогеры имеют встроенную память (от нескольких Мб до нескольких Гб) для хранения собранной информации, при этом при записи она подвергается шифрованию. Кроме того, они могут поддерживать беспроводные интерфейсы взаимодействия, например, выступать в качестве точки доступа Wi-Fi, а также в качестве Wi-Fi устройства, включая такие функции, как отчеты по электронной почте, отметки времени и потоковую передачу данных (рис. 1). Стоимость профессиональных аппаратных кейлогеров составляет порядка 40-60$ (http://www.keelog.com/ru/).

а) б) в)

Рис. 1. Примеры аппаратных кейлогеров
а) USB кейлогер; б) кейлогер, спрятанный внутри удлинителя USB;
в) USB-модуль, предназначенный для установки внутри USB-клавиатуры

Основным недостатком использования аппаратных кейлогеров является необходимость получения физического доступа к аппаратуре компьютера, в то время как программный кейлогер может быть установлен удаленно без непосредственного доступа к контролируемой системе.

Большинство программных кейлогеров может быть отнесено к вредоносному ПО, поскольку они приспособлены для скрытного внедрения и работы. Сигнатуры таких программ вносятся в антивирусные базы данных и могут детектироваться как Riskware (потенциально опасное ПО), даже если такая программа распространяется вполне легально (например, как утилита RemoteSpy американской компании CyberSpy Software). Однако часть из них, имеющая «открытый» режим, может использоваться вполне легально, в частности, встраиваться в DLP-системы или в системы родительского контроля.

Основной способ обхода клавиатурных кейлогеров – использование виртуальной (экранной) клавиатуры для ввода конфиденциальной информации. Однако многие программные кейлогеры поддерживают дополнительные функции, включая запись движений мыши и снятие скриншотов.

Поиск информации в открытых источниках

На сегодняшний день сеть Интернет стала информационным пространством, представляющим альтернативу средств массовой информации и традиционным способам коммуникации. Не удивительно, что поиск в Интернет широко используется для обнаружения и фиксации криминалистически значимой информации, хранящейся на ресурсах сети. Источником такой информации являются следующие виды ресурсов: электронная почта, социальные сети, видеохостинги, интернет-магазины, веб форумы, ftp-серверы, пиринговые сети, облачные хранилища информации и чаты.

Поиск по информационным ресурсам Интернета может быть реализован через различные поисковые системы (Google, Yandex и т.п.), использующие производительные алгоритмы обнаружения информации по заданным реквизитам. Такой поиск не требует материальных затрат на приобретение специализированного программного и программно-аппаратного обеспечения. Выявленная информация должна анализироваться на предмет ее достоверности (корректность), объективности и однозначности.

Получение сведений, размещенных на Интернет ресурсах, может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных и следственных мероприятий. Поиск информации на открытых Интернет ресурсах быстрее, а иногда и эффективнее, чем при добывании ее с помощью негласных мероприятий, кроме того, в условиях дефицита времени такие источники подчас являются единственным средством быстрого получения необхо-

димой информации. Сведения, размещенные на ресурсах Интернета, можно использовать для выявления иной криминалистически значимой информации, относящейся к расследуемому событию.

Важнейшим доказательством распространения запрещенных законом материалов через сеть Интернет являются общедоступные веб страницы с этими материалами, а также файлы видеозаписей, фотоснимков, зафиксированные на сайтах, ftp-серверах в пиринговых сетях, облачных хранилищах.

Сообщения о совершении в отношении конкретных физических и юридических лиц преступлений можно обнаружить на форумах, в гостевых книгах на сайтах, в чатах, на страницах социальных сетей. Получение сведений, размещенных на Интернет ресурсах, может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных и следственных мероприятий.

Информационный поиск может осуществляться и с целью получения дополнительной информации о пользователе или группе пользователей сети. Сведения об участниках судопроизводства возможно получить в открытом доступе на их личных страницах в социальных сетях (ВКонтакте, Facebook, Twitter, Instagram и т.п.) либо в персональных блогах.

Информация, содержащаяся в аккаунтах социальных сетей, является важным объективным источником информации о личности как подозреваемых, так и иных участников судопроизводства. Фиксация факта общения в сети, наличия лиц в «друзьях», общие фотографии могут быть использованы для доказывания факта контактов с подозреваемым, мотива преступления, наличия личной заинтересованности и других обстоятельств, кроме того, такие сведения могут быть положены в основу принятия решения о производстве следственных действий (обыска, допроса, принятия решения о контроле и записи телефонных и иных переговоров и др.) или оперативно-розыскных мероприятий.

Для поиска открытых персональных данных могут использоваться открытые государственные базы данных: сайты судов, база недействительных паспортов, база судебных приставов, база дипломов и т.п.

В последнее время для обозначения подобных мероприятий широко используется термин OSINT (Open Source INTelligence) – поиск, сбор и анализ информации, полученной из общедоступных источников.

Наряду с обычным поиском могут использоваться операторы поиска Google (Google Dorks), а также специализированные веб сервисы, например, сервисы поиска в различных социальных сетях по никнейму (https://namechk.com/, https://knowem.com/), проверка наличия регистрации пользователя с указанным никнеймом на популярных сайтах (https://knowem.com/, https://checkusernames.com/), поиск фотографий (Google, Яндекс, https://www.tineye.com/, расширение для браузера

PhotoTracker Lite), поиск аккаунта ВКонтакте по фотографии человека (FindFace, SearchFace, FindClone)[4], сервис Web Archive, сохраняющий снимки сайтов (https://web.archive.org/), поисковая система Shodan, содержащая информацию о подключенных к сети активах и устройствах, поиск кода (https://searchcode.com/) и др.

Мощным инструментом анализа является построение социального графа (графа дружеских связей) пользователя социальной сети. Кроме визуального анализа плотности контактов в группе можно выделять подгруппы (кластеры) – множество узлов, которые имеют больше контактов друг с другом, чем с узлами в других кластерах. Кроме того, социальных граф может быть использован для выявления сходных атрибутов у аккаунтов, в том числе и неявных. Автоматизация построения графа дружеских связей может быть легко реализована для социальных сетей с открытым API (например, ВКонтакте), однако известные приложения такого рода регулярно блокируются. Если же доступ к API сети ограничен, то визуализация связей значительно усложняется.

Ряд специальных инструментов OSINT включены в Kali Linux:

- Maltego от компании Paterva (существуют также версии для Windows и MacOS) – инструмент для выявления отношений, построения, анализа и визуализации связей между различными субъектами или объектами: людьми, группами людей (в социальных сетях), компаниями, веб сайтами, Интернет инфраструктурами (доменами, DNS записями, сетевыми блоками, IP адресами), документами и файлами, фразами и надписями и др.;
- theHarvester – инструмент для сбора e-mail адресов, имен поддоменов, виртуальных хостов, открытых портов/ банеров и имен работников из различных открытых источников (поисковые системы, сервера ключей pgp);
- Social Mapper – поиск аккаунтов в социальных сетях по имени и фото;
- InSpy – поиск в LinkedIn на основе названия работ, компании или адреса e-mail;
- OSRFramework – набор утилит для проверки пользовательских имен, e-mail адресов, доменов, поиска аккаунтов в социальных сетях, глубокого поиска в Интернете, извлечения по регулярным выражениям и др.;
- Metagoofil – поиск публичных документов заданного типа на целевом ресурсе, локальная загрузка, извлечение метаданных и составление отчетов о результатах;

---

[4] Такие сервисы используют открытый API ВКонтакте и технологии нейронных сетей, они регулярно блокируются социальной сетью за нарушение правил, но перезапускаются вновь под новыми именами. Кроме того, подобные сервисы могут быть доступны спецслужбам.

- SubFinder – обнаружение поддоменов с использованием пассивных методов (без обращения к целевому сайту);
- HostHunter – извлечение имен хостов из большого набора целевых IP адресов;
- Amass – анализ пространства имен целевого домена DNS и составление карты сети;
- Machinae – сборщик сведений, связанных с безопасностью, по частичным данным: IP адреса, доменные имена, URL, e-mail адреса, хэши файлов и SSL отпечатки.

Еще один инструмент OSINT – виртуальная машина Buscador (https://inteltechniques.com/buscador/), представляющая собой Linux систему с предустановленными утилитами OSINT, анонимизации и шифрования.

Повышение эффективности интернет-мониторинга предполагает применение контент-анализа, который представляет собой формализованный аналитический метод исследования содержания документов. Основными объектами такого анализа могут быть сетевые информационные ресурсы и тексты в местах сетевого общения (социальные сети, блоги, форумы и т.п.) криминальной направленности. Контент-анализ позволяет установить присутствие в тексте или массивах текстов заданных ключевых слов, зафиксировать смысловые единицы содержания, частоту их употребления, соотношение различных элементов текста. Наиболее широкие возможности контент-анализа социальных сетей представляет использование программ UFED, Мобильный криминалист, XRY, U2. Сопоставление и обобщение полученных материалов позволяет установить связи лиц, их контакты, выявить криминальные социальные группы и т.д.

В своей деятельности правонарушители широко используют различные способы электронной конспирации: предоставление заведомо неверных регистрационных данных, использование данных подставных лиц, использование похищенных реквизитов доступа в сеть Интернет, переадресация обращений пользователей, периодическая смена места размещения ресурса и т.п. Кроме того, при работе в сети используются средства анонимизации, такие как прокси-сервера и VPN (позволяющие, в том числе, обходить блокировку IP адресов, осуществляемую Роскомнадзором), но чаще всего используются анонимные сети, обобщенно называемые «теневым Интернетом» (Darknet)[5]. Вместе с тем, ни одно из технических

[5] Результаты анализа 5 тыс. сайтов в даркнете, проведенного экспертами из Королевского колледжа Лондона (2016 г.), показали, что 57% из них посвящены криминалу, 15% – покупке и продаже наркотиков. По данным экспертов из Trend Micro (2015 г.), 41% страниц даркнета использовали русский язык, на втором месте с небольшим отставанием – английский.

решений не может гарантировать 100% анонимность, что подтверждается успехами правоохранительных органов по отключению серверов крупных торговых площадок даркнета[6].

Анонимные сети децентрализованы, соединения устанавливаются только между участниками – доверенными узлами (friend-to-friend) с применением особых портов и протоколов. IP адреса серверов скрыты. Источник и пункт назначения никогда не соединяются напрямую друг с другом, связь осуществляется несколькими скачками через случайно выбранные узлы сети в разных концах света, что не позволяет отследить конечного пользователя.

Одна из самых популярных и широко используемых анонимных сетей основана на использовании браузера Tor. Браузер запускает локальный прокси-сервер SOCKS, который затем подключается к сети Tor на домене .onion. Tor использует трехуровневое шифрование через двунаправленные туннели. Проект Tor изначально являлся исследовательской разработкой военно-морского флота США, а сейчас управляется некоммерческой организацией. В сети работают свои поисковые системы (Grams, Candle, Fess и др.). Существуют теневые сети на основе других технологий – Freenet, I2P (Invisible Internet Project). В отличие от Tor, проект I2P больше ориентирован на использование сети в контексте приложений (службы электронной почты, IRC, торренты и т. д.).

Мониторинг закрытых сообществ даркнета используется специалистами для киберразведки и аналитики угроз (Threat Intelligence), получения оперативной информации об используемых правонарушителями новых схемах и инструментах, готовящихся атаках и их целях, выявления связей правонарушителей между собой и т.д. Наиболее известным поставщиком услуг Threat Intelligence на российском рынке является компания Group-IB, подобный сервис предоставляет также компания Лаборатория Касперского (Kaspersky).

Определение принадлежности IP адресов

Для того чтобы найденная информация приобрела статус доказательства, она должна быть не только соответствующим образом документирована и приобщена к материалам дела, но также должен быть установлен субъект, ее разместивший. Чтобы установить пользователя того или иного аккаунта в социальной сети или разместившего интересующий следствие контент, необходимо обладать информацией о его IP адресе. Искомая информация может быть предоставлена непосредственно владельцами того интернет-ресурса, которым пользуется абонент.

---

[6] Отключение крупных площадок даркнета повлекло миграцию правонарушителей на альтернативные децентрализованные платформы, например, каналы в мессенджере Telegram и I2P.

Для получения сведений об IP адресе участника социальной сети или зарегистрированного пользователя другого сервиса (например, мессенджера) сотрудником правоохранительных органов (следователем, дознавателем) направляется запрос руководству компании – владельцу сервиса с просьбой предоставить используемый IP адрес и регистрационные данные абонента с определенным никнеймом. Если используются динамические IP адреса, то в запросе должно быть указано точное время выхода в сеть.

Как правило, построение цепочки доказательств выглядит следующим образом: правонарушение → IP адрес → компьютер → человек.

Знание IP адреса пользователя позволяет установить город и страну проживания субъекта, а также получить информацию о его провайдере. Для установления провайдера, предоставившего пользователю возможность выхода в Интернет, можно воспользоваться сервисом WHOIS – открытой базой данных IP адресов Интернет провайдеров (https://2ip.ru/whois/, http://www.whois-service.ru/lookup/, https://www.ripe.net/)[7]. Из данных регистратора можно узнать, за кем закреплена соответствующая подсеть или диапазон IP адресов. Обычно таковым субъектом является оператор связи или его клиент. Очень редко в базе данных регистратора значится непосредственный пользователь IP адреса.

В свою очередь провайдер уже имеет данные о фактическом расположении технического устройства (компьютера), с помощью которого был осуществлен выход в сеть Интернет, или о лице, которое приобрело SIM-карту. Бывает, что этот оператор не знает точного местоположения клиента, поскольку между ним и клиентом находится оператор-посредник, возможно, не единственный. В таком случае придется пройти по всей цепочке операторов.

В принципе, функция определения местоположения конечного оборудования (компьютера пользователя) предусмотрена в COPMe. Однако на практике такая функция в действительности не работает в силу того, что операторы связи учитывают своих клиентов по-разному, держат эти данные в самых различных форматах и редко организуют к ним онлайновый доступ правоохранительных служб.

После установления провайдера ему направляется официальный запрос о предоставлении регистрационных данных пользователя, которому в конкретное время присваивался конкретный IP адрес. Кроме того, может потребоваться информацию о соединениях, которые осуществлялись с данного IP адреса с определенными Интернет ресурсами.

---

[7] https://dnslytics.com/reverse-ip − показывает домены, имеющие тот же IP адрес, то же доменное имя в разных зонах.

В соответствии со ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» *провайдеры обязаны сохранять информацию* о пользователях и о фактах приема, передачи, доставки и (или) обработки ими сообщений в течение *одного года*, а сами сообщения – до *шести месяцев*. Все данные должны храниться на территории Российской Федерации. Состав хранимой информации о пользователях и о фактах приема, передачи, доставки и (или) обработки сообщений определен Постановлением Правительства РФ от 31.07.2014 № 759 (ред. от 16.12.2017). Порядок, сроки и объемы хранения содержимого сообщений определяются Постановлением Правительством РФ от 26 июня 2018 г. № 728.

Получаемые от провайдера сведения о регистрационных данных абонента, которому выделен IP адрес, содержат персональные данные лица, на имя которого оформлен договор об оказании услуг доступа к сети «Интернет», а также информацию о соединениях пользовательского оборудования с сетью «Интернет», получение которой осуществляется в рамках предусмотренного статьей 186.1 УПК РФ следственного действия «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» в порядке, установленном ст. 165 УПК РФ. Поэтому запрос в организацию-провайдер направляется следователем (дознавателем) одновременно с *постановлением суда* о разрешении получения такой информации.

После того, как был установлен компьютер, который использовал данный IP адрес, следует доказать, что этим компьютером в соответствующее время управлял подозреваемый.

Взаимодействие с провайдером (оператором связи) для получения информации о сетях, клиентах и их активности является неотъемлемой частью расследований компьютерных правонарушений, связанных с Интернет ресурсами или использованием сетевой инфраструктуры. В частности, без обращения к провайдерам не обойтись при решении вопроса о принадлежности IP адреса или ящика (адреса) электронной почты. Вместе с тем, такая информация не может быть предоставлена третьим лицам, например, потерпевшей организации, в силу ст. 7 Федерального закона «О персональных данных» и ст. 63 Федерального закона «О связи», в соответствии с которыми оператор обязан обеспечить конфиденциальность персональных данных и соблюдение тайны связи.

Существует ряд особенностей и трудностей в задаче установления принадлежности IP адресов. Например, использование протокола IP v.6, трансляция IP адресов, VPN туннелирование, несимметричная маршрутизация, провайдер, не учитывающий или не знающий своих клиентов, использование прокси-серверов и иных посредников для сокрытия истинного IP адреса и т.д. Поэтому при установлении принадлежности и местопо-

ложения IP адреса в ходе оперативно-розыскных мероприятий или предварительного следствия обязательно участие технического специалиста.

Определение принадлежности доменных имен

Регистраторы доменных имен обязаны использовать единую базу данных (централизованную или распределенную) для обеспечения уникальности регистрируемых имен. Регистрации подлежат все доменные имена первого и второго уровня, а также некоторые выделенные доменные имена третьего уровня. Все остальные доменные имена распределяются по усмотрению владельца соответствующего домена более высокого уровня.

Все базы данных всех регистраторов являются публично доступными с помощью сервисов whois (и по протоколу whois), аналогично регистраторам IP адресов (https://www.nic.ru/whois/, http://www.whois-service.ru/lookup/, https://2ip.ru/whois/).

В Рунете (зоне ru) существует несколько регистраторов, которые имеют централизованную базу данных, а кроме того – индивидуальные базы данных, являющиеся подмножеством центральной. Формат ответа сервиса whois устанавливается владельцем соответствующей базы данных. Он не регламентируется стандартами, и может различаться у разных регистраторов.

Чтобы установить владельца доменного имени из числа подлежащих регистрации, следует обратиться к базе данных соответствующего регистратора. Для не подлежащих регистрации доменных имен обращаться нужно к владельцу соответствующего домена более высокого уровня. Следует иметь в виду, что домен и веб сайт иногда могут иметь разных владельцев.

В соответствии со ст.8 Федерального закона «О персональных данных», физическое лицо может потребовать не размещать свои контактные данные в публичном сервисе whois, однако такие данные (телефон, почтовый адрес, адрес электронной почты) в любом случае должны быть у регистратора, и могут быть получены следователем.

Определение принадлежности адреса электронной почты

В большинстве случаев адрес электронной почты однозначно связан с почтовым ящиком. И все письма, адресованные на этот адрес, попадают в этот ящик, откуда потом пользователь может их забрать.

Однако есть исключения:

- групповые или коллективные адреса, которые представляют собой *адрес списка рассылки*, все поступающие на этот адрес письма рассылаются определенной группе адресатов (к такому типу часто относятся ролевые адреса, например, info@company.ru или noc@provider.net);

- *технические адреса*, за которыми не стоит ни пользователь, ни почтовый ящик, все поступающие на такой адрес письма обрабатываются в автоматическом режиме программой (например, noreply@domain.com – все, что поступает на такой адрес, отправляется почтовым сервером на устройство /dev/null);
- *адреса для пересылки* (forward) сообщений – все поступающие на такой адрес сообщения не складываются в почтовый ящик, а автоматически перенаправляются на другой, заранее заданный адрес.

Каждое электронное письмо содержит информацию о маршруте следования в процессе отправки-получения. При этом данная информация содержится в техническом заголовке письма (RFC-заголовки) и, как правило, не отображается получателю. Анализ информации о движении электронного письма позволит получить сведения об IP-адресе компьютера, с которого письмо было отправлено, и реальный электронный почтовый ящик. Как почтовые клиенты, так и веб интерфейс почтовых серверов позволяют просмотреть содержимое *технического заголовка* письма.

Высокоуровневые заголовки сообщения «From:» («От:»), «To:» («Кому:») и другие передаются в тексте письма и могут не анализироваться принимающей стороной. Куда именно следует доставить сообщение, принимающий почтовый сервер узнает из директивы «RCPT TO:» (протокол SMTP), адрес в которой не обязан совпадать с адресом в заголовке «To:». В ряде случаев при получении письма в поле «From:» может быть указан произвольный, в том числе не принадлежащий отправителю электронный почтовый адрес. То же можно сказать и о заголовке «Reply-To:». Значение заголовка «Date:» («Дата:») также может быть недостоверным из-за возможности подделки или ошибочной настройки времени у отправителя.

В процессе доставки электронного письма, при пересылке от узла к узлу, в строку «Received:» технического заголовка письма добавляется служебная информация, и отправитель не имеет возможности каким-либо образом изменить эти данные. Как правило, поле «Received:» показывает реальный адрес получателя, а также информацию почтовых серверов, через которые осуществлялась передача письма. Самые ранние по времени формирования строки этого заголовка находятся в нижней части, более поздние – в верхней. Поэтому даже если отправитель попытается подделать строку «Received:», она окажется внизу списка. При прохождении через почтовый сервер копия сообщения не сохраняется, однако делается запись в логе о его получении и отправке. Поэтому источник и отправитель сообщений могут быть вычислены из анализа заголовков «Received:» и соответствующих логов серверов электронной почты.

Если адресат пользуется почтовым клиентом, можно определить местоположение почтового ящика, с которым связан адрес электронной по-

чты. Для этого потребуется содействие провайдера, обслуживающего первичный почтовый шлюз. Как правило, ящик находится на этом же сервере; в других случаях сервер пересылает почту на иной сервер, указанный в его настройках.

Затем следует выяснить, кто пользуется этим почтовым ящиком. Так будет установлен владелец адреса. Доказательствами факта использования почтового ящика определенным лицом могут служить:

- наличие на компьютере этого лица почтового клиента, настроенного для доступа к этому ящику (включая пароль);
- наличие на компьютере полученных сообщений электронной почты со служебными заголовками, свидетельствующими о прохождении сообщений через этот почтовый ящик (при использовании почтового клиента);
- наличие на сервере, где расположен ящик, логов об успешном соединении и аутентификации пользователя данного почтового ящика;
- наличие у других абонентов сообщений от этого лица, написанных в ответ на сообщения, отправленные на этот почтовый ящик (в ответе часто цитируется исходное сообщение, а также среди служебных заголовков присутствует заголовок со ссылками на предыдущие сообщения).

В настоящее время подключение через почтовый клиент осуществляется, в основном, в корпоративной среде, в других случаях, как правило, используется веб почта, когда доступ к почтовому серверу осуществляется через Интернет с помощью веб интерфейса.

В соответствии со ст. 23 Конституции РФ каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. К числу иных сообщений можно отнести электронные сообщения, под которыми в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» понимается информация, переданная или полученная пользователем ИТС.

Содержание переписки может быть предоставлено только *по решению суда*. Однако Постановление Правительства РФ от 31.07.2014 № 759 предусматривает возможность получения сведений о пользователях и фактах обмена сообщениями по запросам органов, осуществляющих оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, без необходимости получения судебного разрешения.

Существуют и прецеденты исключения некоторых сведений из числа относимых к тайнам, охраняемым ст. 23 Конституции РФ. Так, в Постановлении арбитражного апелляционного суда от 19.09.2013 № 09АП-

29641/2013, в дальнейшем нашедшем подтверждение в Определении Высшего Арбитражного суда РФ от 16 июня 2014 г. № ВАС-5501/14, сведения об адресах электронной почты, на которые направлялись электронные сообщения, были исключены из числа сведений, защищаемых ст. 23 Конституции РФ, в связи с тем, что для создания почтового ящика требуется введение логина и пароля, при этом конкретный пользователь – физическое лицо не обязан указывать в адресе электронной почты свои персональные данные (например, реальные Ф.И.О., год рождения, телефонный номер, паспортные данные). При этом к тайне связи суд с полной определенностью отнес лишь содержание самих электронных сообщений.

2.6. Назначение компьютерной экспертизы

Исследование компьютерных средств с помощью специальных познаний может осуществляться как до, так и после возбуждения уголовного дела. Специалисты в ряде случаев (например, при осуществлении проверки до возбуждения уголовного дела) также проводят исследования, но эти исследования называются *предварительными*, и полученные результаты не имеют доказательственного значения. Речь идет о *непроцессуальной форме* исследования компьютерных средств, еще не имеющих статуса вещественных доказательств, но могущих таковыми стать при наступлении определенных процессуальных условий.

С точки зрения задач, содержания и методики, предварительное исследование принципиально не отличается от судебной компьютерно-технической экспертизы, однако результаты такого исследования не могут выступать в качестве источников судебных доказательств.

Считается, что в отличие от некоторых видов оперативной информации, которые могут приобрести доказательственное значение посредством осуществления определенной процессуальной процедуры (например, признания объектов, представленных при рапорте оперативного работника, вещественными доказательствами), результаты предварительного исследования ни прямо, ни косвенно не могут быть трансформированы в судебные доказательства.

Основной *процессуальной формой* использования специальных познаний при расследовании и судебном рассмотрении уголовных и гражданских дел с использованием компьютерных технологий, является **судебная компьютерная экспертиза** (СКЭ).

Объекты экспертного исследования на основании результатов экспертизы обретают статус *доказательств*, причем доказательственная ин-

формация, полученная в результате экспертизы, зачастую не может появиться не из какого иного источника.

Судебная компьютерная экспертиза – самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических. СКЭ проводится в целях: определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием.

В теории судебной экспертизы, как правило, используют термин «компьютерно-техническая экспертиза» и выделяют следующие ее виды [11]: аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная (экспертиза данных) и компьютерно-сетевая.

При назначении экспертизы в экспертно-криминалистическое подразделение МВД России используется термин «**компьютерная экспертиза**», а содержание соответствующих исследований определено как «*исследование компьютерной информации*». В компетенции соответствующих экспертов входит разрешение вопросов только в отношении ПО и данных, имеющихся на носителях информации электронных устройств. Упоминания о возможности исследования компьютерного оборудования (аппаратуры) отсутствуют.

Аналогичной терминологии придерживается и ФСБ России, при этом к типовым задачам таких экспертиз отнесены:

- обеспечение доступа к информации, содержащейся в компьютерах и на компьютерных носителях информации;
- определение назначения и функциональных возможностей программного обеспечения и компьютерных устройств;
- выявление действий, произведенных с компьютером и хранящейся в нем информацией.

Таким образом, к вопросам компьютерно-технической экспертизы кроме перечисленных вопросов можно относить также вопросы исследования компьютерной и сетевой аппаратуры.

На разрешение компьютерной экспертизы ставится конкретный вопрос (вопросы), например, имеются ли на носителях информации программные средства для реализации определенной задачи? При этом перед экспертом должны ставиться вопросы факта, а не права, поскольку последние относятся к компетенции следователя или суда. Например, эксперт не может установить, что данный экземпляр программы является контрафактным, он только указывает на признаки контрафактности, такие как снятие защиты от несанкционированного копирования, изменения в программе, не производимые разработчиком, отличие состава пакета программ от лицензионного (наличие либо отсутствие дополнительных файлов) и т.п.

Эксперт – лицо, обладающее специальными знаниями и назначенное в процессуальном порядке для производства судебной экспертизы и дачи заключения (ст. 57 УПК РФ). Судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями. Уголовно-процессуальный закон не препятствует тому, чтобы в качестве эксперта выступал *специалист*, принимавший участие в следственных действиях (например, в осмотре средств вычислительной техники, обыске, выемке), – этот вопрос оставляется на усмотрение следователя.

Объекты, представляемые на экспертизу в рамках расследования по правонарушениям в компьютерной сфере достаточно разнообразны:

- компьютерная информация (текстовые, графические, аудио- и видеофайлы, электронные документы, базы данных, файлы журналов);
- программное обеспечение;
- электронные носители информации (HDD, SDD, оптические диски, пластиковые карты);
- компьютерная техника (компьютеры, ноутбуки, смартфоны, электронные записные книжки, серверное оборудование);
- периферийные устройства;
- печатающие устройства, множительная техника и документы, изготовленные с их использованием;
- ИТС и линии связи;
- телекоммуникационные устройства (аппаратура сотовой связи, беспроводные цифровые устройства передачи данных, сетевое оборудование, роутеры);
- иные СВТ (цифровые фото- и видеокамеры, цифровая аудио- и видеоаппаратура, контрольно-кассовые аппараты, банкоматы, игровые автоматы, средства спецтехники);
- документация по работе с информацией, СВТ, информационным и телекоммуникационным оборудованием.

Типовые вопросы компьютерной экспертизы *информационных объектов* (*данных*):

1. Каковы свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и т.п.) представленных на исследование информационных объектов?
2. Соответствует ли фактическое состояние информационного объекта стандартному состоянию?
3. Какие расхождения имеются между фактическим состоянием информационного объекта и стандартным его состоянием?
4. Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами

находились определенные данные до их удаления или модификации)?

5. Какие операции выполнялись с предоставленным на исследование информационным объектом?

Типовые вопросы компьютерно-технической экспертизы *программных средств*:

1. Каковы общие характеристики (наименование, тип, версия, состояние и т.п.) ПО, предоставленного на исследование?
2. Какие функции выполняет предоставленное на исследование ПО?
3. Возможно ли использование данного ПО для реализации определенной функциональной задачи?
4. Имеются ли отклонения ПО от установленных параметров?
5. Какие защитные возможности имеет ПО и каким образом они осуществляются?
6. Какие изменения происходили с предоставленным на исследование ПО?
7. Направлены ли внесенные изменения в программное средство на преодоление его защиты?
8. Какова хронология использования программного обеспечения с момента его установки?
9. Имеются ли в ПО враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы?

Типовые вопросы компьютерно-технической экспертизы *аппаратных средств*:

1. Является ли представленный на исследование объект компьютерным средством?
2. Каковы технические характеристики (тип, модель, марка, объем, мощность, среднее время доступа к данным, скорость передачи данных и др.) исследуемого компьютерного средства?
3. Какие функции выполняет данное компьютерное средство?
4. Каково фактическое состояние (исправно, неисправно) представленного аппаратного средства?
5. Имеются ли в нем отклонения от типовых (нормальных) параметров, в том числе и физические дефекты?
6. Какие эксплуатационные режимы установлены на данном аппаратном средстве?
7. С чем связано возникновение имеющихся в компьютерном средстве дефектов и возможно ли их устранение?

Типовые вопросы *компьютерно-сетевой* экспертизы:

1. Имеются ли признаки работы данного компьютерного средства в сети Интернет?

2. Какие аппаратные средства использовались для подключения к Интернету?
3. Имеются ли настроенные соединения с узлом сети Интернет и каковы их свойства (номера телефонов провайдера, имена и пароли пользователя, даты создания)?
4. Каково содержание установок программы удаленного доступа к сети и протоколов соединений?
5. К каким Интернет адресам осуществлялся доступ с данного компьютерного средства?
6. Имеется ли какая-либо информация о проведении электронных платежей и использовании кодов кредитных карт?
7. Имеются ли почтовые сообщения, полученные (а также отправленные) по электронной почте?
8. Имеются ли сообщения, полученные (отправленные) посредством использования программ персональной связи через Интернет, и каково их содержание?

К компетенции компьютерно-технической экспертизы не относятся вопросы:

- лицензионности/ контрафактности экземпляров программ, записанных на исследуемых носителях (требует правовой оценки);
- правомерности действий, произведенных с использованием исследуемых объектов (требует правовой оценки);
- стоимости компьютеров, носителей, лицензий на программы (устанавливается в рамках оценочной экспертизы);
- перевода найденных текстов, интерфейсов программ, переписки и т.п.

Результатом проведенного экспертом исследования, основанного на имеющихся у него специальных знаниях, является *заключение* эксперта. Если эксперт может ответить только на часть поставленных вопросов, он готовит заключение с выводами по этим вопросам и с обоснованием причин, по которым он не может дать ответ на остальные вопросы.

Эксперт вправе возвратить без исполнения постановление на проведение экспертизы, если представленных материалов недостаточно для производства судебной экспертизы или он считает, что не обладает достаточными знаниями для ее производства.

Если при производстве судебной экспертизы эксперт установит обстоятельства, которые имеют значение для уголовного дела, но по поводу которых ему не были поставлены вопросы, то он вправе указать на них в своем заключении.

При формулировании выводов эксперт может допустить ошибки, вызванные как объективными, так и субъективными причинами. Поэтому,

как и любое доказательство, заключение эксперта подлежит оценке с точки зрения его относимости, допустимости (строгого соответствия требованиям уголовно-процессуального закона на всех этапах, начиная с получения материалов для исследования) и достоверности.

Применительно к компьютерным преступлениям наибольшие затруднения вызывает проверка достоверности заключения эксперта, особенно в части научной обоснованности и допустимости использования методик экспертного исследования. Динамичность, высокая скорость развития и смены информационных технологий, огромное разнообразие программных и аппаратных средств приводит в ряде случаев к невозможности выработки стандартных, устоявшихся, апробированных методик компьютерной экспертизы. В процессе оценки заключения эксперта следователь, дознаватель, суд должны принять следующее решение:

- объекты, представленные на исследование, допустимы;
- исходные данные, представленные эксперту, правильны;
- представленные эксперту материалы для производства экспертизы достаточны;
- проведенное экспертом исследование полно;
- заключение эксперта достоверно;
- выводы эксперта подтверждены проведенными им исследованиями;
- заключение эксперта правильно;
- заключение эксперта имеет доказательную силу.

Только в этом случае заключение эксперта может использоваться в качестве доказательства по уголовному делу.

ГЛАВА 3. ОРГАНИЗАЦИЯ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Стандарты и общий цикл управления инцидентами ИБ

В отношении инцидентов ИБ в России принят стандарт ГОСТ Р ИСО/МЭК 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», являющийся переводом международного стандарта ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management. Международный стандарт ISO/IEC TR 18044:2004 в настоящее время уже не действует, он был заменен сначала стандартом ISO/IEC 27035:2011, а в настоящее время действует аналогичный стандарт в двух частях: ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management (Принципы менеджмента инцидентов) и ISO/IEC 27035-2:2016 Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response (Руководство по планированию и разработке реагирования на инциденты).

Следует отметить, что ISO/IEC 27001 (и ГОСТ Р ИСО/МЭК 27001–2006) включает требования, связанные с управлением инцидентами ИБ (группа мер А13). Таким образом, управление инцидентами является неотъемлемой частью менеджмента ИБ в организации (рис. 2) и должно соответствовать требованиям системы менеджмента ИБ (СМИБ). Собранные в процессе обработки инцидента данные должны использоваться для извлечения уроков, что позволит организации устранить обнаруженные уязвимости, внедрить новые или усовершенствовать существующие средства защиты информации, внести улучшения в политики и планы управления инцидентами, а также уточнить оценки рисков ИБ.

ISO/IEC 27035-1:2016, как и более ранний стандарт ISO/IEC 18044, определяет *инцидент* ИБ через понятие *события* ИБ.

Событие информационной безопасности (information security event) − происшествие, указывающее на возможное нарушение политики ИБ или отказ защитных мер.

Событие, связанное с информационной безопасностью, представляет собой идентифицированное происшествие состояния системы, услуги или сети, указывающее на возможное нарушение политики в области информационной безопасности или отказ средств управления, или ранее неизвестную ситуацию, которая может иметь отношение к безопасности.

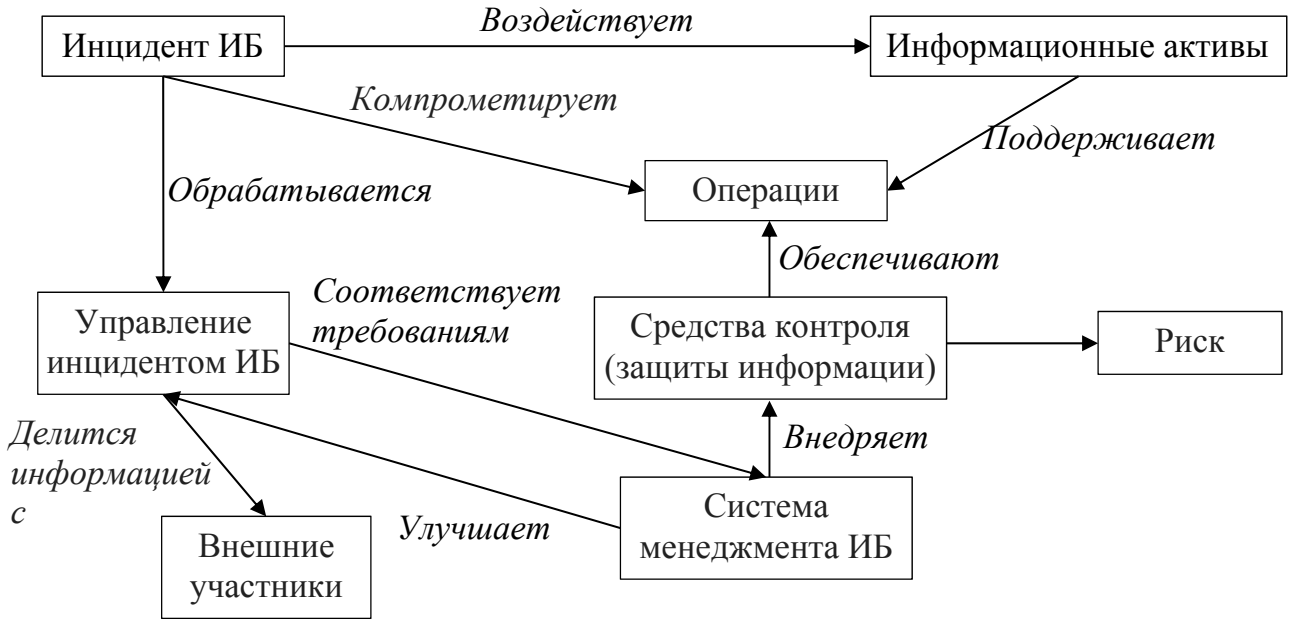

Рис. 2. Связи СМИБ и управления инцидентами ИБ

Возникновение события, связанного с информационной безопасностью, не обязательно означает, что попытка нарушения информационной безопасности была успешной, или что имеются какие-либо последствия относительно конфиденциальности, целостности и/или доступности. Если же нежелательные последствия все же наступили или могут наступить, то событие идентифицируется как инцидент.

Инцидент информационной безопасности (information security incident) – появление одного или нескольких нежелательных или неожиданных событий ИБ, которые могут нанести ущерб активам организации или скомпрометировать ее деятельность.

Таким образом, не все события информационной безопасности, квалифицируются как инциденты информационной безопасности.

Стандарт ISO/IEC 27035-1:2016 приводит следующую связь объектов в цепи инцидентов ИБ (рис. 3). *Угроза* действует нежелательным образом и использует *уязвимости* (слабые места) ИС, услуг или сетей, что приводит к возникновению *событий* ИБ и потенциально вызывает нежелательные *инциденты* информационных активов, подверженных уязвимости. На рис. 3 затененные объекты – те, которые уже существуют; они затрагиваются незатененными объектами, которые приводят к инцидентам ИБ.

В соответствии с американским стандартом NIST SP 800-61 Computer Security Incident Handling Guide (Руководство по обработке инцидентов ИБ) [19], *инцидент ИБ* – это акт нарушения явной или подразумеваемой политики безопасности. Отсылка на политику безопасности позволяет учесть возможные различия между отдельными организациями и их профилями рисков. Одно и то же действие для одной организации может

быть допустимым, а для другой – представлять инцидент безопасности. Например, сотрудникам коммерческих компаний достаточно часто разрешен доступ к корпоративному приложению со своих мобильных устройств, использование личных ноутбуков на рабочем месте, в то же время для предприятия, работающего с секретной информацией, это будет считаться серьезным инцидентом безопасности.

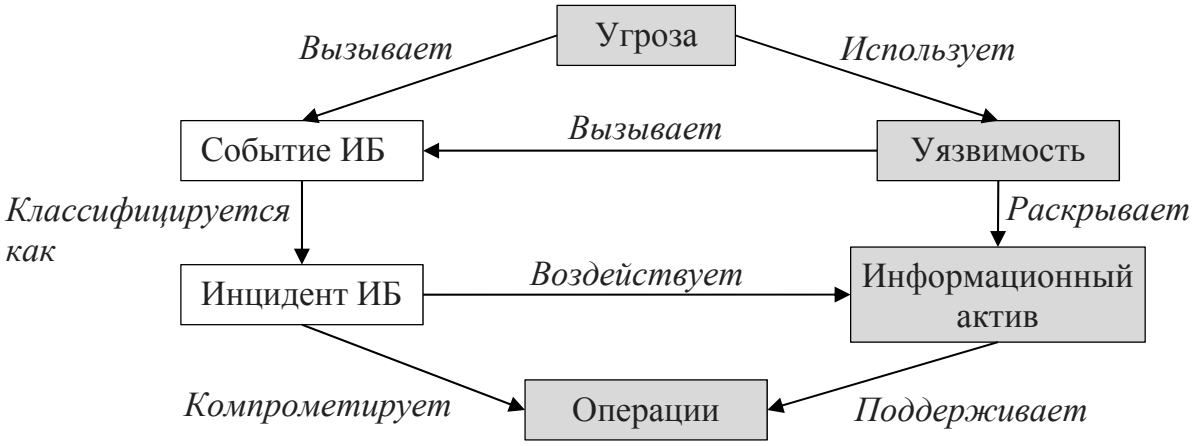

Рис. 3. Связь объектов в цепи инцидентов ИБ

Инциденты ИБ могут быть *преднамеренными* (например, вызванные вредоносным ПО или преднамеренным нарушением политик безопасности) или *случайными* (например, вызванные непреднамеренной человеческой ошибкой или стихийными бедствиями), они могут быть вызваны *техническими* (например, компьютерные вирусы) или *нетехническими* средствами (например, потеря или кража компьютеров). Возможно также деление инцидентов на вызванные *внешними* или *внутренними* причинами. Последствия инцидентов ИБ могут включать в себя несанкционированное раскрытие, изменение, уничтожение или недоступность информации, либо повреждение или кражу активов организации, содержащих информацию.

Раздел 6 ГОСТ Р 18044 ИСО/МЭК ТО 18044–2007 содержит примеры инцидентов ИБ, такие как:

- *отказ в облуживании* – неспособность систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям;
- *сбор информации* – действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки;
- *несанкционированный доступ* – несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети.

Очевидно, данный список не является исчерпывающим.

ГОСТ Р ИСО/МЭК 27001–2006 определяет *инцидент ИБ* как любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

При этом в качестве инцидентов информационной безопасности приводятся следующие события:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Компания Group-IB выделяет следующие основные типы компьютерных инцидентов:

- компрометация сети;
- заражение вредоносным ПО;
- утечка данных;
- фишинг;
- DOS и DDoS атаки;
- взлом веб ресурсов;
- целевые атаки;
- банковское мошенничество.

Стандарт ГОСТ Р ИСО/МЭК 18044–2007 выделяет этапы управления инцидентами ИБ в соответствии с моделью непрерывного совершенствования: планирование и подготовка, использование, анализ и улучшение. Согласно ISO/IEC 27035-1:2016, процесс управления инцидентами ИБ состоит из следующих пяти отдельных этапов:

1. планирование и подготовка;
2. обнаружение и регистрация;
3. оценка и принятие решение (идентификация инцидента);
4. принятие ответных мер;
5. извлечение уроков.

Рекомендация NIST определяет четыре фазы жизненного цикла реагирования на инциденты:

1. подготовка;
2. обнаружение и анализ;
3. сдерживание, ликвидация и восстановление;
4. деятельность после инцидента.

Этапы реагирования на инцидент замкнуты в цикл (рис. 4), что обеспечивает более точное рассмотрение инцидента и возможность предотвращения подобных инцидентов в будущем.

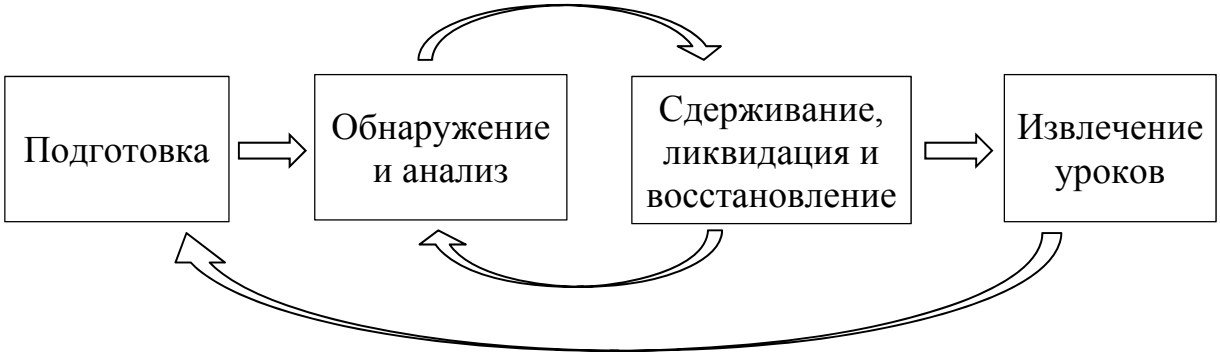

Рис. 4. Цикл обработки инцидента безопасности NIST SP 800-61

Реагирование на инцидент должно осуществляться в зависимости от его категории, определение которой может базироваться на оценках приоритета информации и информационной системы, влияния каждого типа нарушений политики ИБ, масштаба ущерба, уровня тревоги и серьезности нарушения.

В любом случае, все вышеперечисленные стандарты описывают, с точностью до группировки и названия этапов, следующие основные шаги: подготовка, обнаружение, сдерживание (локализация), ликвидация (искоренение), восстановление, извлечение уроков (выводы).

Сначала организация должна *подготовиться* к реагированию на инциденты (и, если возможно, снизить вероятность их возникновения). Первоначальный этап подготовки включает разработку политик и планирование деятельности по управлению инцидентами, а также создание группы реагирования на инциденты (IRT, incident response team), обучение персонала и принятие необходимых технических мер, таких как внедрение и настройка систем журналирования и резервного копирования.

Обнаружение событий ИБ обеспечивается за счет сбора информации об угрозах и уязвимостях безопасности из местной среды и внешних источников данных и новостных лент, мониторинга систем и сетей, анализа на наличие уязвимостей, использования средств обнаружения и оповещения об аномальных и подозрительных действиях.

Затем информация, связанная с появлением событий ИБ, оценивается и принимается решение, следует ли классифицировать эти события как инциденты ИБ. Если есть подозрение, что произошел инцидент ИБ, вся относящаяся к нему информация и действия группы реагирования на инциденты регистрируются для последующего анализа.

После идентификации инцидента ИБ, требуется определить, какие части информационной инфраструктуры были *затронуты*, и, по возможности *предотвратить дальнейшую эскалацию* инцидента. Это может подразумевать отключение пораженных систем или отдельных функций, перенаправление атаки в «песочницу», смену паролей и т.п.

Затем может потребоваться *устранение* компонентов инцидента – удаление вредоносных программ, отключение взломанных учетных записей пользователей, выявление использованных уязвимостей и принятие необходимых мер по их устранению.

Кроме того, может потребоваться *восстановление* системы до работоспособного состояния, восстановление данных из резервных копий.

Не менее важным является деятельность после закрытия инцидента, заключающаяся в *извлечении уроков* из произошедшего для предотвращения подобных случаев в будущем, а также повышения эффективности реагирования, обучении и улучшении деятельности по управлению инцидентами ИБ.

Стандарт ISO/IEC 27035-1:2016 вводит понятие *расследования информационной безопасности*, другой стандарт этой серии ISO/IEC 27043 Information technology − Security techniques − Incident investigation principles and processes использует понятие *процессы цифрового расследования* (digital investigation processes). При этом здесь смысл слова investigation ближе к понятию *исследование*, то есть стандарт описывает, в сущности процедуры сбора доказательств и процессы, характерные для проведения криминалистического исследования компьютерных систем и компьютерной экспертизы для понимания произошедшего.

Согласно ISO/IEC 27035-1:2016, **расследование информационной безопасности** (information security investigation) − применение экспертиз, анализов и интерпретации, для того, чтобы помочь понять инцидент ИБ.

Более ранний стандарт ISO/IEC 18044 и соответствующий ему ГОСТ Р ИСО/МЭК 18044−2007 не содержит каких-либо определений, касающихся расследования, однако на этапе реагирования на инцидент ИБ в качестве дополнительной меры указывает «проведение правовой экспертизы» с использованием слова *расследование* в поясняющем тексте (термин «правовая экспертиза» также не разъясняется).

Стандарты ISO/IEC 27035-1:2016, ISO/IEC 27035-2:2016 рассматривают расследование инцидентов как одно из действий на этапе *принятия ответных мер*, а также, в случае необходимости, на этапе *деятельности после инцидента* (*post incident activity*), когда выполняется дополнительное расследование.

С ISO/IEC 27035 связан ряд стандартов серии ISO/IEC 27000, которые конкретизируют процессы и виды деятельности по управлению инцидентами ИБ с точки зрения сбора свидетельств инцидента, а также их

криминалистического исследования. Фундаментальная цель этих стандартов – продвижение передовых методов и процессов для криминалистического сбора и исследования цифровых доказательств.

ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (ГОСТ Р ИСО/МЭК 27037–2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме [8]) – посвящен первоначальному сбору цифровых свидетельств инцидента.

ISO/IEC 27041:2015 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method (Руководство по обеспечению пригодности и адекватности метода расследования инцидентов) – рассматривает обеспечение достоверности процессов цифровой криминалистики (например, гарантируя, что соответствующие методы и инструменты используются должным образом). Рассматривает формирование требований, связанных с расследованием инцидента ИБ, проверку пригодности (валидацию) процессов цифровой криминалистики, а также использование внешнего тестирования и документации в процессе валидации.

ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence (Руководство по анализу и интерпретации цифровых доказательств) – затрагивает такие вопросы, как стандартный контроль доказательств, выбор и использование криминалистических инструментов, а также профессионализм и компетентность следователей.

ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes (Принципы и процессы расследования инцидентов) – предоставляет руководящие принципы, которые включают идеализированные модели общих процессов расследования инцидентов ИБ в различных сценариях расследования с использованием цифровых доказательств (от процессов подготовки к инциденту вплоть до возвращения доказательств для хранения или распространения).

ISO/IEC 27050 – Information technology – Security techniques – Electronic discovery (Электронное обнаружение) – описывает, по сути, процесс компьютерной экспертизы.

Электронное обнаружение – процесс обнаружения свидетельств, представленных в цифровой форме, одной или несколькими сторонами, участвующими в расследовании, судебном разбирательстве или аналогичном разбирательстве. Процесс электронного обнаружения включает следующие этапы: идентификация относящейся к делу компьютерной информации, сохранение (юридический контроль идентифицированной

компьютерной информации), сбор (извлечение из исходных носителей информации), обработка, просмотр, анализ, производство (официальное представление исходных носителей и результатов анализа в суд в качестве цифровых доказательств).

Предполагается, что стандарт ISO/IEC 27050 будет состоять из 4 частей, в настоящее время приняты три первых части.

ISO/IEC 27050-1:2016 Information technology – Security techniques – Electronic discovery – Overview and concepts (Обзор и концепции) – рассматривает область применения и контекст стандарта ISO/IEC 27050, определяет термины, понятия, процессы обнаружения цифровых доказательств.

ISO/IEC 27050-2:2018 Information technology – Security techniques – Electronic discovery – Guidance for governance and management of electronic discovery (Руководство по стратегическому и операционному управлению электронным обнаружением) – предоставляет руководство по выявлению и обработке информационных рисков, связанных с электронным обнаружением, руководство по управлению компьютерной экспертизой, предлагает несколько возможных метрик.

ISO/IEC 27050-3:2017 Information technology – Security techniques – Electronic discovery – Code of practice for electronic discovery (Свод норм и правил электронного обнаружения) – определяет требования и предлагает практическое руководство по семи основным этапам электронного обнаружения.

ISO/IEC 27050-4 (проект) Information technology – Electronic discovery – Technical readiness (Техническая готовность) – руководство по технологии электронного обнаружения, то есть по инструментам и системам компьютерной криминалистики. Предположительно будет опубликован в 2021 году.

ISO/IEC 30121:2015 Information technology – Governance of digital forensic risk framework (ГОСТ Р ИСО/МЭК 30121–2017 Информационные технологии. Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме [9]) – дает руководству организации основу для заблаговременной подготовки к цифровым расследованиям до того, как они потребуются. Использование ИТ в организации должно стратегически максимизировать эффективность поиска свидетельств, их доступность, а также оптимизировать связанные с этим затраты. Стандарт применим при разработке стратегических процессов (и решений), связанных с хранением и доступностью данных, а также экономической эффективностью свидетельств, представленных в цифровой форме.

Все перечисленные стандарты относятся к группе стандартов менеджмента, то есть дают рекомендации организационного уровня и не

привязаны к каким-либо техническим решениям или конкретным поставщикам.

Исследование подозрительных систем, сбор и сохранение свидетельств инцидента, восстановление цепочки событий и оценка текущего состояния системы в рамках обработки инцидентов ИБ невозможны без применения методов и средств компьютерной криминалистики. Технологии компьютерной криминалистики и потенциальные способы их использования во время реагирования на инциденты ИБ или устранения неполадок рассматриваются в американском стандарте NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response (Руководство по интеграции техник компьютерной криминалистики в реагирование на инциденты) [20].

3.2. Средства обнаружения инцидентов ИБ

Точное обнаружение возможных инцидентов может представлять достаточно непростую задачу:

- инциденты могут быть обнаружены различными способами, с разными уровнями детализации и точности, кроме того, возможны ложные срабатывания автоматизированных систем обнаружения;
- некоторые инциденты имеют явные признаки, которые легко обнаружить (например, дефейс веб страницы), тогда как многие другие инциденты почти невозможно обнаружить, поскольку они не имеют подобных явных симптомов;
- объем событий ИБ, которые потенциально могут являться признаками инцидентов ИБ, как правило, очень велик, например, организация может получать тысячи или даже миллионы предупреждений от датчиков обнаружения вторжений в день, однако далеко не все они могут свидетельствовать о действительно произошедших инцидентах ИБ (например, сбой сервера или изменение критических файлов, могут произойти по причинам, отличным от инцидента ИБ, включая человеческую ошибку);
- для правильной идентификации группы событий в качестве инцидента ИБ могут потребоваться глубокие специальные технические знания и обширный опыт, при этом информация об инциденте может быть получена от разных систем (брандмауэр, IDPS и приложения) и записана в нескольких разных журналах, каждый из которых может отражать какую-то определенную часть данных об инциденте (например, журнал брандмауэра может содержать IP-адрес источника запроса, тогда как в журнале приложения может указываться имя пользователя).

Таким образом, при оценке событий безопасности и идентификации инцидента приходится исходить из неоднозначных, противоречивых и неполных симптомов, чтобы определить, что произошло.

Технические средства обнаружения признаков инцидентов ИБ [16] функционируют на уровнях:

- сетевого периметра и периметра хоста (межсетевые экраны, маршрутизаторы, системы обнаружения вторжений IDS);
- хоста (средства антивирусной защиты, программы контроля целостности файлов, контроль автозагрузки);
- приложений (журналы приложений).

Межсетевые экраны выполняют фильтрацию входящего сетевого трафика, могут действовать на разных уровнях стека протоколов и способны обнаруживать и блокировать сетевые атаки. Мониторинг сквозных соединений может осуществляться на маршрутизаторе, что позволяет отражать атаки канального уровня. На уровне периметра хоста действует персональный брандмауэр, в частности, подобное ПО встроено в операционные системы (ОС) Windows, а также могут устанавливаться решения сторонних производителей (например, Comodo Firewall, Outpost Firewall, Trend Micro Internet Security, Avast Internet Security и др.). Межсетевые экраны уровня хоста доступны как часть большинства серверных ОС (Linux, Windows, BSD, Mac OS X Server).

Системы обнаружения/ предотвращения вторжений (IDS/IPS, Intrusion Detection/ Prevention System) выявляют подозрительные события и записывают соответствующие данные о них, включая время обнаружения атаки, тип атаки, IP-адреса источника и назначения и имя пользователя (если применимо и известно). Различают сетевые (NIDS, network based IDS), хостовые (HIDS, host based IDS) и распределенные (DIDS, distributed IDS). Последние получают информацию с нескольких датчиков (программных или аппаратных), установленных на узлах ИС. Как правило, наряду с сигнатурным анализом IDS используют анализ аномалий, реализуя проактивный мониторинг.

Современные *антивирусные средства* позволяют детектировать различные виды вредоносного и нежелательного ПО, а также определять подозрительную активность программ за счет использования методов сигнатурного, поведенческого и эвристического анализа. Как и IDS, антивирусные системы допускают ложные срабатывания либо могут не обнаружить новую или уникальную атаку.

Многие сценарии атак включают внесение изменений или подмену системных файлов или ПО, добавление запуска несанкционированных компонент в автозагрузку. *Программы контроля целостности* файлов могут обнаружить изменения, внесенные в важные файлы во время инцидентов. Работа проверочных средств основана на расчете контрольной суммы

(как правило, значения хэш-функции) для каждого назначенного файла. Если при пересчете контрольной суммы ее значение отличается от предыдущего, значит файл был изменен. Проверка целостности системных компонент Windows и их восстановление могут быть произведены встроенной утилитой sfc. Компоненты автозагрузки ОС Windows могут настраиваться в реестре, поэтому имеет смысл использовать специальные утилиты, например, Autoruns из набора Sysinternals Suite.

Для контроля внутренних нарушителей и угроз используют *системы защиты от утечек информации* (DLP, Data Leak Prevention), при этом обнаружение и категоризация информация, нуждающейся в защите от утечек, производится на прикладном уровне (содержания сообщений/ документов). Мониторинг и контроль действий пользователя может осуществляться как на хосте, так и на сетевом шлюзе. Использование данных анализа DLP систем требует определенного юридического оформления (см. п. 3.3), поскольку может затрагивать личную информацию сотрудников.

Журналы сетевых устройств, таких как брандмауэры и маршрутизаторы, обычно не являются основным источником содержательной информации об инцидентах. Хотя эти устройства обычно настроены на блокирование несанкционированных подключений и входного трафика, они работают на уровне «сырых» данных (raw data) и предоставляют мало информации о характере несанкционированной деятельности. Тем не менее, такие данные могут представлять ценность при сопоставлении событий, обнаруженных другими техническими средствами.

Большое значение для анализа инцидента ИБ имеют *журналы ОС*, *служб* и *приложений*, которые могут, например, содержать информацию о том, каким учетным записям был предоставлен доступ и какие действия были выполнены. Журналирование событий и политики аудита должны быть включены и настроены на подготовительном этапе цикла управления инцидентами ИБ. Большинство ОС могут быть настроены на аудит и запись определенных типов событий, таких как попытки аутентификации и изменения политики безопасности. Записи аудита могут предоставить ценную информацию, включая время, когда произошло событие, и его происхождение (источник).

Огромный объем данных, создаваемых в файлах журналов, затрудняет их обработку, хранение и извлечение имеющей ценность для обнаружения инцидентов информации. Существуют решения для анализа больших данных, машинных данных и управления журналами, такие как Splunk и Sumo Logic, а также инструмент с открытым исходным кодом Elasticsearch, позволяющий выполнять агрегацию данных и комбинировать различные типы поиска.

Чаще всего данные журналов используются реактивно (то есть уже после произошедшего события), чтобы получить дополнительные сведе-

ния о контексте события. Учитывая это, крайне важно, чтобы файлы журналов были защищены и сохранялись в отдельной системе от той, которая их сгенерировала.

Многие инциденты могут быть обработаны более эффективно и результативно, если в жизненный цикл ИС заблаговременно включены следующие мероприятия:

- регулярное резервное копирование систем и поддержание предыдущих резервных копий в течение определенного периода времени;
- включение аудита на рабочих станциях, серверах и сетевых устройствах;
- пересылка записей аудита для защиты централизованных серверов журналов;
- настройка критически важных приложений для выполнения аудита, включая запись всех попыток аутентификации;
- ведение базы данных хэш-значений для файлов распространенных ОС и приложений, и мониторинг целостности файлов на особо важных ресурсах;
- ведение записей (например, базовых показателей) конфигурации сети и системы;
- установление политик хранения данных, которые поддерживают проведение исторических проверок системы и сетевой активности.

Для оценки того, произошел ли конкретный инцидент, необходимо выявить корреляцию событий безопасности, отраженных в разных источниках. Например, NIDS может детектировать начало атаки против определенного хоста, но для того, чтобы определить, была ли атака успешной, может потребоваться изучить журналы указанного хоста.

Наибольшую степень автоматизации обнаружения инцидентов ИБ обеспечивают *SIEM системы* (Security Information and Event Management), обеспечивающие:

- консолидацию и фильтрацию данных от различных источников (сетевых устройств, приложений, ОС, межсетевых экранов, IDS, антивирусных средств, DLP);
- централизованное хранение журналов событий в едином формате и обогащение событий недостающей информацией;
- выявление корреляции событий (поиск взаимосвязей и закономерностей) и их обработку по правилам, что позволяет с высокой вероятностью определять аномалии, потенциальные угрозы, сбои в работе ИТ-инфраструктуры, попытки несанкционированного доступа, внешние атаки;
- автоматическое оповещение об инцидентах ИБ, ведение базы данных инцидентов и генерацию отчетов;

- предоставление инструментов для анализа событий и разбора инцидентов;
- предоставление документированных свидетельств, могущих выступать в качестве доказательств в суде.

SIEM позволяет выявить реально произошедшие инциденты безопасности из массы регистрируемых событий безопасности и акцентировать внимание только на критических и действительно важных угрозах. Однако эти системы достаточно дороги и сложны в настройке, требуют высококвалифицированного персонала как для развертывания, так и дальнейшей поддержки.

Данные, генерируемые техническими системами, являются лучшими свидетельствами. Это, так называемые, свидетельства «первой инстанции», которые создаются (возникают) без участия исследователя. Примерами являются журнал аудита системы контроля доступа, системные журналы ОС, журналы IDS, SIEM-системы и т.п., которые в данном случае считаются электронными документами.

Технические средства обнаружения событий безопасности достаточно эффективны, однако необходимо помнить и о других источниках информации, например, сообщениях пользователей или технических сотрудников о сбоях или иных признаках инцидентов. Для правильной идентификации и понимания инцидента важную роль играет отслеживание новых уязвимостей, эксплойтов и индикаторов компрометации (признаков инцидентов). Эта информация может быть доступна в открытых источниках, таких как рассылки групп CERT и компаний, осуществляющих Threat Intelligence (feeds – новостные ленты), информация партнеров и поставщиков аппаратного и программного обеспечения, опыт других команд реагирования на инциденты. Источником информации могут быть также платные подписки и сервисы Threat Intelligence.

Оперативные данные Threat Intelligence позволяют заранее подготовиться к инцидентам, отслеживая появление новых векторов угроз, «цепей атаки» (kill chain), способов компрометации информационных процессов и другие изменения в инструментарии и тактике злоумышленников.

3.3. Правовые основания использование данных мониторинга и DLP-систем

Если система мониторинга и контроля действует на прикладном уровне (то есть на уровне пользовательских данных) возникает вопрос о допустимости использования полученных с ее помощью сведений в уголовном и гражданском процессе. К такому классу, относятся, в частности DLP-системы. При их использовании встает проблема допустимости с

точки зрения права контроля за перепиской работников и их действиями в сети Интернет.

С одной стороны, собственником компьютеров, сервера электронного ящика, точек доступа в Интернет является работодатель. Из этого следует и право компании контролировать процесс использования работниками принадлежащего ей имущества в соответствии с его целевым назначением (ч. 2 ст. 209 ГК РФ). Кроме того, одной из трудовых обязанностей работодателя является обязанность обеспечить работника оборудованием, инструментами, технической документацией и иными средствами, необходимыми ему для исполнения трудовых обязанностей (ст. 22 ТК РФ). Этой обязанности работодателя соответствует обязанность работника добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором, соблюдая при этом правила внутреннего трудового распорядка (ст. 21, ч. 1 ст. 189 ТК РФ).

С другой стороны, статьей 23 Конституции РФ гарантировано право каждого на неприкосновенность частной жизни, тайны переписки, телеграфных и иных сообщений. Этот же принцип защиты тайны связи реализован в нормах ст. 63 ФЗ «О связи» и ст. 138 УК РФ, устанавливающей уголовную ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Ограничение тайны переписки допускается только в случаях, предусмотренных федеральными законами.

Согласно разъяснениям, приведенным Пленумом Верховного Суда РФ, доказательства должны признаваться полученными с нарушением закона, если при их собирании и закреплении были нарушены гарантированные Конституцией РФ права человека и гражданина или установленный уголовно-процессуальным законодательством порядок их собирания и закрепления, а также если собирание и закрепление доказательств осуществлено ненадлежащим лицом или органом, либо в результате действий, не предусмотренных процессуальными нормами.

Например, ответ на вопрос «Законно ли увольнение работника за распространение коммерческой тайны, если этот факт был установлен при просмотре его личной (не корпоративной) почты?» отрицателен. Если сведения о пересылке информации, содержащей коммерческую тайну, были получены работодателем в результате несанкционированного доступа к личной почте работника, то такие доказательства будут считаться полученными с нарушением принципов тайны переписки и не смогут подтвердить правомерность увольнения[8].

---

[8] Кассационное определение Судебной коллегии по гражданским делам Волгоградского областного суда от 01.09.11 по делу № 33-11601/11 – в Каспаров С. Проверка электронной почты сотрудников. Как контролировать переписку на законных основаниях, 17.05.2013. URL: http://ppt.ru/news/117831

Соответственно, при решении вопроса о возможности использования информации, полученной при осуществлении контроля работодателем за корпоративной перепиской сотрудников, нужно понять, где проходит граница между частной жизнью работника и его рабочими обязанностями, если речь идет, например, о сообщениях, которыми он обменивается с корпоративной почты (своего рабочего места).

Право работодателя контролировать переписку работника не исключается полностью, однако это право должно быть *закреплено в нормативном правовом акте* или хотя бы в *локальном нормативном акте* организации. В частности, право работодателя на контроль за электронными сообщениями работников, которые отправляются с корпоративных адресов электронной почты, может быть установлено в Правилах внутреннего трудового распорядка организации наряду с обязанностью работника использовать электронную почту только в рабочих целях (ч. 4 ст. 189 ТК РФ). Рекомендуется также указать конкретные цели, в которых работодатель вводит такой контроль.

Кроме того, требуется соблюдение еще одного – получение *согласия работника* на осуществление контроля за его электронной перепиской или, по крайней мере, *осведомленность работника* об этом факте. Точнее, сотрудник должен быть *ознакомлен под роспись* с локальном нормативным актом, в котором устанавливается право работодателя контролировать корпоративную почту или осуществлять мониторинг действий сотрудника. Это отвечает требованиям российского трудового права – согласно ст. 22 ТК РФ, работодатель обязан знакомить работников под роспись с принимаемыми локальными нормативными актами, непосредственно связанными с их трудовой деятельностью. Организация может также заручиться письменным согласием работника на контроль работодателем его переписки с корпоративного адреса электронной почты. Например, такое условие может быть включено непосредственно в трудовой договор.

Таким образом, информация, полученная в результате использования работодателем DLP-систем, может быть использована в качестве доказательств по уголовному делу, а также служить основанием для дисциплинарной ответственности в рамках ТК РФ только в случае легитимного применения работодателем этих систем. То же относится и к использованию других систем мониторинга, позволяющих получать нетехническую информацию. Это в свою очередь предусматривает наличие локального нормативного акта, регламентирующего использование DLP-систем или систем мониторинга данным учреждением, а также осведомленности работника о контроле его электронной переписки и активности в сети Интернет с использованием этих систем и/ или получение от него согласия на осуществление такого контроля.

Как правило, при внедрении DLP-системы организация предпринимает следующие действия.

1. Сведения о DLP-системе или иной системе мониторинга вносятся в трудовые договоры (или дополнительные соглашения к нему), в правила внутреннего трудового распорядка и другие нормативные документы, регламентирующие деятельность сотрудника в организации (например, должностные инструкции). Указывается, что все ресурсы, которые используются в работе, являются собственностью работодателя. Владельцем электронной почты и абонентом телефонной сети является организация, таким образом, они предоставляются работнику во временное пользование в период выполнения служебных обязанностей, и их использование в личных целях запрещено. Тогда, если сотрудник пользуется ими в личных целях, это становится его проблемой, кроме того, он подлежит дисциплинарному взысканию за нецелевое использование рабочих ресурсов или за нарушение правил трудового распорядка.

2. Чтобы сотрудники не могли пожаловаться на нарушение тайны связи, в трудовой договор (или дополнительные соглашения к нему), правила внутреннего распорядка и должностные инструкции вносятся положения о том, что рабочее оборудование и средства коммуникации принадлежат работодателю. Они передаются сотруднику в пользование и предназначены только для выполнения должностных обязанностей, их использование в личных целях запрещается.

Если сотруднику для работы требуется учетная запись в каком-либо мессенджере, то выдача таких учетных записей с паролями должна быть регламентирована, сотрудник должен получать ее под личную ответственность и подтвердить получение ее личной подписью.

3. Разрабатывается регламент мониторинга, в котором должны быть подробно расписаны правила использования, обработки, хранения и передачи конфиденциальной информации внутри организации, а также ответственность, предусмотренная за их нарушения. Регламент должен содержать пункт о том, каким образом полученные в ходе мониторинга сведения могут быть использованы в дальнейшем, причем заявленная информация должна соответствовать действительности. В случае необходимости проведения аудио- и видеозаписи в рамках мониторинга, уведомление об этом также должно быть прописано в регламенте.

4. Все сотрудники компании должны быть ознакомлены с содержанием этого регламента и других организационно-распорядительных документов под роспись.

5. Должны быть приняты необходимые внутренние локальные нормативные акты и разработана организационно-распорядительная документация, определяющие режим коммерческой тайны, режим защиты персональных данных.

6. В политики безопасности и инструкции пользователям информационных систем, сервисов и средств защиты информации могут вноситься правила их использования, определяться ответственность за невыполнение этих правил, указываться, что использование корпоративных средств обработки информации контролируется средствами мониторинга. Также должны быть прописаны правила разграничения доступа к защищаемой информации.

Работодатель тоже имеет определенные обязательства, например, не допустим умышленный тайный сбор личной информации сотрудников, для использования в собственных целях.

3.4. Первичное реагирование на инцидент ИБ

В большинстве случаев на начальном этапе реагирования на инцидент ИБ невозможно знать, что явилось его причиной и будут ли собранные свидетельства инцидента предметом изучения в рамках предварительного расследования и судебного разбирательства в дальнейшем (ведь о природе инцидента, виновнике и наличии умысла еще неизвестно).

Поэтому основной задачей реагирования на инцидент является обеспечение неизменности и сохранности криминалистически значимых данных для возможности их судебного исследования в будущем, а также проведение мероприятий, которые позволяют снизить ущерб и составить необходимые для правоохранительных органов документы. Группа реагирования на инциденты должна обеспечить, чтобы цифровые доказательства собирались и хранились в надежном месте, и чтобы их безопасное сохранение постоянно контролировалось.

Компанией Group-IB разработаны рекомендации по реагированию на инциденты ИБ[9], в соответствии с которыми, сущностью *технических мероприятий* является обеспечение целостности данных, потенциально имеющих отношение к инциденту. При этом сначала должны сниматься короткоживущие (энергозависимые) данные – получение дампов оперативной памяти и сетевого трафика, передаваемого в локальной вычислительной сети организации в момент реагирования на инцидент. В дальнейшем, при проведении криминалистических исследований копии содержимого оперативной памяти и сетевого трафика могут использоваться

---

[9] Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания, 03.10.2012. URL: https://www.group-ib.ru/brochures/Group-IB_dbo_instruction.pdf;
Инциденты информационной безопасности. Рекомендации по реагированию, 2011. URL: http://aciso.ru/upload/iblock/cc7/recommendations_SMALL_FIN_3.pdf

для обнаружения следов работы вредоносных программ (в том числе и бестелесных вирусов, работающих исключительно в энергозависимой памяти) и следов системной активности нарушителя.

Энергонезависимые носители информации (HDD, SDD) следует отключить, что позволит обеспечить сохранность криминалистически значимых данных. Упаковка, опечатывание и надлежащее хранение этих носителей обеспечат достаточный уровень достоверности результатов криминалистического исследования. Если отключение энергонезависимых носителей информации невозможно, создают их криминалистические образы на работающей системе.

Также рекомендуется осуществить копирование лог-файлов сетевого оборудования путем экспорта соответствующих типов данных (журналов доступа, журналов сетевых событий и т. п.) из интерфейса управления устройством на съемный носитель.

Организационные мероприятия заключаются в уведомлении руководства организации, подразделений (служб) ИБ о факте инцидента и об иных сведениях технического характера. Документы, составленные при проведении организационных мероприятий, могут использоваться как основания для рассмотрения вопросов о возбуждении уголовных дел или для уточнения вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации организации.

Типовой сценарий при нарушениях ИБ может быть основан на приведенных ниже базовых действиях.

1. Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
2. Локализовать область ИТ-инфраструктуры, задействованной в инциденте.
3. Ограничить доступ к объектам, задействованным в инциденте.
4. Оформить служебную записку на имя Генерального директора организации о факте возникновения инцидента.
5. Привлечь компетентных специалистов для консультации.
6. Создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем. Протоколировать все действия, которые осуществляются в ходе реагирования на инцидент.
7. Обеспечить сохранность и должное оформление доказательств.
   7.1. Снять энергозависимую информацию с работающей системы.
   7.2. Собрать информацию о протекающем в реальном времени инциденте (лог-файлы сетевого оборудования и сетевого трафика).
   7.3. Отключить от сети питание.
8. В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения.

8.1. Оформить протоколом все операции с носителями информации.
8.2. Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения.
8.3. Задокументировать процесс на фото- и видеокамеру.
8.4. Сохранить опечатанные объекты вместе с протоколом в надежном месте до передачи носителей на исследование или в правоохранительные органы.

9. После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.
10. При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.
11. При проведении расследования обеспечить корректное взаимодействие с заинтересованными подразделениями правоохранительных органов (Управление «К», Центр информационной безопасности ФСБ РФ) и другими внешними организациями (компаниями, предоставляющими услуги в области расследования инцидентов и обеспечения ИБ).
12. По завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.
13. При обращении в правоохранительные органы представить им подробное описание инцидента, описание собранных доказательств и результаты их анализа.

3.5. Процедура сбора свидетельств инцидента ИБ

Одним из принципов управления инцидентами ISO/IEC 27035-1:2016 называет упрочнение доказательств, что подразумевает наличие четких процедур по исследованию инцидента, которые могут помочь проследить, чтобы сбор и обработка всех данных были *законными* и *юридически допустимыми*. Процедура сбора свидетельств инцидента должна обеспечивать такие их свойства как:

- значимость (собранные свидетельства содержат ценную информацию для содействия расследованию конкретного инцидента);
- полнота (собранных свидетельств достаточно для объективного суждения об инциденте);
- достоверность (свидетельства получены из доверенных источников и неизменны, все процессы, используемые при обращении с потенциальными свидетельствами контролируемы и повторяемы, а результаты воспроизводимы);
- допустимость (свидетельства получены легальным способом).

По своему характеру свидетельства, представленные в цифровой форме, могут быть уязвимыми. Они могут быть изменены, фальсифицированы или разрушены в результате ненадлежащего обращения или изучения. Организации должны понимать, что в процессе сбора свидетельств инцидента, проведения расследования или ответных действий на инцидент в результате некомпетентных действий, использования устаревших процессов и инструментов критические цифровые доказательства могут быть частично или полностью разрушены.

Компания Group-IB отмечает высокую частоту случаев некорректного реагирования на инциденты, в ходе которых системными администраторами, сотрудниками подразделений ИБ организаций или иными уполномоченными лицами были уничтожены криминалистически значимые данные, позволяющие привлечь к уголовной ответственности злоумышленников, или была существенно снижена юридическая значимость данных, собранных в ходе внутреннего расследования инцидента.

Процедуры, выполняемые специалистами, должны быть документированы и обеспечивать уверенность в поддержке целостности и достоверности потенциальных свидетельств. При этом, согласно ГОСТ Р ИСО/МЭК 27037–2014, должно обеспечиваться соблюдение следующих основных принципов:

- сведение к минимуму обращения с исходным цифровым устройством или потенциальными свидетельствами, представленными в цифровой форме;
- учет любых изменений и документирование предпринятых действий (в такой степени, чтобы эксперт мог сформировать мнение о достоверности);
- соблюдение действующих на местах правил в отношении свидетельств;
- специалист не должен предпринимать действия, выходящие за рамки его компетентности.

При осуществлении снятия информации специалист должен:

- документировать все действия;
- определять и применять метод установления точности и достоверности копии свидетельств, представленных в цифровой форме, по сравнению с исходным источником (например, сравнение хэш-кодов);
- сознавать, что сохранение потенциальных свидетельств, представленных в цифровой форме, не всегда может быть проведено без изменений.

Существует четыре ключевых аспекта в обращении со свидетельствами, представленными в цифровой форме: контролируемость, обоснованность и повторяемость либо воспроизводимость (в зависимости от конкретных обстоятельств).

Контролируемость. Заинтересованные лица должны иметь возможность оценить выполняемые действия с целью определения того, соблюдался ли соответствующий научный метод, технический прием или процедура. Это достигается путем надлежащего *документирования* всех предпринятых специалистом действий.

Обоснованность. Специалист должен быть способен обосновать все действия и методы, использованные для обращения с цифровыми свидетельствами. Обоснование может быть достигнуто демонстрацией того, что принятое решение было *наилучшим выбором* для получения всех потенциальных свидетельств, представленных в цифровой форме. Это также может быть продемонстрировано посредством *успешного воспроизведения* или *валидации* использованных действий и методов.

Повторяемость. Факт повторяемости признается, если те же результаты теста получают при следующих условиях:

- использование такой же процедуры и метода измерений;
- использование таких же инструментальных средств и при таких же условиях;
- возможно повторение в любое время после первоначального тестирования.

Обладающий соответствующими навыками и опытом специалист должен быть способен выполнять все задокументированные процессы и прийти к *тем же самым результатам* без дополнительных указаний или объяснений. Для достижения повторяемости необходим контроль качества и документирование процесса.

В то же время могут быть обстоятельства, когда повторить тестирование невозможно, например, когда с исходного жесткого диска была снята копия, а затем он был возвращен в использование, или когда речь идет об энергозависимой памяти. В этом случае снимающий информацию специалист должен убедиться, что процесс получения свидетельств достоверен.

Воспроизводимость. Факт воспроизводимости признается, если те же результаты теста получают при следующих условиях:

- использование такого же метода измерения;
- использование различных инструментальных средств и при различных условиях;
- возможно повторение в любое время после первоначального тестирования.

Начальный процесс обработки потенциальных свидетельств, представленных в цифровой форме, состоит из их идентификации, сбора, получения и сохранения.

Идентификация. Процесс идентификации включает поиск, распознавание и документирование потенциальных свидетельств, представлен-

ных в цифровой форме. В процессе идентификации должны определяться цифровые носители информации и устройства обработки, которые могут содержать потенциальные цифровые свидетельства, имеющие отношение к инциденту.

Как правило, специалист должен пытаться максимально увеличить количество данных, сохраняемых путем сбора и получения свидетельств. Может возникнуть необходимость в установлении приоритетов для элементов по степени *изменчивости* и (или) *значимости*/ потенциальной ценности для формирования доказательств.

Потенциальные свидетельства, представленные в цифровой форме, можно разбить на две категории: *энергозависимые* (изменчивые) и *энергонезависимые* (неизменчивые). Изменчивые данные легко могут быть разрушены или навсегда потеряны, если не применяются меры по обеспечению защиты данных. Например, отключение электропитания цифрового устройства может привести к потере изменчивых данных. Неизменчивые данные остаются на носителе даже при отключении электропитания. Поскольку некоторые виды цифровых свидетельств могут иметь короткий срок жизни, следует принять незамедлительные меры для сбора и получения таких данных утвержденными методами.

Следует идентифицировать изменчивость данных, чтобы свести к минимуму ущерб для потенциальных свидетельств, представленных в цифровой форме. Изменчивые данные обязательно должны быть исследованы в случае, если есть подозрение, что было применено шифрование или возможно вирусное заражение.

Как правило, рассматривается следующий порядок изменчивости данных (начиная с наиболее изменчивых) [18]:

1) процессор, регистры и системный кэш;
2) таблица маршрутизации, ARP-кэш, таблица процессов, статистика ядра;
3) оперативная память;
4) временные системные файлы;
5) область подкачки (swap) или виртуальная память (называемая в ОС Windows «файлом подкачки»);
6) жесткий диск и съемные носители информации;
7) данные об удаленном доступе и мониторинге;
8) физическая конфигурация, топология сети;
9) Резервные копии и распечатки данных.

Данные, находящиеся на удаленных сетевых устройствах (таких как прокси-серверы, маршрутизаторы, IDS/IPS и межсетевые экраны), также будут иметь порядок изменчивости. Например, стоит отметить, что сетевые кэши и удаленные журналы могут быть неустойчивыми и должны быть собраны как можно скорее.

К элементам с большой значимостью/ потенциальной доказательной ценностью относятся те, которые, скорее всего, будут содержать данные, непосредственно относящиеся к расследуемому инциденту.

Следует сознавать, что не все виды цифровых носителей информации могут быть легко идентифицированы и локализованы, например, облачная обработка данных, NAS (Network Attached Storage, сетевая система хранения данных) и SAN (Storage Area Network, сеть с выделенной зоной хранения данных) добавляют виртуальный компонент к процессу идентификации.

Сбор. Сбор (изъятие) является одним из процессов обработки цифровых свидетельств, если устройства, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, перемещаются из их рабочей среды в лабораторию или иную контролируемую среду для последующего получения и анализа свидетельств.

Устройства, содержащие потенциальные свидетельства, представленные в цифровой форме, могут быть в одном из двух состояний: когда питание системы включено или когда питание системы выключено. Общие рекомендации заключаются в том, что если устройство включено, то не следует выключать его, а если устройство выключено, то не следует его включать.

Если устройство *включено*, до выключения системы следует рассмотреть вопрос получения изменчивых данных из цифрового устройства и его текущего состояния. Криптографические ключи и другие критические данные могут находиться в активной памяти или в неактивной памяти, которая еще не была очищена. При подозрении на шифрование следует рассмотреть вопрос *логического получения данных*. Если шифрование действительно имеет место, нужно помнить, что действующая серверная ОС может не заслуживать доверия, поэтому необходимо рассмотреть вопрос использования соответствующих надежных и утвержденных инструментальных средств.

Конфигурацией цифрового устройства может быть определено, нужно ли специалисту завершать работу устройства посредством обычных административных процедур или следует вынуть вилку кабеля электропитания устройства из розетки электропитания.

Цифровые устройства, содержащие потенциальные цифровые свидетельства, могут быть источником и физических свидетельств (например, отпечатки пальцев, ДНК и т.д.). Специалист должен проявлять осторожность, чтобы не испортить такие свидетельства, и координировать свои действия с соответствующими специалистами.

Процесс сбора включает документирование всех действий, а также упаковку устройств перед их транспортировкой.

Извлечение цифровых носителей информации не всегда рекомендовано, и специалист должен быть уверен в своей компетентности, должен осознавать необходимость и возможность выполнения этого действия.

Получение свидетельств. Процесс получения свидетельств включает создание цифровой копии свидетельств (например, физического диска, логического раздела диска или выбранных файлов), и документирование использованных методов и выполняемых действий.

Специалист должен выбрать надлежащий метод получения свидетельств, исходя из ситуации, затрат и времени, и документально оформить решение об использовании конкретного метода или инструментального средства. Если в результате процесса неизбежны изменения в цифровых данных, выполняемая деятельность должна быть задокументирована для учета изменений в данных.

В процессе получения свидетельств следует создавать *копию* потенциального цифрового свидетельства или цифровых устройств, которые могут содержать потенциальные свидетельства.

И оригинал, и копия свидетельства, представленного в цифровой форме, должны быть *верифицированы* с помощью проверенной функции верификации (например, криптографической хэш-функции), подтвержденной как точная на данный момент времени и являющейся приемлемой для лица, которое будет использовать свидетельства. И оригинал, и каждая копия свидетельства, представленного в цифровой форме, должны давать один и тот же результат при верификации.

Возможны обстоятельства, когда процесс верификации не может быть выполнен, например, при получении свидетельств в работающей системе, если оригинал содержит ошибки секторов или период получения свидетельств ограничен по времени. Если создание образа не может быть проверено, то это должно быть задокументировано и обосновано.

Если процесс верификации не может быть осуществлен для источника в целом, вследствие ошибок источника, то осуществляется верификация тех частей источника, которые могут быть надежно прочитаны.

Могут быть случаи, когда невозможно или недопустимо создание копии свидетельства, представленного в цифровой форме, например, когда источник слишком велик. Другой пример – критичные системы, не допускающие отключения. В таких случаях специалист должен осуществить *логическое получение* свидетельства, нацеленное только на определенные типы данных, директории или адреса. Такое копирование обычно происходит на уровне файлов и разделов диска. Во время логического получения свидетельства, в зависимости от используемого метода, могут быть скопированы только активные файлы и распределенное пространство цифрового носителя информации, а удаленные файлы или нераспределенное пространство могут не копироваться.

Специалист должен быть осмотрителен при использовании конкретного инструментального средства для сбора или получения потенциальных свидетельств, представленных в цифровой форме.

При оценке риска для свидетельств, представленных в цифровой форме, следует рассмотреть следующие аспекты (которые, однако не являются исчерпывающими):

- какой вид методов сбора/ получения свидетельств должен применяться?
- какое оборудование может потребоваться на месте?
- каков уровень изменчивости данных и информации, связанных с потенциальными свидетельствами, представленными в цифровой форме?
- возможен ли удаленный доступ к любому цифровому устройству и представляет ли это угрозу для целостности доказательств?
- что произойдет в случае повреждения данных/оборудования?
- могла ли произойти компрометация данных?
- могло ли цифровое устройство быть сконфигурировано так, чтобы вызвать разрушение (например, используя логическую бомбу), испортить или запутать данные в случае выключения или неконтролируемого доступа?

Сохранение. Процесс сохранения включает защиту потенциальных цифровых свидетельств и цифровых устройств, которые могут содержать потенциальные свидетельства, от фальсификации или повреждения. При наилучшем сценарии развития не должно быть никакого повреждения самих данных или любых связанных с ними метаданных (например, меток даты и времени).

3.6. Группа реагирования на инциденты

Цель создания группы реагирования на инциденты (IRT), согласно ISO/IEC 27035-2:2016, – предоставить организации возможности для оценки инцидентов ИБ, реагирования на них и извлечения уроков, а также обеспечения необходимой координации, управления, обратной связи и коммуникации. IRT также может выполнять превентивную роль, улучшая политики ИБ и практику обеспечения безопасности в организации, с тем чтобы уменьшить вероятность возникновения и смягчить последствия инцидентов.

IRT могут быть структурированы различными способами в зависимости от специфики конкретной организации (размера, квалификации сотрудников, отрасли). В зависимости от типа области мониторинга, IRT может быть организована как одиночная, иерархическая и удаленная. В случае *одиночной* IRT область мониторинга представляет собой единую организацию или единый центр контроля. *Иерархическая* IRT охватывает, как правило, несколько областей контроля, при этом группы, отвечающие за определенные логические или физические сегменты организации, под-

чинены единому центру. IRT *удаленного* типа собирает информацию о событиях безопасности из отдаленных местностей (удаленно), этот тип обычно используется в случае аутсорсинга управления инцидентами с привлечением специализированных предприятий (центров реагирования).

IRT могут существовать на постоянной основе или собираться в ответ на конкретный инцидент безопасности.

Основные виды деятельности IRT могут включать:

- управление интегрированными системами безопасности и контроль безопасности агентов, установленных в гетерогенных системах (IDS/IPS, межсетевой экран и т.д.);
- внедрение согласованной политики для минимизации рисков путем применения последовательного набора ответных задач;
- оперативное реагирование на угрозы, нарушения и атаки для снижения ущерба и стоимости восстановления.

Обязанности IRT могут также включать в себя следующие мероприятия по мониторингу и управлению:

- круглосуточное интегрированное управление и мониторинг (мониторинг целей, упреждающий мониторинг угроз и ответы на инциденты, управление журналами);
- управление отчетами по безопасности, управление исправлениями безопасности, отчеты об инцидентах;
- административное управление (управление политиками для различных сред);
- технический менеджмент: управление сетью, системой, приложениями, содержимым и безопасностью служб;
- управление системой: контроль и обеспечение пропускной способностью системы, производительностью, конфигурация безопасности и управление конфигурацией среды.

Для обозначения внутренней группы реагирования чаще используются термины CSIRT (Computer Security Incident Response Team) группа реагирования на инциденты компьютерной безопасности или SIRT (Security Incident Response Team) группа реагирования на инциденты безопасности – это конкретная организационная единица (один или несколько сотрудников), на которую возложена ответственность за координацию и поддержку реагирования на инциденты компьютерной безопасности. Часто CSIRT/SIRT работает только с внутренними инцидентами или инцидентами, направленными на внутренние информационные активы организации.

Еще одно название CERT (Computer Emergency Response Team) – компьютерная группа реагирования на чрезвычайные ситуации – является зарегистрированной торговой маркой Университета Карнеги-

Меллона (США) с 1997 года, использование этого названия для обозначения консалтинговых услуг или поставщика услуг безопасности необходимо получать официальное разрешение. Поэтому под CERT обычно подразумевается внешняя группа экспертов, оказывающих профессиональную поддержку в локализации инцидента, ликвидации последствий и расследовании хронологии распространения атаки. Кроме того, по мнению CERT/CC из Университета Карнеги-Меллона, CERT охватывает более широкую область мониторинга (в масштабах отрасли или даже страны), действуя как партнер с правительством, специалистами отрасли, правоохранительными органами и научными кругами в целях повышения безопасности и отказоустойчивости компьютерных систем и сетей. CERT занимается исследовательской деятельностью, изучает проблемы, которые имеют широкое значение для кибербезопасности, включая Threat Intelligence, и разрабатывает передовые методы и инструменты обеспечения ИБ.

Примерами групп CERT в России являются Центр реагирования на компьютерные инциденты в ИТС органов государственной власти РФ (GOV-CERT.RU), Центр оперативного реагирования на инциденты ИБ CERT-GIB, созданный компанией Group-IB; центры ГосСОПКА для субъектов КИИ.

Еще один термин, который часто можно услышать в контексте групп реагирования на инциденты – SOC (Security Operations Center) – центр обеспечения безопасности. SOC обычно строится вокруг SIEM системы, выполняет обнаружение инцидентов ИБ и аналитику событий. Тем не менее, сфера действия SOC шире и распространяется на другие области безопасности, в то время как CSIRT/SIRT и CERT фокусируются конкретно на реагировании на инциденты (рис. 5).

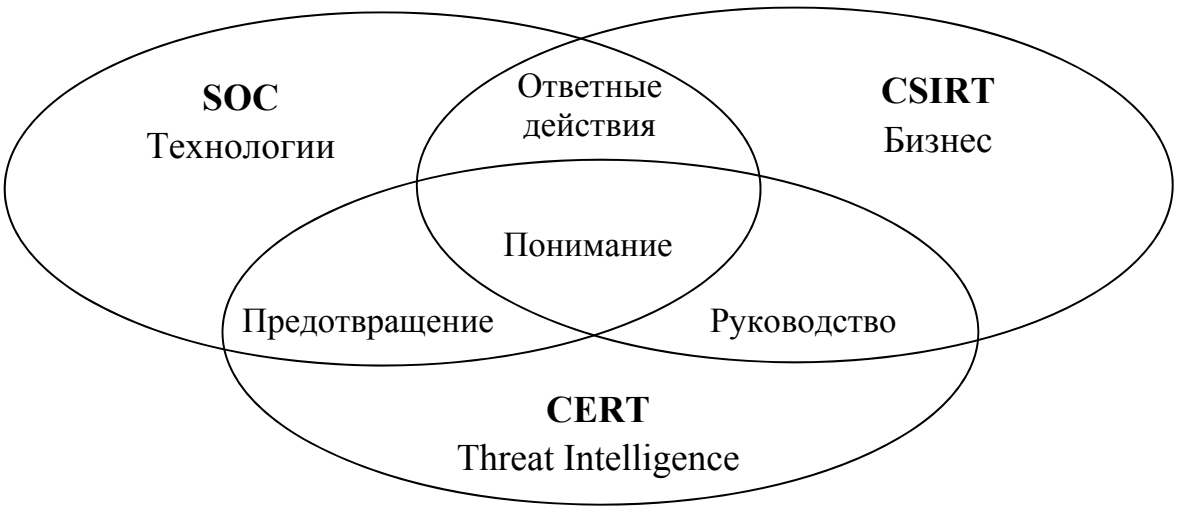

Рис. 5. Соотношение ролей CSIRT, CERT и SOC в обработке инцидента

Несмотря на то, что SOC часто встречается в контексте реагирования на инциденты, он почти всегда имеет и другие элементы безопасности в пределах своей ответственности. Выполняемый SOC мониторинг не ограничивается реагированием на инциденты, например, SOC может собирать метрики для предоставления услуг безопасности, поддержки управленческой отчетности, оценки рисков или аудита. Реакция на инцидент, чаще всего, входит в компетенцию SOC как функция оперативной безопасности.

Развертывание SOC имеет преимущества, если необходимость мониторинга имеет первостепенное значение, а организационная структура способствует централизации операций безопасности в одном физическом или логическом месте. Если же организационная структура более децентрализована, создание CSIRT может иметь больше смысла.

ГЛАВА 4. МЕТОДЫ И СРЕДСТВА ИССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

4.1. Выявление элементов инфраструктуры, затронутых инцидентом

Локализация инцидента ИБ невозможна без определения того, какая часть информационной инфраструктуры организации затронута инцидентом. Увеличение масштабов систем, рост объема обрабатываемой, передаваемой и хранимой информации делает нецелесообразным (а в ряде случаев, и практически неосуществимым) тотальное снятие информации и криминалистическое исследование всех элементов ИС организации. Кроме того, элементы информационной инфраструктуры могут быть задействованы в критически важных бизнес-процессах и не могут быть отключены без дополнительных затрат по миграции данных или потери производительности. Поэтому на первоначальном этапе расследования инцидента ИБ очень важно выявить скомпрометированные хосты и другие элементы ИС для их дальнейшего изолирования и детального исследования.

На основе первичной информации о выявленном или предполагаемом инциденте ИБ можно определить *характерные признаки компрометации* – имеющие определенное состояние свойства и измеряемые события безопасности, связанные с работой компьютеров и сетей. Примерами характерных признаков компрометации являются информация о файле (название, хэш-значение, размер, сигнатура и т.п.), значение ключа системного реестра, запуск службы, отправка HTTP-запроса.

Признаки компрометации могут быть разделены на хостовые, сетевые и социальные. К *сетевым* признакам компрометации относятся доменные имена, URL, почтовые адреса, совокупность IP-адресов и портов. *Хостовые* признаки компрометации – это запущенные процессы, изменения веток реестра и файлов, хэш-значения и сигнатуры вредоносного ПО. Социальные признаки компрометации формируются на основе данных СКУД или видеонаблюдения (например, нахождение в определенном помещении в конкретный временной промежуток).

Формализация признаков компрометации в контексте рассматриваемого инцидента ИБ и средств детектирования позволяет сформировать *индикаторы компрометации* (IoC, Indicator of Compromise) – конструкции, используемые для описания характерных признаков компрометации в совокупности с контекстной информацией (рис. 6).

Индикатор может включать один или несколько характерных признаков в контексте потенциально возможных инструментов, тактик и процедур обнаружения, а также ряд сопутствующих метаданных, например, степень уверенности в индикаторе (вес индикатора), ограничения по об-

работке, подтвержденные временные окна, возможный негативный эффект, необходимые для обнаружения механизмы тестирования структуры, оптимальный порядок действий, источник индикатора и т.п.

```
<IndicatorItem id="09cd0494-702c-4fe2-bbd4-29538cb3b685" condition="contains">
        <Context document="FileItem" search="FileItem/StringList/string" type="mir" />
        <Content type="string">http://%s/record.asp?device_t=%s</Content>
        <Comment>unique strings found in most samples in family</Comment>
</IndicatorItem>
```

Рис. 6. Пример индикатора компрометации в формате OpenIOC

Можно сказать, что *индикатор компрометации* – это описание данных об угрозе для автоматизированного анализа специализированными программными средствами элементов информационной инфраструктуры и детектирования инцидента ИБ.

Обнаружение сетевых признаков компрометации (например, однократное обращение к IP-адресу потенциально опасного хоста по не специфичному порту) обычно еще не является однозначным свидетельством инцидента ИБ, а детектирование хостовых индикаторов (например, запуск файла, хэш-сумма которого совпадает с хэш-суммой вредоносного файла), как правило, говорит об успешности атаки.

Индикаторы компрометации могут использоваться для настройки IDS/IPS, SIEM систем и систем класса Endpoint Detection and Response (EDR). Кроме того, поиск объектов в файловой системе и реестре скомпрометированных хостов в сетевой инфраструктуре может осуществляться с помощью Power Shell скриптов, для поиска объектов в оперативной памяти могут использоваться YARA анализаторы (https://github.com/virustotal/yara). Наряду с многочисленными коммерческими решениями существуют программные инструменты с открытым кодом, позволяющие получать и работать с индикаторами компрометации, например, проект GOSINT от Cisco (https://github.com/ciscocsirt/GOSINT), автоматизирующий сбор, обработку и экспорт высококачественных индикаторов компрометации, и простой сканер Loki (https://github.com/lukaszbb/Loki), включенный в Kali Linux.

Loki Поддерживает следующие типы индикаторов: хэш-значения, YARA правила (применяются к содержимому файла и памяти процесса), имена файлов с использованием регулярных выражений. Loki заимствует некоторые из наиболее эффективных правил из наборов правил полнофункционального сканера Thor APT от компании Nextron Systems. База данных сигнатур IoC доступна для редактирования, что позволяет добавлять свои собственные индикаторы.

Инструмент YARA (https://github.com/virustotal/yara) также включен в Kali Linux (имеется и Windows реализация), он позволяет проверять содержимое файлов на диске (конкретный файл или все файлы в заданном каталоге) или сканировать процессы в оперативной памяти (или ее дампе) на соответствие заданным сигнатурам. Сигнатура может представлять собой фрагмент текста или шестнадцатеричного кода с использованием регулярных выражений. YARA правила описывают также и логику применения сигнатур. В качестве условия можно использовать размер файла (не может быть применено к исполняемому процессу). Можно указывать определенное смещение в файле или адресном пространстве процесса, в том числе, и виде диапазона.

Например, представленному на рис. 6 индикатору компрометации соответствует следующее YARA правило:

```
rule Indicator_09cd0494_702c_4fe2_bbd4_29538cb3b685
{
strings:
    $a = "http://%s/record.asp?device_t=%s"
condition:
    $a
}
```

Существуют инструменты для автоматического перевода в YARA правила IoC, описывающих содержимое файла, а также баз некоторых антивирусных средств (например, ClamAV).

Другой пример YARA правила описывает pdf файл, содержащий веб ссылки:

```
rule pdf_link {
meta:
    description = "A PDFv1.7 that contains a link or
external content"
strings:
    $pdf_magic = {25 50 44 46}
    $s_tag_a = "<a " nocase ascii wide
    $s_url = /\(http.+\)/ nocase ascii wide
condition:
    $pdf_magic at 0 and any of ($s*)
}
```

Секция string правила описывает тестовые или бинарные значения, или шаблоны значений, а секция condition – логическое правило их комбинации. В этом правиле строка `$pdf_magic` содержит бинарный код, характерный для файлов формата pdf (сигнатуру или «магическое число», определяющее данный формат). Строка `$s_tag_a` содержит начало записи html тэга ссылки на случай, если документ был преобразован из веб страницы. При этом будет осуществляться поиск текста без учета регистра

символов как в ASCII кодировке, так и в кодировке 2 байта на один символ. Строка `$s_url` – регулярное выражение, обозначающее любой адрес, начинающийся с http и заключенный в круглые скобки (что соответствует стандарту PDF для записи активных ссылок и URL в формах).

Условие в секции condition рассматривает только файлы, начинающиеся с «магического числа» pdf формата, а также требует одновременного выполнения хотя бы одного из условий, описанных переменными, начинающимися на s (то есть наличие тэга ссылки или URL в документе).

YARA правила записываются в файл, который указывается при вызове сканирования. YARA широко используются поставщиками антивирусных решений и чаще всего используются именно для детектирования вредоносного ПО.

Работа с индикаторами компрометации представляет собой итерационный процесс. Собранные начальные данные об инциденте позволяет выявленных некоторые признаки атаки и сгенерировать первичные индикаторы компрометации. После того, как затронутые инцидентом узлы информационной инфраструктуры выявлены, они подвергаются более глубокому анализу в процессе криминалистического исследования. Это, в свою очередь позволяет сформировать новые индикаторы компрометации и провести более точное сканирование инфраструктуры, а также выявить факты повторного заражения.

4.2. Криминалистические исследования компьютерных систем

Ход конкретного расследования произошедшего инцидента ИБ или правонарушения в компьютерной сфере во многом определяется спецификой конкретного дела. Однако можно выделить некоторые общие подходы, изложенные, например, в рамках методологии сетевой криминалистики (OSCAR), включающей следующие основные этапы [17]:

- *получение информации* об инциденте (включая временные рамки произошедшего, вовлеченные персонал и системы), технической и организационной среде (Obtain);
- выработка *стратегии* расследования – оценка своих ресурсов и планирование расследования, включая определение вероятных источников свидетельств и приоритета их сбора (Strategize);
- *сбор* запланированных свидетельств, включающий документирование всех производимых действий, снятие данных, обеспечение неизменности свидетельств в процессе сбора и хранения (Collect);
- *анализ* – основная фаза работы с данными для восстановления картины произошедшего, является итерационной, так как может потре-

бовать сбора дополнительных свидетельств и расширения области анализа (Analyze);

– *отчет*, основанный на фактах, обоснованно детализированный и понятный нетехническим специалистам (Report).

В общих чертах действия аналитиков в ходе расследования выглядят следующим образом:

– выдвигаются начальные версии, объясняющие причины возникновения инцидента и возможный сценарий его развития;
– версии ранжируются по приоритету, на основе статистики прошлых инцидентов, исходя из критичности инцидента или системы, а также на базе собственного опыта аналитика;
– в порядке убывания приоритета каждая версия прорабатывается, производится поиск доказывающих или опровергающих ее фактов на основе собранных свидетельств.

Не существует единого подхода к проведению расследований. Место компьютерного правонарушения или инцидента безопасности представляет собой цифровое окружение, создаваемое программами и оборудованием. Процесс анализа этого места включает этапы консервации системы, поиска улик и реконструкции событий [12]. Расследование событий в компьютерных системах невозможно без глубокого понимания технических аспектов их работы и криминалистического исследования, подразумевающего анализ текущего состояния системы или ее ретроспективный анализ.

Если расследование обычно касается подозреваемых лиц и их действий, то криминалистическое исследование рассматривает только технические аспекты функционирования компьютерных систем. Например, проводящий исследование криминалист может установить IP-адрес атакующего или IP-адрес сервера управления и контроля (C&C) или, в некоторых случаях, профиль атакующего. Связь между установленной характеристикой компьютерной системы и субъектом (например, связь между IP-адресом компьютера и его пользователем, адресом e-mail и его владельцем) устанавливается только в ходе расследования.

В отличие от компьютерной экспертизы, назначаемой в рамках судопроизводства постановлением следователя, криминалистическое исследование можно инициировать самостоятельно или провести по запросу правоохранительных органов до возбуждения дела. Его результаты могут лечь в основу внутреннего расследования или, оформленные в виде официальной Справки об исследовании, представлены в качестве доказательств в гражданских, административных и уголовных делах. Криминалистическое исследование может быть инициировано одной из сторон процесса или правоохранительными органами в рамках оперативно-

розыскных мероприятий. Документ, отражающий ход и результаты исследования, не являющегося частью судебной экспертизы, может называться заключением специалиста, справкой специалиста, справкой эксперта, актом об исследовании.

Компьютерная или цифровая криминалистика (форензика, forensics) – это практика исследования компьютерных систем, цифровых носителей и цифровых систем телекоммуникаций на предмет поиска возможных артефактов. Слово артефакт здесь указывает на любой интересующий объект. Термин «доказательство» является юридическим понятием, и, как правило, не употребляется если артефакт фактически не будет представлен как часть судебного дела. Стандарты управления инцидентами используют вместо него слово «свидетельство», а компьютерная криминалистика – «артефакт». Можно сказать, что артефакт является потенциальным доказательством. Цифровые доказательства – это совокупность цифровых артефактов, обнаруженных на целевом вычислительном устройстве, которые могут использоваться в качестве доказательств в суде.

Криминалистическое исследование позволяет зафиксировать цифровые следы инцидента ИБ или совершения правонарушения. Исследование позволяет установить хронологию инцидента, возможные причины его возникновения, в том числе степень участия внутренних сотрудников, а также получить широкий спектр данных для дальнейшего расследования (IP-адреса, доменные имена, адреса электронной почты, идентификаторы мессенджеров нарушителей и т.п.). Целью цифровой криминалистики является проведение структурированного исследования при сохранении целостности свидетельств и документированной цепочки их хранения, чтобы составить как можно более полное и точное представление о картине произошедшего.

Процесс криминалистического исследования компьютерных систем включает в ряд типовых шагов:

- идентификация (получение информации об инциденте, определение скомпрометированных цифровых устройств и наилучших источников потенциальных цифровых доказательств);
- изъятие цифровых носителей, связанных с расследованием;
- создание образов (копий) изъятых носителей информации;
- верификация неизменности свидетельств в процессе сбора (расчет хэш-значений);
- анализ – поиск артефактов, которые могут подтвердить или опровергнуть поставленные расследованием вопросы, в ходе анализа должна обеспечиваться неизменность цифровых свидетельств);
- формирование отчета, содержащего сделанные в ходе анализа выводы;

– сохранение (защита собранных свидетельств их от любых изменений или удаления).

В сфере цифровой криминалистики (форензики) можно выделить несколько более узких направлений в соответствии с источником полученных цифровых свидетельств.

Компьютерная криминалистика (computer forensics) – самый старый тип цифровой криминалистики, занимается исследованием цифровых свидетельств и поиском артефактов на настольных компьютерах, ноутбуках, цифровых запоминающих устройствах (HDD, SSD, флэш-накопители и SD-карты) и в оперативной памяти (RAM), а также поиском следов в системных данных ОС (реестре, журналах) и установленных приложениях. В рамках этого направления выполняется восстановление и анализ удаленных данных из хранилища целевого устройства.

Сетевая криминалистика (network forensics) – этот тип криминалистических исследований связан с мониторингом и анализом потока трафика в компьютерных сетях для извлечения компрометирующих доказательств (например, обнаружения источника атак безопасности) или для обнаружения вторжений.

Криминалистический анализ данных (forensic data analysis) – этот раздел занимается анализом файлов, структур данных и бинарных последовательностей на предмет выявления несанкционированных действий или воспроизведения сценария атаки.

Мобильная криминалистика (mobile device forensics) занимается извлечением артефактов с мобильных устройств (телефонов, смартфонов, планшетов и других носимых устройств, таких как умные часы или фитнес браслеты). Такие устройства обычно учитывают местоположение, что означает, что они имеют встроенные системы позиционирования (GPS или аналогичные).

Криминалистика аппаратных устройств (hardware forensics) – анализ аппаратного обеспечения и технических устройств. Это направление наиболее сложно и предполагает разбор данных на низком уровне (микроконтроллера, прошивки или BIOS), исследование специфических особенностей работы устройства.

Существуют и другие виды цифровой криминалистики, такие как криминалистика электронной почты, криминалистика облачных хранилищ, криминалистика конкретных приложений (например, криминалистика веб браузера), криминалистика файловых систем, криминалистика мультимедиа (текст аудио, видео и изображений) и др. Эти отдельные узкие направления подпадают под уже упомянутые основные типы. Иерархия видов криминалистического анализа, основанная на архитектуре данных компьютерных систем [12] представлена на рис. 7.

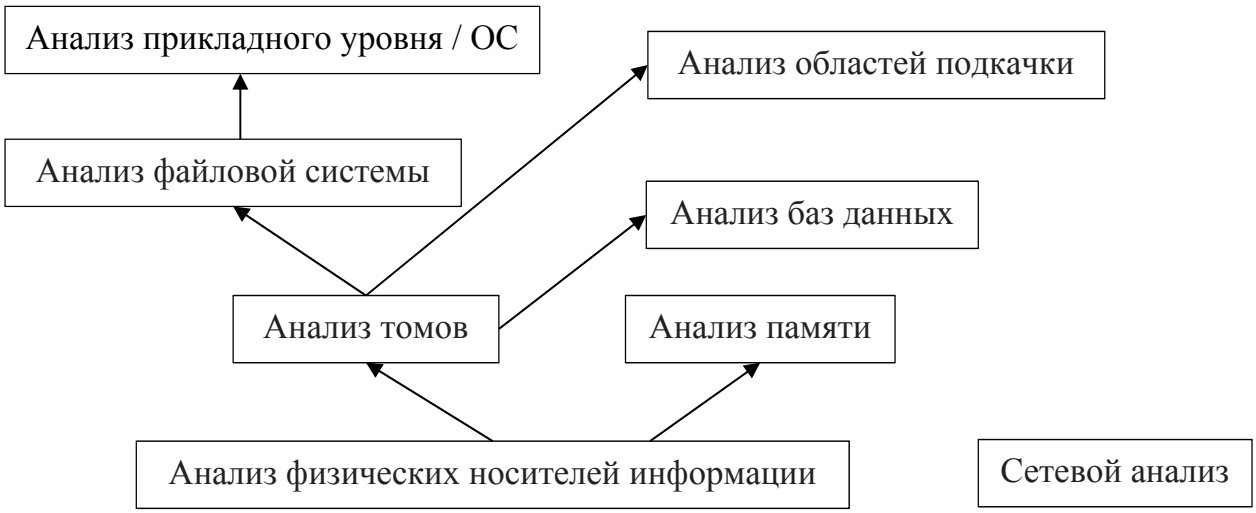

Рис. 7. Иерархия видов криминалистического анализа

На нижних уровнях архитектуры можно рассмотреть две области независимого анализа, основанных на устройствах хранения информации (HDD, SSD, CD/DVD диски) и на устройствах обмена данными.

Различают два основных подхода к проведению криминалистического анализа компьютерных систем:

- анализ работающей системы в режиме реального времени («живой» анализ);
- ретроспективный («посмертный» или «мертвый») анализ, когда криминалист получает все доступные данные с места происшествия, а затем проводит анализ свидетельств.

В каждом конкретном случае может быть отдано предпочтение тому или иному подходу, но, как правило, их комбинация дает наилучший результат, так как может наиболее четко объяснить состояние исследуемой системы. В этом случае сначала проводится живой анализ включенных и доступных систем, его результаты записываются и затем проводится «посмертный» анализ всех полученных данных, включая живые.

Существует ряд проблем, вызванных, прежде всего, быстрым развитием и разнообразием информационных технологий и цифровых устройств, так и совершенствованием технологий защиты (многие из которых к тому же активно берутся на вооружение нарушителями для противодействия возможным расследованиям):

- шифрование;
- облачное хранение данных;
- рост объемов данных;
- рост числа технологических интеллектуальных устройств;
- рост количества правонарушений в компьютерной сфере;
- технологические особенности SSD накопителей.

Кроме того, существуют проблемы организационного и юридического плана, касающиеся вопросов юрисдикции, обеспечения конфиденциальности, нехватки квалифицированных специалистов и ресурсов для обеспечения непрерывного обучения, координации и отсутствия стандартизированного международного законодательства при проведении трансграничных расследований.

4.3. Инструменты снятия данных

Создание образа носителя информации

Основным направлением компьютерной криминалистики является исследование цифровых носителей информации. Чтобы гарантировать неизменность информации, а также оставить возможность проведения повторной или дополнительной экспертизы, исследовать оригинал носителя нежелательно, все исследования проводят с его копией. Копирование может быть проведено во время следственного действия вместо изъятия оригинального носителя. В этом случае ее также оставляют неизменной в качестве мастер-копии, а исследования проводят над снятой с нее рабочей копией. Созданная копия должна побитово соответствовать исследуемому носителю.

Существуют различные варианты копирования информации с оригинального носителя (рис. 8):

- создание полного образа (клонирование физического диска);
- создание частичного образа (копирование раздела);
- создание логического образа (копирование на уровне файловой системы).

В случае создания полного образа, копия будет содержать не только живые файлы, но и служебные данные, свободные области файловых систем, скрытые и неразмеченные области диска [12]. Криминалист должен максимально увеличить количество данных, сохраняемых путем сбора и получения свидетельств (ГОСТ Р ИСО/МЭК 27037-2014), поэтому, как правило, создается полная копия клонированием физического диска. Однако оптимальный выбор варианта копирования информации обусловлен обстоятельствами конкретного дела. Логическое копирование может быть целесообразно, если целевой диск слишком велик, и точно известно, какие данные с него требуются (например, если необходимо получить только файлы журналов с серверного диска или RAID хранилища).

Посекторное копирование (клонирование) может осуществляться на *другой носитель* информации (такого же или большего размера) или *в файл образа* или раздел на другом носителе. Копирование «носитель на

носитель» можно произвести с помощью специальных аппаратных устройств (дубликаторов дисков) либо программно (например, с помощью команды dd в ОС Linux). Копирование «носитель в файл» (создание образа диска) производится с помощью специализированного ПО.

Рис. 8. Варианты копирования данных с носителя информации

При использовании *аппаратных дубликаторов* диска оригинальный носитель информации должен быть извлечен из устройства, где он использовался, и подключен к дубликатору с помощью соответствующего интерфейса. Наибольшей известностью пользуются дубликаторы производства Tableau и Guidance Software Inc. Клонирование дисков с помощью аппаратных устройств обеспечивает полную автономность и отличается высокой скоростью, однако такие решения недешевы.

При использовании программных решений возможны два режима копирования, условно называемых «живым» и «мертвым» снятием данных.

Живое снятие данных означает, что ОС на анализируемом устройстве продолжает работать и используется для копирования данных. Живое снятие данных всегда сопряжено с определенным риском, так как в ОС или другое ПО могли быть внесены изменения, поэтому нельзя гарантировать, что во время клонирования носителя поставляются верные данные. Например, такой тип вредоносного ПО, как руткиты, поставляют ложную информацию – как правило, они скрывают некоторые файлы в каталогах или работающие процессы. Чаще всего речь идет о файлах, установленных нарушителем после взлома системы. Также существует возможность модификации ОС таким образом, чтобы она автоматически подменяла данные в некоторых секторах диска. В таком случае полученный образ диска не будет отражать информацию об инциденте. Поэтому живого снятия данных, по возможности, избегают.

При *мертвом* снятии данных копирование носителя производится без содействия установленной на компьютере системы, работа ведется в доверенной ОС. Получение образа носителя без загрузки хостовой ОС может производиться в режиме Live CD. Загрузка происходит с надежного компакт-диска или загрузочного флэш-накопителя, при этом возможно использование оборудования исходного компьютера. Запуск ОС с Live CD позволяет делать копию исследуемого носителя без его извлечения. При загрузке с Live CD для мертвого снятия данных существует техническая возможность изменения оборудования так, чтобы оно возвращало ложные данные даже в надежной ОС, однако этот вариант гораздо сложнее реализуем и менее вероятен, чем модификация хостовой ОС.

Чаще всего носитель все же извлекается из устройства и клонирование происходит на лабораторном стенде (компьютере эксперта).

Средство клонирования/ копирование носителя должно удовлетворять следующим требованиям:

- создавать посекторную копию;
- обрабатывать ошибки чтения оригинального носителя;
- не вносить никаких изменений в оригинальный носитель;
- вести журнал дублирования.

Причины ошибок могут быть весьма различными – как отказ всего диска, так и сбои в ограниченном количестве секторов. При этом попытки прочитать сбойный сектор могут ухудшить состояние поврежденного магнитного диска. Общепринятым способом обработки ошибок чтения поврежденных секторов является сохранение адреса сектора и запись нулей вместо данных, которые не могут быть считаны с диска. Запись нулей позволяет сохранить правильное местоположение других данных.

Для гарантии тождественности копии или образа диска после копирования следует произвести верификацию. Верификация производится расчетом хэш-значений (например, SHA-256) оригинального носителя и копии с последующим их сравнением. Совпадение значений гарантирует побитовое совпадение копии с оригиналом. Однако, если в ходе чтения исходного носителя возникают ошибки, полученные хэш-коды могут не совпадать. Это обстоятельство требует ведения журнала дублирования для документирования возможных ошибок чтения в отчете о расследовании.

Еще одна проблема – обеспечение неизменности (целостности) исходного носителя. При подключении носителя информации к обычной ОС, как правило, производится автоматическое монтирование файловых систем и изменение его содержимого. Например, ОС Windows, создает скрытые папки Корзины, сохраняет информацию о конфигурации и, в некоторых случаях, обновляет временные метки в атрибутах файлов.

Для обеспечения целостности исследуемого носителя информации его следует подключать через *аппаратный блокиратор записи* (bridge) или использовать программные методы блокирования. Например, в ОС Windows, может быть заблокирована запись в USB-порт установкой значения «WriteProtect»=dword:00000001 для ветки реестра [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies].

В ОС Windows 7/10 данные ключи в реестре по умолчанию отсутствуют и их необходимо создавать вручную. Предпочтительно использовать настройку с помощью шаблонов безопасности, включив политику Конфигурация компьютера/Административные шаблоны/ Система / Доступ к съемным запоминающим устройствам / Съемные диски: запретить запись. Блокировка записи в USB-порт может производиться и с помощью специального ПО.

В случае использования Linux-систем выбирают криминалистические сборки (forensics mode) с запретом автоматического монтирования подключаемых дисков, разделы физических или виртуальных дисков монтируются с опцией read only (-o ro), а файлы образов – дополнительно в режиме петлевого устройства (loop).

Создание полной копии диска или копии раздела при использовании Linux системы может быть осуществлено командой dd, а расчет хэш-значений – командой sha256sum. Более развитая утилита dc3dd, включенная в Kali Linux, позволяет рассчитывать хэш-значения «на лету» (одновременно с копированием), ведет журнал ошибок чтения и позволяет разделить образ на файлы заданного размера. При записи копии в файл, образ создается в raw формате (без сжатия), поэтому размер образа будет совпадать с размером исходного носителя. Копирование может производиться также с помощью утилиты Guymager (включена в Kali Linux), имеющей графический интерфейс и позволяющей создавать образы в признанном экспертами формате E01 (или EWF, Encase Image file Format) со сжатием, разбивать образ на части и производить расчет хэш-значений.

В ОС Windows для получения образа диска может использоваться специальное криминалистическое ПО, например, FTK Imager от компании AccessData (имеется реализация для MacOS), или некоторые программы управления дисками (например, Acronis или Paragon Hard Disk Manager). Криминалистическое ПО позволяет создавать образы в формате E01, задавая произвольную степень сжатия, разбивать образ на фрагменты нужного размера и проводить контроль целостности.

Снятые образы можно монтировать на реальной или виртуальной системе, или исследовать с помощью специализированного криминалистического ПО (например, Autopsy, Belkasoft Evidence Center, AccessData Forensic Toolkit (FTK), EnCase Forensic от Guidance Software, X-Ways Forensics) или ПО для восстановления данных (например, R-Studio).

Снятие энергозависимых данных

Энергозависимые данные безвозвратно теряются при выключении питания или перезагрузке устройства, к ним относятся содержимое оперативной памяти, сетевого трафика, временные сетевые журналы, файлы гибернации и подкачки. Такие данные также могут быть перезаписаны при обычном использовании вычислительного устройства (например, при закрытии определенного приложения на компьютере зарезервированное им пространство данных исчезнет из оперативной памяти, что позволит другим приложениям использовать это пространство для своей работы).

Существует множество цифровых артефактов, которые находятся только в *оперативной памяти*, без записи на жесткий диск. Например, оперативная память ОС Windows может содержать:

- перечень запущенных процессов;
- сведения о сетевых соединениях;
- содержимое буфера обмена;
- список выполненных консольных команд;
- открытые/ активные ключи реестра;
- пароли учетных записей Интернета (электронной почты, социальных сетей и облачных хранилищ);
- расшифрованные файлы;
- ключи шифрования;
- последние сообщения в мессенджерах и чатах;
- журналы просмотра веб страниц;
- вредоносный код.

Процесс захвата данных из энергозависимой памяти известен как снятие *дампа памяти*, способы его получения зависят от типа ОС. При запуске утилиты снятия дампа, содержимое оперативной памяти неизбежно меняется, и некоторые данные могут быть перезаписаны. Поэтому предпочтительно использование утилит, занимающих немного места в оперативной памяти и не требующих установки.

Для получения дампа оперативной памяти в ОС Windows могут использоваться бесплатные утилиты AccessData FTK Imager Lite, Belkasoft Live RAM Capturer, Memoryze от компании FireEye, Magnet RAM Capture, DumpIt от Comae Technologies, WinPmem из проекта Recall (https://github.com/google/rekall/releases).

Большинство программных средств, используемых для захвата оперативной памяти, должны быть запущены с правами администратора. Это необходимо для обхода активных систем противодействия отладке, способных обнаружить и предотвратить попытку других программ считать данные из защищенных областей памяти, что требует от инструмента захвата работы в привилегированном режиме ядра ОС.

При необходимости получения дампа с работающего компьютера с ограниченными правами пользователя можно воспользоваться аппаратным инструментом сбора (на целевой компьютер потребуется установить небольшой драйвер), однако такие решения недешевы.

Для снятия дампа памяти в ОС компании Apple (MacOS) могут использоваться бесплатные утилиты Mac Memory Reader от компании Demisto, Mandiant's Memoryze от компании FireEye, Recall (https://github.com/google/rekall-profiles) и Volafox (https://github.com/n0fate/ volafox).

Для ОС Linux доступно использование LiME – Linux Memory Extractor (https://github.com/504ensicslabs/lime) или fmem (https://github.com/ NateBrune/fmem), реализованных в виде модулей ядра, утилит lmap и pmem из проекта Rekall (https://github.com/google/rekall/tree/master/tools/linux/lmap и https://github.com/google/rekall/tree/master/tools/pmem) либо не требующего установки скрипта Linux Memory Grabber (https://github.com/halpomeranz/lmg/).

Анализ полученного дампа оперативной памяти может быть произведен с помощью программ Rekall (https://github.com/google/rekall) или Volatility (https://github.com/volatilityfoundation/volatility). Для поиска и просмотра артефактов из дампа оперативной памяти могут использоваться и специальные криминалистические программные комплексы, такие как Belkasoft Evidence Center, AccessData Forensic Toolkit (FTK), EnCase Forensic от Guidance Software и др.

Под короткоживущими данными понимают не только содержимое оперативной памяти, но и другие системные данные. Для их получения могут быть использованы инструменты командной строки Windows и Linux систем, приведенные в табл. 2.

Таблица 2. Команды для получения системной информации

Назначение	Windows	Linux/ Unix
текущая сетевая конфигурация и открытые сетевые соединения	ipconfig, arp, route, net, netstat	ifconfig, arp, route, netstat
активные процессы	pslist	ps, top
открытые (используемые) файлы	openfiles	lsof
вошедшие в систему пользователи	quser	w, last
отображение системного времени	date, time	date

Исследование полного трафика или его статистики возможна только с помощью сторонних программ – снифферов. Такие инструменты можно использовать для криминалистического анализа в качестве пассивного сетевого анализатора, чтобы просматривать проходящий по сети трафик в

режиме реального времени, обнаруживать операционные системы, сеансы, имена хостов, открытые порты и прочее. Одним из наиболее популярных в мире и широко используемых анализаторов сетевых протоколов является Wireshark, доступный как для Windows, так и для Linux систем. NetworkMiner –пассивный анализатор трафика для ОС Windows, имеющий функцию перехвата и сохранения файлов, изображений, сообщений, переданных за время работы сниффера. Еще один широко известный анализатор трафика – TCPDump для Linux систем (WinDump – аналог для Windows), в Linux системах также может быть использована утилита TCPFlow, и RawCap – для Windows.

4.4. Инструменты криминалистического анализа компьютерных систем

Выбор используемых в ходе криминалистического исследования инструментов остается за проводящем его специалистом, этот выбор, криминалист должен быть готов обосновать в суде. Возможно использование лицензионного проприетарного ПО, либо общедоступного свободно распространяемого ПО с открытым кодом. Нелицензионные (взломанные) версии ПО не могут использоваться, так как это означает внесение неконтролируемых изменений, что не гарантируется корректность работы криминалистических инструментов и достоверность полученных результатов.

Инструменты криминалистического анализа компьютерных систем не являются средствами защиты информации, поэтому не требуют обязательной сертификации ФСТЭК или ФСБ. Для государственных лабораторий компьютерно-технической экспертизы существует список необходимого оснащения, включающий как программные, так и аппаратные инструменты[10].

Выбор криминалистического ПО зависит и от объема проводимых исследований. Если речь идет о крупной криминалистической лаборатории, действующей в масштабах страны и требующей обеспечения удаленного взаимодействия всех сторон расследования, координации совместной работы над делом нескольких экспертов, не обойтись без интегрирующих платформ, таких как AccessData AD Lab или Quin-C. Предпочтение, скорее всего, будет отдаваться коммерческим комплексным инструментам, автоматизирующим процесс анализа разнородных свидетельств и генера-

[10] Приказ Министерства юстиции РФ от 26 ноября 2015 г. № 269 «Об утверждении Требований к минимальной комплектации материально-технической базы по каждому виду судебных экспертиз, проводимых в федеральных бюджетных судебно-экспертных учреждениях Министерства юстиции Российской Федерации».

ции отчетности. В этом классе инструментов преобладает проприетарное ПО:

- EnCase Forensic (https://www.guidancesoftware.com/) – общепризнанный криминалистический инструмент от компании Guidance Software, поддерживающий полный цикл исследования от сбора свидетельств до формирования отчетов, поддерживает работу с зашифрованными носителями и мобильными платформами, используется Интерполом и правоохранительными органами многих стран;
- Belkasoft Evidence Center (https://belkasoft.com/ru/ec) – российский криминалистический инструмент;
- AccessData Forensic Toolkit (FTK) (https://accessdata.com/) – криминалистический инструмент, использующий распределенную обработку данных, ускоряя тем самым поиск артефактов;
- X-Ways Forensics (http://www.x-ways.net/forensics/) – немецкий криминалистический продукт с невысокими требованиями к аппаратному обеспечению.

Проприетарное ПО, как правило, предназначено для работы в ОС Windows, имеют удобный графический интерфейс, отличаются стабильными выпусками и наличием технической поддержки, имеют различные опции поставки и т.д. Однако коммерческие инструменты имеют ограничения, поскольку они достаточно дорогостоящи и, как правило, поставляются с лицензиями с ограниченным сроком действия.

Из-за высокой стоимости коммерческих криминалистических продуктов многие эксперты предпочитают использовать инструменты с открытым кодом. Лишь некоторые из этих инструментов обладают широким набором функций, похожих на коммерческие (например, Autopsy), в то время как большинство представляют собой небольшие утилиты, созданные для выполнения какой-то одной определенной функции (например, извлечение истории браузера или извлечение информации заголовка электронной почты). Большинство из них реализованы для работы в среде ОС Linux, но некоторые (например, Autopsy, Volatility) портированы на Windows. Наиболее известные криминалистические инструменты с открытым кодом:

- набор инструментов командной строки The Sleuth Kit для анализа носителей информации и их образов (Linux), Autopsy – графическая оболочка для Windows-реализации (www.sleuthkit.org);
- Volatility (https://www.volatilityfoundation.org/) – кроссплатформенный инструмент для анализа образов оперативной памяти (RAM);
- Mandiant Redline (https://www.fireeye.com/services/freeware.html) – инструмент анализа живой памяти на наличие признаков вредоносной активности;

- Memoryze для создания образов RAM, анализа образов и живой памяти (https://www.fireeye.com/services/freeware.html);
- AccessData FTK Imager и FTK Imager Lite – средство просмотра дисков и создания образов носителей информации и оперативной памяти (https://accessdata.com/product-download);
- утилиты для захвата оперативной памяти Magnet Process Capture и памяти отдельного процесса Magnet Process Capture (https://www.magnetforensics.com/resources/?cat=Free%20Tool);
- Encrypted Disk Detector – утилита проверки наличия зашифрованных томов (https://www.magnetforensics.com/resources/?cat=Free%20Tool);
- Bulk Extractor (Linux) – утилита извлечения полезной информации (адреса электронной почты, номера кредитных карт, URL-адреса и др.) из образов жесткого диска, файлов или каталогов файлов (http://downloads.digitalcorpora.org/downloads/bulk_extractor/).

Популярные средства с открытым кодом объединены в рамках специализированных Linux дистрибутивов, предварительно сконфигурированных для целей компьютерной криминалистики. Они загружаются в режиме Live CD (или с USB-накопителя) и не монтируют подключаемые тома в автоматическом режиме. При загрузке ОС с таких дистрибутивов для криминалистических нужд основным критерием является гарантия блокировки записи на монтируемые устройства. К сожалению, не все дистрибутивы вполне корректны в этом плане, например, может перезаписываться служебная информация на томах с журналируемыми файловыми системами. К наиболее известным криминалистическим Linux-сборкам относятся:

- CAINE (Computer Aided INvestigative Environment) на базе Ubuntu с широким спектром предустановленных утилит для анализа Linux и Windows систем и частичной автоматизацией типовых сценариев анализа (https://www.caine-live.net/);
- DEFT (Digital Evidence & Forensic Toolkit) на базе Ubuntu (http://www.deftlinux.net);
- Kali Linux Forensic mode на базе Debian (https://www.kali.org/);
- Parrot OS Forensic mode на базе Debian (https://parrotlinux.org/).

Поскольку во время запуска Live□дистрибутива остается возможной непреднамеренная запись на исследуемый накопитель (например, при поиске загрузочного носителя, записи драйверов в initramfs и создании swap□файла или автоматическом монтировании обнаруженных дисковых разделов для поиска Root FS перебором всех подключенных дисков), рекомендуется физически подключать исследуемый носитель информации уже после загрузки Live□дистрибутива.

Linux системы с предустановленным набором криминалистических инструментов широко используются не только для снятия данных в режиме

Live CD, но и для офлайнового анализа. Большой популярностью пользуется виртуальная машина SIFT (SANS Investigative Forensics Toolkit) на базе Ubuntu (http://digital-forensics.sans.org/community/downloads).

Из платных Linux дистрибутивов наиболее популярны Grml-Forensic (https://grml-forensic.org/), Helix (https://www.e-fense.com/products.php), SMART Linux (http://www.asrdata.com/forensic-software/smartlinux/), Linux версия инструмента EnCase Portable – LinEn Boot CD (https://www.guidancesoftware.com/).

Несмотря на огромное количество криминалистических утилит, в том числе и с открытым кодом, лучше использовать протестированные и признанные в экспертной среде инструменты, которые не вызывают обоснованных сомнений в результатах проведенного анализа. Криминалистическое ПО или оборудование считается действительным для использования во время официального судебного разбирательства, если оно ранее использовалось авторитетной научной лабораторией, правоохранительным органом, образовательным институтом/ университетом и т.п.

Кроме того, для поиска и извлечения артефактов рекомендуется использовать не единственный продукт, а различные инструменты, которые в силу реализации разных алгоритмов могут давать отличные результаты. Для достаточного обоснования той или иной версии расследования криминалистом должны быть получены подтверждающие ее артефакты из разных источников (с персональных устройств, из сети, с корпоративных систем), что позволяет избежать ошибок, вызванных искажением свидетельств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/289 (дата обращения 25.07.2019).
2. *Баркалов Ю.М., Гайдин А.И., Потанина И.В.* Процессуальные и организационно-тактические особенности фиксации доказательственной информации, обнаруженной в сети Интернет. Метод. рекомендации. − Воронеж: Воронежский институт МВД России, 2016. – 52 с.
3. *Баркалов Ю.М., Нестеровский О.И., Лиходедов Д.Ю.* Организационно-техническое обеспечение специальных мероприятий. Метод. рекомендации. – Воронеж: Воронежский институт МВД России, 2016. – 82 с.
4. *Введенская О.Ю*. Расследование преступлений в сфере компьютерной информации: лекции, 2016. – Краснодар: Краснодарский ун-т МВД РФ. Кафедра криминалистики. – 126 с.
5. ГОСТ Р 57429–2017 Судебная компьютерно-техническая экспертиза. Термины и определения. – М.: Стандартинформ, 2017. – 12 с.
6. ГОСТ Р ИСО/МЭК 27000–2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология – М.: Стандартинформ, 2014. – 22 с.
7. ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. – 31 с.
8. ГОСТ Р ИСО/МЭК 27037–2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. – М.: Стандартинформ, 2014. – 48 с.
9. ГОСТ Р ИСО/МЭК 30121–2017 Информационные технологии (ИТ). Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме. – М.: Стандартинформ, 2017. – 12 с.
10. ГОСТ Р ИСО/МЭК ТО 18044–2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009. – 50 с.
11. *Грибунов О.П.*, *Старичков М.В*. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. – М.: ДГСК МВД России, 2017. – 160 с.

12. *Кэрриэ Б.* Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.
13. *Масалков А.С.* Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.
14. Федеральная служба безопасности Российской Федерации. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения», Москва, 12 ноября 2018 г. № 33 [Электронный ресурс]. URL: http://www.fsb.ru/files/fsbdoc/normakt/standart_sto_2018.doc (дата обращения 25.07.2019).
15. *Федотов Н.Н.* Форензика. Компьютерная криминалистика – М.: Юридический мир, 2007. – 432 с.
16. *Чернокнижный Г.М.* Защита сетевых информационных технологий: учебное пособие – СПб.: Изд-во СПбГЭУ, 2018. – 128 с.
17. Network Forensics Investigative Methodology (OSCAR) [Электронный ресурс]. URL: http://comp.org.uk/network-forensics-investigative-methodology-oscar.html (дата обращения 25.07.2019).
18. *Nihad A. Hassan*. Digital Forensics Basics: A Practical Guide Using Windows OS – Apress, 2019. – 360 p.
19. NIST SP 800-61 Rev. 2 Computer SecurityIncident Handling Guide. Recommendations of the National Institute of Standards and Technology, Aug. 2012 [Электронный ресурс]. URL: https://nvlpubs.nist.gov/ nistpubs/ SpecialPublications/NIST.SP.800-61r2.pdf (дата обращения: 01.03.2018).
20. NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology, Aug. 2006 [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (дата обращения: 01.03.2018).

Учебное издание

Васильева Ирина Николаевна

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Издано в авторской редакции

Подписано в печать 10.12.19. Формат 60×84 1/16.
Усл. печ. л. 7,25. Тираж 60 экз. Заказ 1870.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ