СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.3-2016

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

СБОР И АНАЛИЗ ТЕХНИЧЕСКИХ ДАННЫХ ПРИ РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Дата введения: 2017-01-01

Издание официальное

Москва
2016

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие приказом Банка России от 30 ноября 2016 года № ОД-4234.

Содержание

Введение

Документами Банка России в области стандартизации обеспечения информационной безопасности, в том числе стандартом Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее – СТО БР ИББС-1.0) определена необходимость выполнения организациями банковской системы (далее – БС) Российской Федерации (далее – РФ) деятельности по выявлению инцидентов информационной безопасности (далее – ИБ) и реагированию на инциденты ИБ.

К числу инцидентов ИБ относятся свершившиеся, предпринимаемые или вероятные реализации угроз ИБ, целью и (или) результатом которых являются:

– несанкционированное распоряжение денежными средствами, которое привело или может привести к:
  - осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
  - несвоевременности осуществления переводов денежных средств;
  - осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях на осуществление переводов денежных средств (реквизитов платежей);
– деструктивное воздействие на информационную инфраструктуру, используемую для осуществления переводов денежных средств, которое привело или может привести к нарушению непрерывности оказания платежных услуг.

Такие угрозы ИБ могут осуществляться как работниками организации БС РФ и иными лицами, имеющими легально предоставленный доступ к информационной инфраструктуре, используемой для осуществления переводов денежных средств (внутренними нарушителями ИБ), так и лицами, не имеющими такого доступа, в том числе не являющимися работниками организации БС РФ (внешними нарушителями ИБ).

Одними из ключевых направлений работ в рамках реагирования на инциденты ИБ являются:

– определение технических способов и схем реализаций угроз ИБ, целью и (или) результатом которых являются несанкционированное распоряжение денежными средствами и (или) нарушение непрерывности оказания платежных услуг (далее – угрозы ИБ), на основе сбора и анализа технических данных, формируемых объектами информационной инфраструктуры организации БС РФ и (или) клиентов;
– предотвращение повторных реализаций угроз ИБ с использованием ранее примененных технических способов и схем;
– проведение идентификации субъектов, реализующих угрозы ИБ, на основе результатов обработки технических данных, полученных в рамках реагирования на инциденты ИБ;
– проведение своевременного выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, используемыми для осуществления переводов денежных средств, на основе результатов обработки технических данных, полученных в рамках реагирования на инциденты ИБ.

Для обеспечения возможности выполнения указанных направлений работ в рамках системы менеджмента инцидентов ИБ (в том числе на стадии сбора и фиксации информации об инциденте ИБ), реализуемой в соответствии с рекомендациями в области стандартизации Банка России РС БР ИББС-2.5 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности” (далее – РС БР ИББС-2.5), организации БС РФ рекомендуется применение методов сбора, обработки, анализа и документирования данных, формируемых объектами информационной инфраструктуры, в том числе техническими средствами защиты информации, используемыми организациями БС РФ и их клиентами для осуществления переводов денежных средств (далее – технические данные), связанных со свершившимися, предпринимаемыми или вероятными реализациями угроз ИБ.

Настоящий документ устанавливает рекомендации к деятельности организаций БС РФ, реализующих функции операторов по переводу денежных средств или операторов услуг платежной инфраструктуры, по применению организационных, технологических и технических подходов, связанных со сбором, обработкой, анализом и распространением (передачей) технических данных.

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

СБОР И АНАЛИЗ ТЕХНИЧЕСКИХ ДАННЫХ ПРИ РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Дата введения 2017-01-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, реализующие функции операторов по переводу денежных средств или операторов услуг платежной инфраструктуры, и устанавливает рекомендации к организационным, технологическим и техническим подходам, связанным со сбором, обработкой, анализом и распространением (обменом) технических данных, в рамках деятельности по выявлению следующих типов инцидентов ИБ и реагированию на них:

– инциденты ИБ, информация о которых получена от клиентов операторов по переводу денежных средств (далее – клиентов), в том числе инциденты ИБ (события ИБ), выявленные клиентами, классифицированные клиентами как потенциальные попытки несанкционированных переводов денежных средств от их имени;
– инциденты ИБ (события ИБ), выявленные организацией БС РФ, классифицированные организацией БС РФ как попытки реализации угроз ИБ или как приготовление к их реализации;
– инциденты ИБ, информация о которых получена организацией БС РФ от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (далее – FinCert Банка России), а также иных организаций, например, операторов связи, провайдеров сети Интернет.

Положения настоящего стандарта могут применяться организациями, не входящими в БС РФ, реализующими функции операторов услуг платежной инфраструктуры, банковских платежных агентов (субагентов).

В настоящем стандарте не рассматриваются рекомендации, направленные на обеспечение выявления несанкционированных переводов денежных средств на основе анализа реквизитов распоряжений на осуществление переводов денежных средств, в том числе рекомендации к правилам настройки автоматизированных систем, реализующим функции противодействия мошенническим операциям (“системы антифрод”).

Настоящий стандарт не устанавливает рекомендации к реализации системы менеджмента инцидентов ИБ, в том числе не регламентирует процедуры обнаружения инцидентов ИБ и классификации отдельных событий ИБ или их групп в качестве инцидентов ИБ. В настоящем стандарте предполагается, что реализация системы менеджмента инцидентов ИБ осуществлена организацией БС РФ в соответствии с положениями РС БР ИББС-2.5. При этом настоящий стандарт развивает положения РС БР ИББС-2.5 в части сбора и анализа технических данных.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ, а также в договорах.

Положения настоящего стандарта имеют рекомендательный характер, если только в отношении отдельных положений обязательность их применения не установлена законодательством РФ, нормативными правовыми актами, в том числе нормативными актами Банка России.

Обязательность применения настоящего стандарта может быть установлена договорами, заключенными организациями БС РФ, или решением организации БС РФ о присоединении к настоящему стандарту.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:
СТО БР ИББС-1.0;
РС БР ИББС-2.5;
рекомендации в области стандартизации Банка России РС БР ИББС-2.6 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем” (далее – РС БР ИББС-2.6).

3. Термины и определения

В настоящем стандарте применяются термины в соответствии с СТО БР ИББС-1.0, РС БР ИББС-2.5, РС БР ИББС-2.6, а также следующие термины с соответствующими определениями.

3.1. **Инцидент ИБ при осуществлении переводов денежных средств, Инцидент ИБ –** событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

– несанкционированные переводы денежных средств, которые привели или могут привести к:
  - осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
  - несвоевременности осуществления переводов денежных средств;
  - осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях на осуществление переводов денежных средств (реквизитов платежей);
– деструктивные воздействия на информационную инфраструктуру, используемую для осуществления переводов денежных средств, которые привели или могут привести к нарушению непрерывности оказания платежных услуг.

3.2. **Несанкционированный перевод денежных средств –** перевод денежных средств лицами, не обладающими правом распоряжения денежными средствами.

4. Обозначения и сокращения

АБС – автоматизированная банковская система;
ИБ – информационная безопасность;
БС – банковская система;
ДБО – дистанционное банковское обслуживание;
НСД – несанкционированный доступ;
РФ – Российская Федерация;
СУБД – система управления базами данных;
СВТ – средство вычислительной техники;
СКЗИ – средство криптографической защиты информации.

5. Общие положения по организации процесса обработки технических данных в рамках реагирования на инциденты ИБ

5.1. В настоящем стандарте рассматриваются следующие группы рекомендаций по организации обработки технических данных при выявлении инцидентов ИБ и реагировании на них:

– рекомендации по сбору технических данных с компонентов информационной инфраструктуры, задействованных в осуществлении переводов денежных средств;
– рекомендации по проведению поиска (выделения) из собранных технических данных содержательной (семантической) информации, ее анализу и оформлению;
– рекомендации по распространению (передаче) выделенной и оформленной содержательной (семантической) информации;
– рекомендации по распределению зон ответственности подразделений организации БС РФ в рамках процесса обработки технических данных, включая анализ, оформление и распространение (передачу) содержательной (семантической) информации;
– рекомендации по взаимодействию с клиентами организации БС РФ в рамках процесса сбора технических данных;

– рекомендации по компетенции персонала организации БС РФ и (или) иных внешних организаций, задействованных в процессах обработки технических данных;
– рекомендации по обеспечению наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры, используемой для осуществления переводов денежных средств или для обеспечения защиты информации при осуществлении переводов денежных средств.

5.2. При организации обработки технических данных рекомендуется соблюдать следующие общие принципы:
– любые выполняемые процедуры и сервисные команды обработки технических данных, реализуемые организацией БС РФ и (или) ее клиентами (в том числе процедуры сбора, хранения, передачи технических данных) не должны вносить изменения в исходные технические данные и (или) их эталонные копии;
– сбор технических данных, поиск (выделение) из технических данных содержательной (семантической) информации, ее анализ должны проводиться лицами, обладающими необходимым опытом и компетенцией;
– выполнение всех процедур и сервисных команд обработки технических данных, реализуемых организацией БС РФ и (или) ее клиентами (в том числе процедуры и сервисные команды их сбора, хранения и передачи), должно сопровождаться выполнением процедур и сервисных команд, обеспечивающих возможность последующего контроля целостности (неизменности) технических данных;
– обработка технических данных должна сопровождаться описанием и протоколированием:
  • всех выполняемых процедур и сервисных команд, использованных для сбора, сохранения и передачи технических данных. Реализация описания и протоколирования выполненных процедур и сервисных команд должна обеспечивать возможность их точного повторного выполнения;
  • перечня использованных технических средств и инструментов, применяемых для сбора, сохранения и передачи технических данных, а также параметров их настройки;
  • места, даты и времени[1] выполнения сбора, сохранения и передачи технических данных;
  • места, даты и времени выполнения процедур и сервисных команд;
  • идентификационных данных лиц, выполнивших процедуры и сервисные команды сбора, сохранения и передачи технических данных;
– обеспечение хранения указанных описаний и протоколов совместно с обрабатываемыми техническими данными, а также обеспечение их доступности для представления;
– обеспечение протоколирования действий по передаче копий собранных технических данных между лицами, участвующими в расследовании инцидентов ИБ, хранения указанных протоколов совместно с обрабатываемыми техническими данными, а также обеспечение их доступности для представления.

При наличии соответствующих знаний рекомендуется сопровождать выполнение процедур и сервисных команд обработки технических данных описанием и протоколированием ожидаемого изменения в состоянии информационной инфраструктуры (например, появления временных файлов, изменения даты и времени последнего обращения к файлу).

Описание возможного формата и содержания протокола выполнения процедур и сервисных команд обработки технических данных приведено в приложении А к настоящему стандарту. Пример протокола снятия криминалистической копии (создание образа) накопителя на жестких магнитных дисках приведено в приложении Б к настоящему стандарту.

Рекомендуется осуществлять указанные выше описание и протоколирование не менее чем двумя лицами.

5.3. Организация процесса обработки технических данных должна обеспечивать:
– сохранность и неизменность технических данных;
– относимость собранных и обрабатываемых технических данных к конкретному инциденту ИБ;
– доступность, целостность и конфиденциальность технических данных при их обработке.

При этом организация сбора технических данных должна быть организована с учетом возможности:
– изменения, повреждения и (или) уничтожения исходных технических данных;
– потери исходных технических данных с течением времени.

5.4. Обеспечение возможности контроля целостности (неизменности) технических данных в большинстве случаев может быть реализовано:

[1] Здесь и далее рекомендуется протоколирование времени с указанием часового пояса.

– использованием технических средств для вычисления контрольных сумм или значений хэш-функций исходных и копий технических данных с последующим:
  • сравнением вычисленных значений для фиксации целостности данных;
  • составлением акта с документированием полученного вычисления контрольной суммы или значения хэш-функций;
  • обеспечением хранения акта совместно с обрабатываемыми техническими данными;
– документированием отдельных технических данных незначительного объема на бумажном носителе с:
  • составлением акта о соответствии содержания задокументированных технических данных на бумажном носителе и исходных технических данных на машинном носителе;
  • сшиванием документов с техническими данными и акта в единый пакет или их упаковкой в пакеты (контейнеры), обеспечивающие невозможность доступа без видимого нарушения целостности упаковки.

  Рекомендуется осуществлять составление и заверение указанных актов не менее чем двумя лицами.
  Вычисление значений хэш-функций рекомендуется реализовывать в соответствии с ГОСТ Р 34.11-2102 [2].

5.4.1. Для собираемых технических данных рекомендуется обеспечить наличие как минимум четырех копий, одна их которых используется для последующей обработки и анализа, а остальные хранятся организацией БС РФ в неизменном (эталонном) виде для целей:
- возможной передачи в правоохранительные органы;
- возможной передачи в FinCert Банка России;
- собственного использования организацией БС РФ.

5.5. Особое внимание при распространении (передаче) технических данных и выделенной из них содержательной (семантической) информации следует уделять обеспечению сохранности (нераспространению) информации, защищаемой в соответствии с требованиями законодательства РФ, в первую очередь содержащей банковскую тайну и персональные данные. Для этого при реализации поиска (выделения) из технических данных содержательной (семантической) информации рекомендуется руководствоваться следующими общими правилами:
– при наличии возможности следует разделять содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой методом группирования информации:
  • в отдельных постраничных разделах документов, а также путем помещения ее в раздельные документы на бумажном носителе;
  • в различных файлах данных;
– следует обеспечить поиск (выделение) только той содержательной (семантической) информации, защищаемой в соответствии с требованиями законодательства РФ, которая имеет отношение к конкретному инциденту ИБ (или их группе);
– обработка содержательной (семантической) информации не должна приводить к формированию сводной информации обо всех клиентах организации БС РФ или информации о клиентах организации БС РФ, не имеющих отношения к конкретному инциденту ИБ (или их группе), в отношении которого осуществляется реагирование.

В случае отсутствия возможности разделить содержательную (семантическую) информацию, защищаемую в соответствии с требованиями законодательства РФ, от не являющейся таковой носители содержательной (семантической) информации, передаваемые в правоохранительные органы, должны быть классифицированы и маркированы в соответствии с правилами, установленными в организации БС РФ, и передаваться по акту, в котором среди прочего определяется обязанность принимающий стороны обеспечить конфиденциальность передаваемой информации.

6. Рекомендации по сбору технических данных

6.1. Сбор технических данных рекомендуется реализовывать в рамках установленной и документированной деятельности по сбору и фиксации информации об инцидентах ИБ, выполняемой в соответствии с РС БР ИББС-2.5.

В рамках деятельности по сбору и фиксации информации об инцидентах ИБ рекомендуется для каждого инцидента ИБ обеспечить, помимо сбора технических данных, сбор и документирование обзорной информации об инциденте ИБ – профиля инцидента ИБ, описывающего:
– способ выявления инцидента ИБ;
– источник информации об инциденте ИБ;

– содержание информации об инциденте ИБ, полученной от источника;
– сценарий реализации инцидента ИБ;
– дату и время выявления инцидента ИБ;
– состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности для деятельности организации БС РФ;
– способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования;
– контактная информация работников организации БС РФ, в зону ответственности которых входит обеспечение эксплуатации информационной инфраструктуры, задействованной в реализации инцидента ИБ;
– информация об операторе связи и провайдере сети Интернет.

Непосредственный сбор технических данных рекомендуется осуществлять в рамках установленной и документированной деятельности по сбору и фиксации информации о следующих инцидентах ИБ:
– инциденты ИБ, результатом которых являются и (или) могут являться несанкционированные переводы денежных средств (далее – инциденты ИБ, связанные с несанкционированными переводами денежных средств);
– инциденты ИБ, результатом которых является деструктивное воздействие на объекты информационной инфраструктуры организации БС РФ, которые привели или могут привести к нарушению непрерывности оказания платежных услуг (далее – инциденты ИБ, связанные с деструктивным воздействием).

В составе инцидентов ИБ, связанных с несанкционированными переводами денежных средств, рекомендуется рассматривать:
– инциденты ИБ, связанные с несанкционированным доступом (далее – НСД) к объектам информационной инфраструктуры клиентов;
– спам-рассылки, осуществляемые в отношении клиентов, реализуемые в рамках реализации методов “социального инжиниринга”[1], предпринимаемые с целью распространения компьютерных вирусов, функционально предназначенного для совершения несанкционированных переводов денежных средств;
– атаки типа “отказ в обслуживании” (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов, предпринимаемые с целью блокирования нормального функционирования информационной инфраструктуры после успешной реализации несанкционированных переводов денежных средств;
– воздействие компьютерных вирусов на информационную инфраструктуру клиентов, потенциально функционально предназначенного для совершения несанкционированных переводов денежных средств;
– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем дистанционного банковского обслуживания (далее – систем ДБО) организаций БС РФ;
– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры автоматизированных банковских систем (далее – АБС) организаций БС РФ;
– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем обработки карточных транзакций (далее – систем фронт-офиса) организаций БС РФ;
– инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры систем посттранзакционного обслуживания карточных операций (далее – систем бэк-офиса) организаций БС РФ, в том числе системам электронного документооборота, формирования платежных клиринговых позиций, клиринга и подготовки данных для проведения расчетов.

В составе инцидентов ИБ, связанных с деструктивным воздействием, рекомендуется рассматривать:
– атаки типа “отказ в обслуживании” (DDOS-атаки), реализуемые применительно к информационной инфраструктуре систем ДБО, систем фронт-офиса организаций БС РФ;
– деструктивное воздействие компьютерных вирусов на информационную инфраструктуру организации БС РФ.

6.2. Организацию сбора технических данных рекомендуется проводить в следующем порядке:
– предварительное планирование и создание условий для сбора технических данных:
  • разработка и утверждение плана (регламента) сбора технических данных, реализуемого в случае выявления инцидентов ИБ;
  • включение ответственных за выполнение ролей в рамках процессов обработки технических данных в группу реагирования на инциденты ИБ, создаваемую в соответствии с РС БР ИББС-2.5;

[1] Реагирование на инциденты ИБ, связанные со спам-рассылками, целесообразно осуществлять в случаях наличия в теле почтовых сообщений ссылок на потенциально вредоносный (в том числе фишинговый) сайт, размещенный в сети Интернет.

- обеспечение необходимых технических средств и инструментов для сбора и обработки технических данных;

– сбор технических данных при выявлении инцидента ИБ:
  - оперативное определение перечня компонентов информационной инфраструктуры, задействованной в реализации инцидента ИБ;
  - оперативное ограничение доступа к компонентам информационной инфраструктуры, задействованной в реализации инцидента ИБ, а также техническим данным для цели обеспечения их сохранности до выполнения сбора;
  - сбор и документирование сведений об официально назначенном эксплуатационном персонале (администраторах) информационной инфраструктуры, задействованной в реализации инцидента ИБ, получение документально оформленных подтверждений лиц из состава эксплуатационного персонала о предоставлении/непредоставлении их аутентификационных данных третьим лицам и о внесении изменений/невнесении изменений в протоколы (журналы) регистрации, формируемые компонентами информационной инфраструктуры;
  - непосредственный сбор технических данных, в том числе проверка и обеспечение целостности (неизменности) собранных данных, маркирование носителей собранных данных;
– обеспечение сохранности машинных носителей информации и защиту от воздействий, которые могут повредить их информационное содержимое, путем безопасной упаковки, опечатывания, исключающего возможность несанкционированного использования (подключения) носителя данных без нарушения целостности упаковки (печати), а также безопасного хранения и транспортировки носителей собранных данных.

6.3. Рекомендации к предварительному планированию сбора технических данных.

В плане (регламенте) сбора технических данных рекомендуется определить для каждого потенциального инцидента ИБ из числа указанных в подпункте 6.1 настоящего раздела следующие положения:
– состав собираемых технических данных;
– приоритеты (последовательность) сбора технических данных;
– инструкции по использованию технических средств инструментов, описание процедур и сервисных команд, необходимых для сбора технических данных;
– описание процедур и сервисных команд, в том числе технических, проверки (контроля) целостности собранных данных;
– правила описания и протоколирования выполненных процедур и сервисных команд, описания места сбора технических данных;
– правила создания копий собираемых технических данных и требования к их количеству;
– правила маркирования, безопасной упаковки и хранения носителей собранных технических данных;
– правила регистрации и хранения описаний и протоколов, связанных со сбором технических данных.

В плане (регламенте) сбора технических данных рекомендуется также определить необходимость и условия подготовки обращения в МВД России, его территориальное подразделения и (или) FinCert Банка России.

При планировании сбора технических данных возможно рассмотрение следующих типовых сценариев, определяющих степень оперативности предпринимаемых действий:
– сбор данных в реальном масштабе времени в случае, когда система ДБО, АБС, система фронт-офиса, система бэк-офиса (далее при совместном упоминании – целевые системы) непосредственно не подвержена компьютерной атаке, а компьютерная атака выявлена на периметре информационной инфраструктуры;
– сбор данных непосредственно после реализации инцидента ИБ (например, в течение 24 часов);
– сбор данных по прошествии значительного времени после инцидента ИБ.

Рекомендуется реализовать сбор следующих технических данных:

6.3.1. Информационная инфраструктура клиента[1]:
– энергонезависимые технические данные, расположенные на запоминающих устройствах средств вычислительной техники (СВТ), используемых клиентами для осуществления доступа к системам ДБО:
  - серверном оборудовании;
  - настольных компьютерах, ноутбуках;
  - мобильных устройствах и планшетах;

[1] В настоящем стандарте предполагается, что сбор технических данных реализуется при наличии технической возможности с использованием функциональных возможностей объектов информационной инфраструктуры, эксплуатация которых осуществляется или организована клиентом.

– энергозависимые технические данные, расположенные в оперативной памяти СВТ, используемые клиентами для осуществления доступа к системам ДБО;
– энергозависимые технические данные операционных систем СВТ, используемых клиентами для осуществления доступа к системам ДБО:
  • данные о сетевых конфигурациях;
  • данные о сетевых соединениях;
  • данные о запущенных программных процессах;
  • данные об открытых файлах;
  • список открытых сессий доступа;
  • системные дата и время операционной системы;
– протоколы (журналы) регистрации телекоммуникационного оборудования, используемого клиентами для осуществления доступа к системам ДБО:
  • маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
  • DHCP-сервисы;
– протоколы (журналы) регистрации средств защиты информации:
  • средства (системы) аутентификации, авторизации и разграничения доступа к системам ДБО;
  • средства защиты от НСД, размещенные на СВТ, используемых клиентами для осуществления доступа к системам ДБО;
  • средства межсетевого экранирования;
  • средства обнаружения вторжений и сетевых атак;
  • средства антивирусной защиты;
  • средства криптографической защиты информации (далее – СКЗИ), используемые в системах ДБО;
– протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;
– данные сетевого трафика[1] из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентами для осуществления доступа к системам ДБО;
– протоколы (журналы) регистрации автоматических телефонных станций;
– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа, используемые для контроля доступа в помещения, в которых расположены СВТ, используемые клиентами для осуществления доступа к системам ДБО;
– носители ключевой информации СКЗИ, используемой в системах ДБО.

6.3.2. Информационная инфраструктура организации БС РФ[2]:
– энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ целевых систем:
  • серверном оборудовании целевых систем;
  • серверном оборудовании, поддерживающем функционирование информационной инфраструктуры целевых систем;
  • СВТ, используемых для администрирования целевых систем;
  • банкоматах и POS-терминалах;
– энергозависимые технические данные, расположенные в оперативной памяти СВТ целевых систем:
  • СВТ, используемых для администрирования информационной инфраструктуры целевых систем;
  • серверного оборудования целевых систем;
  • серверного оборудования, поддерживающего функционирование информационной инфраструктуры целевых систем;
– энергозависимые технические данные СВТ целевых систем в составе следующих данных:
  • данные о сетевых конфигурациях;
  • данные о сетевых соединениях;
  • данные о запущенных программных процессах;
  • данные об открытых файлах;
  • список открытых сессий доступа;
  • системные дата и время операционной системы;
– протоколы (журналы) регистрации целевых систем;

[1] Копия и (или) заголовки сетевого трафика.

[2] В настоящем стандарте предполагается, что сбор технических данных реализуется при наличии технической возможности с использованием функциональных возможностей объектов информационной инфраструктуры, эксплуатация которых осуществляется или организована организацией БС РФ.

– протоколы (журналы) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем:
  • маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
  • средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
– протоколы (журналы) регистрации средств защиты информации, используемых в информационной инфраструктуре целевых систем:
  • средства (системы) аутентификации, авторизации и разграничения доступа;
  • средства межсетевого экранирования;
  • средства обнаружения вторжений и сетевых атак, в том числе DDOS-атак;
  • DHCP-сервисы;
  • средства защиты от НСД, размещенные на СВТ, используемых для администрирования информационной инфраструктуры целевых систем;
  • средства антивирусной защиты информационной инфраструктуры;
  • СКЗИ;
– протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;
– протоколы (журналы) регистрации и данные web-серверов и средств контентной фильтрации web-протоколов;
– протоколы (журналы) регистрации систем управления базами данных (далее – СУБД);
– данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;
– протоколы (журналы) регистрации автоматических телефонных станций;
– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа, используемые для контроля доступа в помещения, в которых расположены СВТ целевых систем.

6.3.3. Для сбора технических данных могут выполняться следующие возможные действия:
– отключение СВТ от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (в том числе Wi-Fi адаптера, GSM/LTE модема, Bluetooth адаптера, отключение виртуального коммутатора виртуальной машины);
– “криминалистическое” копирование энергозависимых технических данных СВТ, в том числе:
  • копирование содержимого оперативной памяти СВТ;
  • копирование данных операционных систем;
– отключение СВТ путем прерывания питания (отключение шнура питания или извлечение аккумуляторной батареи, отключения сетевого кабеля[1]) с последующим извлечением запоминающих устройств;
– обеспечение сохранности носителей ключевой информации СКЗИ, используемой в системах ДБО;
– “криминалистическое” копирование (создание образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитного копирования и (или) методом копирования “bit-copy plus”, в том числе копирование (создание образов) жестких магнитных дисков СВТ;
– копирование протоколов (журналов) регистрации;
– копирование сетевого трафика.

При отключении СВТ путем прерывания питания следует учитывать возможность:
– наличия источников бесперебойного питания;
– наличия для разных типов СВТ различающихся схем реагирования на прерывание питания – запуск процедуры штатной остановки, мгновенное отключение, переключение на резервный источник питания;
– наличия необходимости использования комбинации действий, например, одновременного отключения шнура питания и извлечения аккумуляторной батареи совместно с извлечением сетевого кабеля из сетевого интерфейса;
– существования типов СВТ, для которых конструктивно не предусмотрена процедура прерывания питания (например, для некоторых типов мобильных устройств).

Приоритеты и последовательность выполнения действий и операций по сбору технических данных рекомендуется определять на основе следующих факторов:
– фактор минимизации риска возникновения существенного ущерба от инцидента ИБ, в том числе риска совершения несанкционированных переводов денежных средств;

---

[1] Для случаев использования сетевых интерфейсов, поддерживающих питание по вычислительной сети (например, технология Power over Ethernet, PoE).

– фактор первоочередного получения технических данных из энергозависимой памяти;
– фактор учета возможности удаления и (или) перезаписи технических данных в энергонезависимой памяти;
– значимость технических данных для цели реагирования на инцидент ИБ с учетом реализации конкретных процедур обработки информации;
– объем требуемых усилий для сбора технических данных с определенных источников, в частности, наличия у работников необходимой компетенции по сбору технических данных с определенных источников, предполагаемых временных затрат, стоимость специализированных технических средств и инструментов или услуг внешних организаций.

Рекомендуемой реализацией является локальный сбор технических данных без удаленного доступа с использованием вычислительных сетей.

С учетом указанных факторов рекомендуется следующая последовательность действий при сборе технических данных:

6.3.4. Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры клиентов[1]:

1) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа), используемых клиентом для осуществления доступа к системам ДБО (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, указанные в пункте 1;
3) отключение СВТ, указанных в пункте 1, путем прерывания питания[2] с последующим извлечением запоминающих устройств и их передачей в адрес организации БС РФ и (или) экспертам FinCert Банка России (рекомендуется к выполнению с высоким приоритетом значимости);
4) в случае отсутствия технической возможности выполнения пункта 3 – отключение СВТ, указанных в пункте 1, от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);
5) в случае отсутствия технической возможности выполнения пункта 3 – копирование содержимого оперативной памяти СВТ, указанных в пункте 1 (рекомендуется к выполнению с высоким приоритетом значимости);
6) в случае отсутствия технической возможности выполнения пункта 3 – получение данных операционных систем СВТ, указанных в пункте 1 (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системные дата и время операционной системы) (рекомендуется к выполнению с высоким приоритетом значимости);
7) в случае отсутствия технической возможности выполнения пункта 3 – "криминалистическое" копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 1 (рекомендуется к выполнению с высоким приоритетом значимости);
8) копирование протоколов (журналов) регистрации средств защиты информации информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
9) обеспечение сохранности носителей ключевой информации СКЗИ, используемой в системах ДБО (рекомендуется к выполнению с высоким приоритетом значимости);
10) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ;
11) копирование протоколов (журналов) регистрации автоматических телефонных станций;
12) копирование протоколов (журналов) регистрации систем видеонаблюдения и систем контроля доступа, используемых для контроля доступа в помещения, предназначенные для размещения СВТ, указанных в пункте 1, за 1 неделю, предшествующую инциденту ИБ;
13) получение и документирование информации о местоположении клиента – физического лица, осуществляющего доступ к системе ДБО.

6.3.5. Спам-рассылки, осуществляемые в отношении клиентов, реализуемые в рамках реализации методов "социального инжиниринга":

---

[1] В случае наличия риска осуществления несанкционированных переводов денежных средств клиенту следует обеспечить максимально быстрое отключение от вычислительных сетей СВТ, используемых для осуществления доступа к системам ДБО, игнорируя потерю отдельных технических данных.

[2] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

1) копирование протоколов (журналов) регистрации и данных почтовых серверов и средств контентной фильтрации электронной почты за период времени реализации спам-рассылки (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ;
3) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры клиента за период времени реализации DDOS-атаки.

6.3.6. Атаки типа “отказ в обслуживании” (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов:

1) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры клиента за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак информационной инфраструктуры клиента за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
3) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
4) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентом для осуществления доступа к системам ДБО за период времени реализации DDOS-атаки, а также за короткий период времени до и после реализации DDOS-атаки;
5) Дополнительно организации БС РФ рекомендуется:
   – идентифицировать владельца СВТ, входящих в состав бот-сетей, задействованных в реализации DDOS-атаки (далее – СВТ бот-сетей);
   – совместно с владельцем СВТ бот-сетей организовать сбор следующих технических данных:
6) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа, данные о запущенных программных процессах), задействованных в реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
7) копирование содержимого оперативной памяти СВТ, указанного в пункте 6 (рекомендуется к выполнению с высоким приоритетом значимости);
8) получение данных операционных СВТ (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы), указанных в пункте 5 (рекомендуется к выполнению с высоким приоритетом значимости);
9) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре размещения СВТ бот-сетей;
10) копирование протоколов (журналов) регистрации средств межсетевого экранирования, используемых в информационной инфраструктуре размещения СВТ бот-сетей;
11) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак информационной инфраструктуры размещения СВТ бот-сетей;
12) “криминалистическое” копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 5 (рекомендуется к выполнению с высоким приоритетом значимости).

6.3.7. Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры целевых систем организации БС РФ[1]:

1) копирование протоколов (журналов) регистрации целевых систем организации БС РФ за период времени, связанный с инцидентом ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование протоколов (журналов) регистрации и данных web-серверов, средств контентной фильтрации web-протоколов за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
3) копирование протоколов (журналов) регистрации СУБД за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);

[1] В случае наличия риска осуществления несанкционированных переводов денежных средств организации БС РФ следует обеспечить максимально быстрое отключение от вычислительных сетей СВТ, используемых для осуществления доступа к платежным системам, игнорируя потерю отдельных технических данных.

4) копирование протоколов (журналов) регистрации средств защиты информации, используемых в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
5) копирование протоколов (журналов) телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ;
6) получение данных операционных систем СВТ целевых систем (сетевые соединения, список открытых сессий доступа);
7) копирование содержимого оперативной памяти СВТ целевых систем;
8) получение данных операционных систем СВТ целевых систем (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы;
9) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;
10) "криминалистическое" копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 6;
11) копирование протоколов (журналов) регистрации автоматических телефонных станций;
12) копирование протоколов (журналов) регистрации систем видеонаблюдения и систем контроля доступа, используемых для контроля доступа в помещения, предназначенные для размещения СВТ целевых систем, за 1 неделю, предшествующую инциденту ИБ.

6.3.8. Атаки типа "отказ в обслуживании" (DDOS-атаки), реализуемые применительно к информационной инфраструктуре целевых систем организаций БС РФ:
1) копирование протоколов (журналов) регистрации средств межсетевого экранирования информационной инфраструктуры целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование протоколов (журналов) регистрации средств обнаружения вторжений и сетевых атак в информационную инфраструктуру целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
3) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем за период времени реализации DDOS-атаки (рекомендуется к выполнению с высоким приоритетом значимости);
4) копирование сетевого из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем, за период времени реализации DDOS-атаки, а также за короткий период времени до и после реализации DDOS-атаки;
5) Дополнительно организации БС РФ рекомендуется:
   – документировать сведения:
     • о пропускной способности и провайдерах используемых каналов связи;
     • об использовании сервиса защиты от DDOS-атак, предоставляемого внешними организациями;
   – идентифицировать владельца СВТ бот-сетей, задействованных в реализации DDOS-атаки;
   – совместно с владельцем СВТ бот-сетей организовать сбор технических данных по аналогии с рекомендациями, установленными для случая сбора технических данных при атаках типа "отказ в обслуживании" (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов.

6.3.9. Деструктивное воздействие компьютерных вирусов на информационную инфраструктуру организации БС РФ[1]:
1) получение данных операционных систем СВТ целевых систем (сетевые соединения, список открытых сессий доступа) (рекомендуется к выполнению с высоким приоритетом значимости);
2) копирование сетевого из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем;
3) копирование содержимого оперативной памяти СВТ целевых систем (рекомендуется к выполнению с высоким приоритетом значимости);
4) отключение СВТ целевых систем от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);
5) получение данных операционных систем СВТ целевых систем (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы) (рекомендуется к выполнению с высоким приоритетом значимости);

[1] До выполнения действий по сбору технических данных не следует проводить антивирусную проверку.

6) криминалистическое копирование (создание образов) запоминающих устройств СВТ целевых систем (рекомендуется к выполнению с высоким приоритетом значимости);
7) копирование протоколов (журналов) регистрации средств антивирусной защиты информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
8) копирование протоколов (журналов) регистрации и данных почтовых серверов, средств контентной фильтрации электронной почты за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
9) копирование протоколов (журналов) регистрации и данные web-серверов, средств контентной фильтрации web-протоколов за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
10) копирование протоколов (журналов) регистрации средств защиты информации, используемых в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
11) копирование протоколов (журналов) регистрации протоколы (журналы) регистрации телекоммуникационного оборудования, используемого в информационной инфраструктуре целевых систем, за три месяца, предшествующих инциденту ИБ.

6.3.10. Деструктивное воздействие компьютерных вирусов на информационную инфраструктуру клиентов[1]:

1) копирование протоколов (журналов) регистрации средств антивирусной защиты информационной инфраструктуры клиента за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
2) получение данных операционных систем СВТ (сетевые соединения, список открытых сессий доступа), используемых клиентом для осуществления доступа к системам ДБО (рекомендуется к выполнению с высоким приоритетом значимости);
3) копирование сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, указанные в пункте 2;
4) отключение СВТ, указанных в пункте 2, от вычислительной сети путем отключения сетевого кабеля, отключения и (или) выключения сетевых устройств (рекомендуется к выполнению с высоким приоритетом значимости);
5) копирование содержимого оперативной памяти СВТ, указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);
6) отключение СВТ, указанных в пункте 2, путем прерывания питания[2] с последующим извлечением запоминающих устройств и их передачей в адрес организации БС РФ и (или) экспертам FinCert Банка России (рекомендуется к выполнению с высоким приоритетом значимости);
7) в случае отсутствия технической возможности выполнения пункта 5 – криминалистическое копирование (создание образов) данных запоминающих устройств СВТ, указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);
8) в случае отсутствия технической возможности выполнения пункта 5 – получение данных операционных систем СВТ (список запущенных программных процессов, список открытых файлов, сетевые конфигурации, системное время операционной системы), указанных в пункте 2 (рекомендуется к выполнению с высоким приоритетом значимости);
9) копирование протоколов (журналов) регистрации и данных почтовых серверов, средств контентной фильтрации электронной почты за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
10) копирование протоколов (журналов) регистрации средств защиты информации информационной инфраструктуры клиента, за три месяца, предшествующих инциденту ИБ (рекомендуется к выполнению с высоким приоритетом значимости);
11) копирование протоколов (журналов) регистрации телекоммуникационного оборудования, используемого клиентом для осуществления доступа к системам ДБО, за три месяца, предшествующих инциденту ИБ.

---

[1] До выполнения действий по сбору технических данных не следует проводить антивирусную проверку.

[2] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

6.4. Рекомендации по обеспечению необходимыми техническими средствами и инструментами для сбора и обработки технических данных.

Для реализации сбора и обработки технических данных организации БС РФ рекомендуется обеспечить наличие следующих готовых к использованию технических средств и инструментов:

– специально выделенные автоматизированные рабочие места для обработки технических данных, в том числе для поиска (выделения) содержательной (семантической) информации, ее анализа и оформления. Рекомендуется использование автономных автоматизированных рабочих мест, не подключенных к вычислительным сетям[1];
– технические, в том числе программные, средства для сбора технических данных и проверки (контроля) целостности собранных данных;
– технические средства централизованного сбора, хранения и анализа протоколов (журналов) регистрации, а также автоматизированной обработки собранных технических данных (например, систем управления журналами регистрации, SIEM систем);
– технические средства записи и хранения данных сетевого трафика;
– носители данных для сбора и хранения собранных технических данных. При этом рекомендуется:
  • использование носителей, объем хранения которых заведомо превышает объем собираемых технических данных;
  • в случае применения инструментов, реализующих посекторное копирование данных, использование носителей, имеющих ту же физическую основу хранения (данные с HDD-накопителей копируются на HDD-накопители, данные с SSD-накопителей копируются на SSD-накопители). При этом носители-приемники должны быть подготовлены (очищены) специальным образом для обеспечения отсутствия каких-либо посторонних данных, для чего рекомендуется использование средств гарантированного уничтожения информации или штатных средств операционной системы, реализующих функцию форматирования с полным удалением (очисткой) записанной информации, сопровождаемое документированием выполненных процедур и сервисных команд;
  • в случае копирования данных с SSD-накопителей рекомендуется создание образов в файле данных в формате “RAW”. При невозможности создания образов в файле данных в формате “RAW” рекомендуется использование модели SSD-накопителя, идентичной модели накопителя с исходными данными;
– антистатические контейнеры или пакеты для хранения носителей технических данных;
– наклейки, этикетки и перманентные маркеры для маркирования носителей собранных технических данных;
– немагнитные инструменты, используемые для извлечения запоминающих устройств, накопителей на жестких магнитных дисках;
– прошитые книги (блокноты) для фиксации протоколов и описаний выполняемых действий и операций;
– цифровые фотоаппараты и диктофоны.

При сборе технических данных следует избегать использования любых средств и материалов, которые производят или излучают статическое или электромагнитное поле, так как оно может повредить или уничтожить собранные данные.

Рекомендации по составу технических средств сбора технических данных приведены в приложении В к настоящему стандарту.

6.5. Рекомендации по оперативному ограничению доступа к техническим данным для цели обеспечения их сохранности до выполнения сбора.

В планах (регламентах) сбора технических данных должно быть предусмотрено оперативное выполнение действий и операций, направленных на минимизацию риска злоумышленных или случайных действий по изменению, повреждению и (или) уничтожению технических данных до момента их сбора. К таким действиям и операциям относятся:

– реализация ограничений и (или) запрета по физическому доступу к объектам информационной инфраструктуры – источникам технических данных;
– реализация ограничений и (или) запрета по логическому доступу к объектам информационной инфраструктуры – источникам технических данных до момента сбора идентифицированных технических данных;
– проведение сбора технических данных только лицами, обладающими необходимыми опытом и компетенцией.

[1] В качестве альтернативы может быть рекомендовано использование для сбора и обработки технических данных выделенных сегментов вычислительных сетей или отдельных виртуальных машин.

После обнаружения инцидента ИБ до момента сбора технических данных следует обеспечить запрет выполнения:

– антивирусных проверок СВТ – потенциальных источников технических данных;
– установки обновлений и переустановки операционных систем СВТ – потенциальных источников технических данных;
– отключения от вычислительной сети СВТ – потенциальных источников технических данных, за исключением СВТ, используемых клиентами для осуществления доступа к системам ДБО и СВТ, используемых организациями БС РФ для взаимодействия с платежными системами.

С целью минимизации финансового ущерба от инцидентов ИБ организации БС РФ рекомендуется:

доведение до клиентов рекомендаций по максимально возможно быстрому отключению от вычислительных сетей СВТ, используемых клиентами для осуществления доступа к системам ДБО;

максимально возможное быстрое отключение от вычислительных сетей СВТ, используемых организациями БС РФ для взаимодействия с платежными системами.

6.6. Рекомендации по способам непосредственного сбора технических данных, в том числе проверке целостности (неизменности) собранных данных, маркированию носителей собранных данных.

Перед непосредственным сбором технических данных рекомендуется выполнение описания или фиксации места сбора технических данных:

– описание или фиксацию типа, расположения, состояния электропитания СВТ;
– описание или фиксацию наличия и способа подключения СВТ к вычислительным сетям, в том числе беспроводным сетям и к информационно-телекоммуникационной сети “Интернет”;
– описание или фиксацию информации о событиях и процессах на дисплеях СВТ.

Фиксацию места сбора технических данных рекомендуется осуществлять путем фото- или видеосъемки с отметкой даты и времени, для чего на фото- или видеоаппаратуре должны быть выставлены корректные дата и время. Рекомендуется использование фото- или видеоаппаратуры, формирующей EXIF-данные фотографий, позволяющих подтвердить подлинность графического изображения. Дополнительно рекомендуется документирование данных о производителе, модели и серийном номере используемой фото- или видеоаппаратуры.

6.6.1. Рекомендации по выполнению “криминалистического” копирования (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования и (или) методом копирования “bit-copy plus”.

Выполнение операций по “созданию образа” энергонезависимых технических данных СВТ должно сопровождаться описанием и протоколированием:

– всех выполненных процедур и сервисных команд, использованных для выполнения операции по “созданию образа” с указанием даты и времени начала и окончания их выполнения;
– характеристик запоминающих устройств (модель, серийный номер, характеристики, емкость) исходных технических данных и их полученных копий;
– использованных технических средств, примененных для выполнения операций по “созданию образа” (наименование, версия, лицензионные сведения).

Для выполнения “криминалистического” копирования (создания образов) запоминающих устройств рекомендуется следующая последовательность действий и операций:

1) отключение СВТ путем прерывания питания[1];
2) в случае применения:
   2.1) программных средств “криминалистического” копирования (создания образов):
      2.1.1) загрузка операционной системы с предварительно созданного “доверенного” загрузочного носителя, содержащего необходимые программные средства для выполнения операций по “созданию образа”, в том числе программные средства создания побитовой копии, вычисления контрольных сумм или значений хэш-функций, программные средства использования запоминающего устройства в режиме “только для чтения”;
      2.1.2) принятие мер к обеспечению использования запоминающего устройства в режиме “только для чтения”, для чего возможно использование функций операционной системы путем настроек правил ее загрузки с “доверенного” носителя или специализированных аппаратных или программных средств – “write-blocker”[2];

[1] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

[2] Также указанные аппаратные или программные средства известны под общим наименованием “forensic bridge”. В случае отсутствия технической возможности использования запоминающего устройства в режиме “только для чтения” следует учитывать возможность изменения исходных технических данных, в том числе появление временных файлов данных, изменения временных атрибутов файлов данных и директорий, изменений данных системного реестра операционной системы Windows.

2.1.3) в случае отсутствия технической возможности выполнения пунктов 1) и 2.1.1) подключение к СВТ и использование носителя, содержащего необходимые для создания образа программные средства, в отношении которого приняты меры по обеспечению защиты от записи или несанкционированного изменения;

2.2) аппаратных средств – дубликаторов "криминалистического" копирования (создания образов):

2.2.1) извлечение из СВТ запоминающего устройства и подключение его к дубликатору;

3) вычисление и сохранение контрольной суммы или значения хэш-функций исходных данных запоминающего устройства[1];

4) выполнение операции по "созданию образа" на отдельный специально подготовленный носитель информации;

5) вычисление и сохранение контрольных сумм или значений хэш-функций скопированных данных и исходных данных запоминающего устройства, сравнение вычисленного значения со значением, вычисленным в рамках выполнения пункта 5, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;

6) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные данные.

6.6.2. Рекомендации по выполнению копирования содержимого оперативной памяти СВТ и получению данных операционных систем.

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операционных систем рекомендуется выполнять с соблюдением следующих правил:

– все программные средства, используемые для копирования оперативной памяти СВТ и получения данных операционных систем, следует размещать на специально выделенных для этих целей носителях, в отношении которых приняты меры по обеспечению защиты от записи или несанкционированного изменения;
– для копирования оперативной памяти СВТ и получения данных операционных систем следует использовать только программные средства, размещенные на указанном выше защищенном носителе;
– для исполняемых модулей программных средств, используемых для копирования оперативной памяти СВТ и получения данных операционных систем, должны быть известны наименования порождаемых ими программных процессов (для их исключения из рассмотрения при дальнейшем анализе).

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операционных систем должно сопровождаться описанием и протоколированием:

– всех выполненных процедур и сервисных команд, использованных программных средств, примененных для копирования содержимого оперативной памяти СВТ и получения данных операционных систем (наименование, версия, лицензионные сведения, точные сервисные команды и параметры команд);
– контрольной суммы или значения хэш-функций исполняемых файлов программных средств, используемых для копирования оперативной памяти СВТ и получение данных операционных систем;
– даты и времени выполнения процедур и сервисных команд.

Рекомендуемым решением является предварительная подготовка, размещение на специально выделенном носителе и использование программного пакета (скрипта), содержащего все выполняемые процедуры и сервисные команды, необходимые для копирования содержимого оперативной памяти СВТ и получения данных операционных систем.

Выполнение копирования содержимого оперативной памяти СВТ и получение данных операционных систем рекомендуется выполнять в следующем порядке:

– получение данных операционных систем:
  • сетевые соединения;
  • список открытых сессий доступа;
– копирование содержимого оперативной памяти;
– получение данных операционных систем:
  • список запущенных программных процессов;
  • список открытых файлов;
  • сетевые конфигурации;
  • системное время операционной системы с указанием часового пояса.

Дополнительно следует выполнить описание и протоколирование наименования операционной системы, включая данные обо всех установленных обновлениях.

[1] Выполнение операций, указанных в пунктах 4 и 6, технически неприменимо в случае копирования данных с SSD-носителя.

Для выполнения копирования содержимого оперативной памяти СВТ и получения данных операционных систем рекомендуется следующая последовательность действий и операций:

1) выполнение копирования содержимого оперативной памяти СВТ и получение данных операционной системы с использованием программных средств, размещенных на специально выделенных для этих целей носителях, с сохранением полученных результатов в файлах данных, размещенных на накопителе на жестких магнитных дисках СВТ или в файлах данных, размещенных на внешнем носителе информации[1];
2) отключение СВТ путем прерывания питания[2];
3) загрузка операционной системы с предварительно созданного "доверенного" загрузочного носителя, содержащего необходимые программные средства для выполнения логического копирования файлов данных, программные средства вычисления контрольных сумм или значений хэш-функций, программные средства использования запоминающих устройств в режиме "только для чтения";
4) вычисление и сохранение контрольной суммы или значения хэш-функций файлов данных, размещенных на накопителе на жестких магнитных дисках СВТ или внешнем носителе информации, созданных в рамках выполнения пункта 1;
5) в случае сохранения полученных результатов в файлах данных, размещенных на накопителе на жестких магнитных дисках СВТ:

- логическое копирование на внешние носители информации исходных файлов данных, размещенных на накопителе на жестких магнитных дисках СВТ, созданных в рамках выполнения пункта 1;
- вычисление и сохранение контрольных сумм или значений хэш-функций исходных файлов данных, созданных в рамках выполнения пункта 1, и полученных файлов данных, скопированных в рамках выполнения пункта 5, сравнение вычисленного значения со значениями, вычисленными в рамках выполнения пункта 4, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;

6) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные файлы.

В качестве внешних носителей информации рекомендуется использование носителей информации, дополнительная запись и (или) перезапись данных на которые невозможна, например, путем выполнения процедуры "финализации" для компакт-дисков, или использование специального аппаратного ограничителя записи – "write-blocker".

6.6.3. Рекомендации по выполнению копирования протоколов (журналов) регистрации.

В настоящем стандарте предусматривается целесообразность копирования следующих протоколов (журналов) регистрации:

– протоколы (журналы) регистрации целевых систем;
– протоколы (журналы) регистрации телекоммуникационного оборудования:
  - маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
  - DHCP-сервисы;
  - средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
– протоколы (журналы) регистрации средств защиты информации:
  - средства (системы) аутентификации, авторизации и разграничения доступа;
  - средства межсетевого экранирования;
  - средства обнаружения вторжений и сетевых атак, в том числе DDOS-атак;
  - средства защиты от НСД;
  - средства антивирусной защиты информационной инфраструктуры;
  - СКЗИ;
– протоколы (журналы) регистрации и данные почтовых серверов, средств контентной фильтрации электронной почты;
– протоколы (журналы) регистрации и данные web-серверов, средств контентной фильтрации web-протоколов;
– протоколы (журналы) регистрации СУБД;
– протоколы (журналы) регистрации автоматических телефонных станций;
– протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа;

---

[1] Рекомендованным решением является сохранение результатов получения содержимого оперативной памяти СВТ и данных операционной системы в файлах данных, размещенных на внешнем носителе информации, с целью минимизации воздействия на данные запоминающих устройств СВТ, являющихся источниками технических данных.

[2] Прерывание питания осуществляется с учетом описанных выше особенностей данной операции.

В большинстве случаев указанные протоколы (журналы) регистрации хранятся в виде файлов данных, в том числе в проприетарных форматах, текстовых файлах, базах данных, протоколов (журналов) регистрации операционных систем (syslog для UNIX систем, event logs для Windows-систем). При этом для копирования протоколов (журналов) регистрации может быть рекомендована следующая общая последовательность действий:

1) выгрузка (копирование) протоколов (журналов) регистрации за определенный требуемый период времени в файлы данных;
2) вычисление и сохранение контрольных сумм или значений хэш-функций полученных файлов данных;
3) логическое копирование на внешние носители информации (компакт-диски) исходных файлов данных, созданных в рамках выполнения пункта 1;
4) вычисление и сохранение контрольных сумм или значений хэш-функций исходных файлов данных, созданных в рамках выполнения пункта 1, и полученных файлов данных, скопированных в рамках выполнения пункта 3, сравнение вычисленных значений со значениями, вычисленными в рамках выполнения пункта 2, для подтверждения целостности скопированных данных с составлением акта, содержащего полученный результат сравнения;
5) обеспечение безопасной упаковки и хранения носителей информации, содержащих скопированные файлы.

При выполнении копирования протоколов (журналов) и данных телекоммуникационного оборудования необходимо учитывать, что отключение телекоммуникационного оборудования путем прерывания питания, как правило, приводит к удалению всех технических данных. Копирование протоколов (журналов) телекоммуникационного оборудования рекомендуется сопровождать получением данных о его текущем статусе:

- системные дата и время;
- версия программного обеспечения;
- значения контрольных сумм программного обеспечения;
- сетевая информация, таблица маршрутизации;
- текущая конфигурация оборудования;
- конфигурация оборудования, примененная при загрузке;
- состав администраторов оборудования;
- состав запущенных программных процессов.

При копировании протоколов (журналов) регистрации и данных телекоммуникационного оборудования рекомендуется подключение к телекоммуникационному оборудованию через консольный порт (не рекомендуется выполнять удаленное подключение через протоколы Telnet или SSH), при этом категорически не рекомендуется изменять конфигурацию маршрутизатора или вводить какие-либо команды конфигурации.

При организации копирования протоколов (журналов) регистрации рекомендуется обеспечивать:

- принятие необходимых мер к ограничению доступа к собираемым копиям данных с учетом возможного нахождения в копиях данных информации, защищаемой в соответствии с требованиями законодательства Российской Федерации, нормативными актами Банка России, в том числе:
  - персональных данных;
  - аутентификационных данных;
  - данных, используемых для подтверждения распоряжений на перевод денежных средств;
  - банковской тайны;
- принятие мер к обеспечению достаточной емкости носителей и хранилищ, используемых для сбора протоколов (журналов) регистрации, позволяющих избежать перезаписи и (или) потери информации;
- использование специализированных технических средств централизованного сбора, анализа и хранения протоколов (журналов) регистрации (например, систем управления журналами регистрации, SIEM систем), позволяющих минимизировать риски злоумышленных действий по изменению, повреждению и (или) уничтожению протоколов (журналов) регистрации;
- заблаговременное включение в договоры положений, определяющих условия и процедуры получения протоколов (журналов) регистрации СВТ и иных технических средств, находящихся в собственности третьих лиц (например, протоколов (журналов) регистрации почтовых сервисов, сервисов обнаружения и отражения DDOS-атак, технических средств провайдеров сети Интернет и операторов мобильной связи).

6.6.4. Рекомендации по выполнению копирования сетевого трафика.

Для сбора данных сетевого трафика для цели реагирования на инциденты ИБ рекомендуется использование технических средств мониторинга и копирования сетевых пакетов (packet sniffer), а также технических средств, позволяющих автоматизировать анализ собранных сетевых пакетов.

Сбор данных сетевого трафика рекомендуется осуществлять в определенных точках вычислительных сетей, обеспечивающих копирование данных, значимых и существенных для расследования инцидента ИБ, например:

– для информационной инфраструктуры клиента – данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ (настольные компьютеры, ноутбуки), используемые клиентом для осуществления доступа к системам ДБО;
– для информационной инфраструктуры организации БС РФ – данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ целевых систем.

Для копирования файлов данных формируемых техническими средствами мониторинга и копирования сетевых пакетов (packet sniffer) может быть использована последовательность действия, определенная в настоящем стандарте для копирования протоколов (журналов) регистрации.

При организации копирования протоколов (журналов) регистрации рекомендуется обеспечивать принятие необходимых мер к ограничению доступа к собираемым копиям данных с учетом возможного нахождения в копиях данных информации, защищаемой в соответствии с требованиями законодательства Российской Федерации, нормативными актами Банка России, и обеспечению достаточной емкости носителей и хранилищ, используемых для сбора данных сетевого трафика, позволяющих избежать перезапись и (или) потерю информации, значимой для цели реагирования на инциденты ИБ.

6.7. Рекомендации по обеспечению безопасной упаковки, хранения и транспортировки носителей собранных данных.

Копии технических данных, используемые в качестве доказательной базы, должны храниться безопасным образом.

Рекомендуется учитывать, что носители собранных технических данных являются хрупкими и чувствительными к экстремальным температурам, влажности, механическим ударам, воздействию света, статическому электричеству и электромагнитным полям.

При проведении упаковки носителей собранных технических данных рекомендуется:

– маркирование и учет носителей собранных технических данных;
– упаковка носителей собранных технических данных и соответствующих сопроводительных описаний и протоколов в антистатические пакеты или контейнеры, включая использование бумажных пакетов, конвертов, коробок. Не рекомендуется использование пластиковых пакетов или контейнеров;
– маркирование пакетов или контейнеров, используемых для хранения носителей собранных технических данных;
– предотвращение деформации и царапин носителей собранных технических данных.

При хранении и транспортировке носителей собранных технических данных рекомендуется:

– обеспечить хранение и транспортировку носителей собранных технических данных вдали от электромагнитных полей;
– исключить хранение носителей собранных технических данных в транспортных средствах в течение длительного времени;
– обеспечение защиты носителей собранных технических данных от ударов и вибраций, влаги или пыли;
– обеспечение защиты от воздействия экстремальных температур и влажности;
– обеспечение контроля работоспособности в течение требуемого времени для технических средств, использующих батарейки и (или) аккумуляторы.

Рекомендуется применять способ упаковки носителей эталонных копий собранных технических данных и соответствующих сопроводительных описаний и протоколов, обеспечивающий невозможность доступа к носителю и (или) использования носителя без видимого нарушения целостности упаковки. Одним из допустимых способов упаковки и опечатывания носителей небольшого размера является их совместное помещение в полиэтиленовый антистатический пакет с последующей перевязкой его горловины нитью, концы которой опечатываются с наклеиванием пояснительной записки, нанесенной шариковой ручкой, с подписями участвующих в опечатывании лиц и печатью организации БС РФ.

7. Рекомендации по проведению поиска (выделения) содержательной (семантической) информации, ее анализу и оформлению

7.1. Основными целями выполнения процедур, связанных с поиском (выделением) в технических данных и последующим анализом содержательной (семантической) информации являются:
- определение технических способов и схем реализаций угроз ИБ;
- проведение идентификации субъектов, реализующих угрозы ИБ;
- выявление маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры[1], используемых для осуществления переводов денежных средств.

7.2. Для обеспечения возможности выполнения процедур, связанных с поиском (выделением) в технических данных и последующим анализом содержательной (семантической) информации организации БС РФ рекомендуется:
- обеспечить участие компетентных аналитиков в области анализа технических данных;
- обеспечить наличие необходимых технических средств и инструментов для выделения и анализа содержательной (семантической) информации;
- определить и обеспечить выполнение правил документирования выделенной содержательной (семантической) информации и результатов ее анализа.

7.3. Для проведения поиска (выделения) и анализа содержательной (семантической) информации организации БС РФ рекомендуется выполнение следующего общего алгоритма действий:
- определить для каждого инцидента ИБ из числа указанных в пункте 6.1 настоящего стандарта перечень событий ИБ, значимых для поиска (выделения) и анализа содержательной (семантической) информации:
  - исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа;
  - события ИБ или их группа, потенциально имеющие отношение или связанные с инцидентом ИБ;
- провести непосредственный поиск (выделение) из технических данных содержательной (семантической) информации, связанной с указанными событиями ИБ;
- провести анализ, в том числе корреляционный и сравнительный, выделенной содержательной (семантической) информации, в том числе для достижения целей, указанных в пункте 7.1 настоящего стандарта.

7.4. В большинстве случаев деятельность по поиску (выделению) и анализу содержательной (семантической) информации не может быть формализована, а результат ее выполнения определяется опытом и компетенцией аналитика.

Для цели повышения качества и оперативности поиска (выделения) и анализа содержательной (семантической) информации организации БС РФ рекомендуется:
- использование специализированных технических средств и систем централизованного сбора, анализа и хранения протоколов (журналов) регистрации (например, систем управления журналами регистрации или SIEM систем);
- использование известных маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, которые могут быть разработаны аналитиками организации БС РФ самостоятельно или получены из внешних источников, осуществляющих реагирование на инциденты ИБ, например, от FinCert Банка России.

7.5. В составе основных событий ИБ организации БС РФ рекомендуется рассматривать следующие:
- события, связанные с идентификацией и аутентификацией администраторов и эксплуатационного персонала, программных процессов (сервисов), клиентов и участников платежной системы (далее при совместном упоминании – субъекты доступа) в целевых системах и информационной инфраструктуре размещения целевых систем и информационной инфраструктуре клиентов;
- события, связанные с управлением доступом в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;
- события, связанные с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;
- события, связанные с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;

[1] Также указанные данные известны под общим наименованием “индикаторы компрометации, indicators of compromise, IOC”.

– события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;
– события, связанные с антивирусной защитой;
– события, связанные с выполнением криптографических преобразований;
– события, связанные с функционированием средств защиты от несанкционированного доступа;
– события, связанные с осуществлением информационного взаимодействия на всех уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.6. Для инцидентов ИБ, связанных с НСД к объектам информационной инфраструктуры клиентов или информационной инфраструктуре целевых систем, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:
– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:
  • события, связанные с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;
  • события, связанные с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем;
  • события, связанные с выполнением криптографических преобразований;
– события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:
  • события, связанные с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиента;
  • события, связанные с управлением доступом в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;
  • события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем, информационной инфраструктуры клиентов;
  • события, связанные с функционированием средств защиты от несанкционированного доступа;
  • события, связанные с антивирусной защитой;
  • события, связанные с выполнением криптографических преобразований;
  • события, связанные с осуществлением информационного взаимодействия на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
– события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:
  • события, связанные с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов;
  • события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
– события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:
  • события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуре клиентов;
  • события, связанные с функционированием средств защиты от несанкционированного доступа;
  • события, связанные с антивирусной защитой;
  • события, связанные с осуществлением информационного взаимодействия на сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.7. Для инцидентов ИБ, связанных со спам-рассылками, осуществляемыми в отношении клиентов, осуществляемых в рамках реализации методов “социального инжиниринга”, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:
– исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа, а также события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:

  - события, связанные с осуществлением информационного взаимодействия с почтовыми серверами на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
  - события, связанные с функционированием почтовых серверов, средств контентной фильтрации электронной почты;
- события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ, а также события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:
  - события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
  - события, связанные с осуществлением информационного взаимодействия с почтовыми серверами на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
  - события, связанные с функционированием почтовых серверов, средств контентной фильтрации электронной почты.

7.8. Для инцидентов ИБ, связанных с реализацией атак типа “отказ в обслуживании” (DDOS-атаки), реализуемых применительно к информационной инфраструктуре клиентов, систем ДБО и систем фронт-офиса организации БС РФ, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:
- исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:
  - события, связанные с осуществлением информационного взаимодействия на сетевом уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
- события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:
  - события, связанные с осуществлением информационного взаимодействия на сетевом и транспортном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
- события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:
  - события, связанные с изменением состояния информационной инфраструктуры СВТ бот-сетей;
  - события, связанные с антивирусной защитой СВТ бот-сетей;
  - события, связанные с осуществлением информационного взаимодействия информационной инфраструктуры СВТ бот-сетей на сетевом и транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
- события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:
  - события, связанные с изменением состояния информационной инфраструктуры СВТ бот-сетей.

7.9. Для инцидентов ИБ, связанных с деструктивным воздействием компьютерных вирусов на информационную инфраструктуру организации БС РФ и клиентов, рекомендуется рассмотрение следующих событий ИБ, значимых для цели поиска (выделения) и анализа содержательной (семантической) информации:
- исходные (базовые) события ИБ или их группа, являющиеся отправной точкой дальнейшего поиска и анализа:
  - события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;
  - события, связанные с функционированием средств защиты от несанкционированного доступа;
  - события, связанные с антивирусной защитой;
- события ИБ или их группа, информация о которых потенциально может быть использована для определения технических способов и схем реализаций угроз ИБ:
  - события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;
  - события, связанные с функционированием средств защиты от несанкционированного доступа;
  - события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;

– события ИБ или их группа, информация о которых потенциально может быть использована для проведения идентификации субъектов, реализующих угрозы ИБ:
  • события, связанные с антивирусной защитой;
  • события, связанные с осуществлением информационного взаимодействия на аппаратном (физическом), сетевом, транспортном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91;
– события ИБ или их группа, информация о которых потенциально может быть использована для выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры, используемых для осуществления переводов денежных средств:
  • события, связанные с изменением состояния информационной инфраструктуры размещения целевых систем и информационной инфраструктуры клиентов;
  • события, связанные с функционированием средств защиты от несанкционированного доступа;
  • события, связанные с антивирусной защитой;
  • события, связанные с осуществлением информационного взаимодействия на прикладном уровне модели взаимодействия открытых систем, определенной в ГОСТ 28906-91.

7.10. Для событий ИБ, связанных с идентификацией и аутентификацией субъектов доступа в целевых системах и информационной инфраструктуре размещения целевых систем, информационной инфраструктуры клиентов аналитику может быть рекомендовано рассмотрение следующей информации:

энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

– информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:
  • конфигурационная информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;
  • конфигурационная информация о составе пользователей – субъектов доступа, включая информацию о составе учетных записей пользователей, статусах учетных записей пользователей;
– информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:
  • информация, связанная с выполнением операций идентификации и аутентификации;
  • информация, связанная с изменением аутентификационных данных субъектов доступа;

энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

– информация о сетевых соединениях;
– информация об открытых сессиях доступа;

протоколы (журналы) регистрации целевых систем, средств (систем) аутентификации, авторизации и разграничения доступа, СУБД:

– информация о действиях и операциях, связанных с неуспешными попытками доступа к целевым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД;
– информация об идентификации и аутентификации субъектов доступа в целевых системах, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД;
– информация о неуспешных попытках выполнения идентификации и аутентификации субъектов доступа в целевых системах, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов и СУБД, в том числе связанных с невозможностью получения данных от систем аутентификации;
– информация, связанная с изменением аутентификационных данных субъектов доступа;
– информация о составе субъектов доступа, включая информацию о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа.

7.11. Для событий ИБ, связанных с осуществлением доступа к целевым системам и информационной инфраструктуре размещения целевых систем, аналитику может быть рекомендовано рассмотрение следующей информации:

энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

– информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:
  • информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;

- информация о составе субъектов доступа, включая информацию о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа, о включении учетных записей субъектов доступа в группы;
- информация о правах доступа, предоставленных субъектам доступа и группам;
- информация о статусах учетных записей субъектов доступа;
- информация о пользовательских настройках, информация о домашней директории пользователя – субъекта доступа;

– информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:
- информация, связанная с выполнением авторизации субъектов доступа;
- информация об истории выполненных субъектами доступа команд (command history);
- информация об использовании субъектами доступа файлов данных (recently accessed files);
- информация об использовании субъектами доступа ресурсов сети Интернет (история web-браузера);

энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

– информация об операциях, связанных с осуществлением доступа к файлам данных;
– информация о сетевых соединениях;
– информация о запущенных программных процессах;
– информация об открытых файлах данных;
– информация об открытых сессиях доступа;

протоколы (журналы) регистрации целевых систем, средств (систем) аутентификации, авторизации и разграничения доступа, СУБД:

– информация об операциях, связанных с управлением доступом субъектов доступа к целевым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД:
  - информация о составе учетных записей субъектов доступа, статусах учетных записей субъектов доступа;
  - информация о действиях и операциях, связанных с изменением состава и значений атрибутов учетных записей;
  - информация о действиях и операциях, связанных с блокированием (разблокированием) учетных записей;
  - информация о действиях и операциях, связанных с предоставлением, блокированием и (или) прекращением предоставления логического доступа;
  - информация о действиях и операциях, связанных с изменением прав доступа;
  - информация о действиях и операциях, связанных с созданием, изменением, удалением роли, группы;
  - информация о действиях и операциях, связанных с изменением прав доступа роли, группы;
  - информация о действиях и операциях, связанных с назначением ролей (изменением состава групп);
– информация о действиях и операциях, связанных с осуществлением доступа субъектов доступа к целевым системам, информационной инфраструктуре размещения целевых систем, информационной инфраструктуре клиентов, СУБД:
  - информация об авторизации, завершении и (или) прерывании (приостановке) осуществления доступа;
  - информация о действиях и операциях, выполненных субъектами доступа;
  - информация о неуспешных попытках доступа;
  - информация о выполненных субъектами доступа действий и операций, для которых не требуется выполнения предварительной идентификации и аутентификации;
  - информация о выполненных DML-операторах, операторе SELECT- и DDL-операторах;
– информация об изменении конфигурационных данных целевых систем, информационной инфраструктуры целевых систем, СУБД;
– информация об атрибутах выполненных операций в целевых системах, информационной инфраструктуры целевых систем, СУБД:
  - информация о содержании выполненной операции;
  - дата и время осуществления операции;
  - результат выполнения операции (успешная или неуспешная);
  - идентификационные данные субъекта доступа, выполнившего операцию;
  - идентификационные данные СВТ, которое использовалось для выполнения операции.

7.12. Для событий ИБ, связанных с осуществлением удаленного доступа к целевым системам и информационной инфраструктуре размещения целевых систем, аналитику может быть рекомендовано рассмотрение следующей информации:

энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

– информация операционных систем о действиях и операциях по удаленному доступу к объектам файловой системы (загрузка, скачивание, создание, удаление файлов, получение доступа к файлам);

энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

– информация о сетевых конфигурациях;
– информация о сетевых соединениях;
– информация об открытых сессиях доступа;

протоколы (журналы) регистрации телекоммуникационного оборудования, средств межсетевого экранирования, средств обнаружения и предотвращения атак и данные сетевого трафика на сеансовом и прикладном уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:

- информация об установке и окончании сессии взаимодействия на сеансовом уровне;
- информация об использованных идентификаторах субъектов доступа;
- информация о выполняемых операциях и командах, результатах их выполнения;
- информация о возможных реализациях вторжений (атак), в том числе информация о типе реализуемой атаки (например, атака типа “переполнение буфера”, SQL-инъекция), об использованной уязвимости, результативности реализации атаки.

7.13. Для событий ИБ, связанных с изменением информационной инфраструктуры размещения целевых систем, информационной инфраструктуры клиентов, аналитику может быть рекомендовано рассмотрение следующей информации:

энергонезависимые технические данные, расположенные на запоминающих устройствах СВТ:

– информация о составе и атрибутах файлов данных, в том числе исполняемых файлов данных, файлов данных программного обеспечения, командных файлов данных и скриптов, файлов данных, потенциально содержащих мобильный код и исполняемые макросы, файлов документов;
– информация о реализации операций с использованием функций файловой системы (операционной системы), в том числе самокопирование, захват иных файлов данных, передача файлов данных;
– информация конфигурационных файлов данных операционных систем и приложений целевых систем, информация системного реестра операционной системы Windows:
  - информация о программных сервисах, запускаемых автоматически при загрузке операционной системы;
  - информация об установленном программном обеспечении, его обновлениях;
  - информация об обновлениях операционной системы;
  - конфигурационная информация, определяющая размещение файлов протоколов (журналов) регистрации (log-файлов) и временных файлов;
  - информация о запланированных задачах (scheduled jobs), включая информацию о наименовании запланированной задачи, составе выполняемых команд, программ и операций запланированной задачи, планируемых датах и времени выполнения запланированной задачи;
– информация о составе и атрибутах скрытых и удаленных исполняемых файлов данных;
– информация о составе, атрибутах и содержании временных файлов данных;
– информация о порождаемых исполняемыми файлами данных программных процессах;
– информация о составе и атрибутах скрытых исполняемых файлов данных и исполняемых файлов данных, расположенных в скрытых директориях файловых систем;
– информация о составе и атрибутах исполняемых файлов данных, расположенных в неиспользуемых областях в пределах логических модулей выделения файлового пространства (file slack space);
– информация о составе и атрибутах исполняемых файлов данных, расположенных в неиспользуемом пространстве файловой системы (free space);
– содержательная информация об атрибутах и содержании файлов данных:
  - дата и время создания файла;
  - дата и время последней модификации файла;
  - дата и время последнего доступа к файлу;
  - дата и время последнего изменения атрибутов файла, в том числе атрибутов, связанных с изменением прав доступа к файлу и владельца файла данных (inode change);
  - размер файла данных, место размещения в файловой системе;
  - формат или структура файла данных;

- наличие объектов, внедренных в файл данных;
- используемые (реализуемые) исполняемым файлом данных программных интерфейсах (API);
- значение вычисления хэш-функции файла данных;
- сетевые соединения, инициируемые или принимаемые исполняемыми файлами данных;
- дополнительные атрибуты файлов данных файловой системы NTFS (alternate data stream, ADS);

– информация протоколов (журналов) регистрации (system events, application events, audit records) операционных систем и приложений целевых систем:
- информация о загрузке и завершении работы операционной системы;
- информация об изменении конфигурационных данных операционных систем;
- информация о загрузке, выгрузке и изменении функционирования драйверов физических и виртуальных устройств;
- информация об изменении состава или обновлении программного обеспечения;
- информация о подключении и отключении устройств, в том числе отчуждаемых и мобильных устройств;
- информация о запускаемых программных процессах и сервисах;
- информация о составе и работе системных служб (запуск, остановка, возобновление, завершение, удаление, блокирование системных служб);
- информация об ошибках программного обеспечения;
- информация об изменении состава запланированных задачах (scheduled jobs), операциях по управлению расписанием запланированных задач;

энергозависимые технические данные операционных систем и данные, расположенные в оперативной памяти СВТ:

– информация, полученная из неиспользуемых областей в пределах логических страниц или блоков выделения пространства оперативной памяти (memory slack space):
– информация, полученная из неиспользуемого пространства оперативной памяти (memory free space, garbage):
– информация о сетевых конфигурациях;
– информация о сетевых соединениях;
– информация о запущенных программных процессах;
– информация об открытых файлах данных;
– информация об открытых сессиях доступа;
– информация о системных дате и времени операционной системы, включая информацию о часовом поясе;

данные, связанные с функционированием СУБД:

– информация о создании резервных копий баз данных и их восстановлении из резервных копий;
– информация об изменении конфигурационных данных СУБД и баз данных;
– информация об операциях, связанных с созданием, вызовом, загрузкой программных модулей и хранимых процедур и функций, в том числе внешних хранимых процедур (DDL-процедур).

7.14. Для событий ИБ, связанных с антивирусной защитой, аналитику может быть рекомендовано рассмотрение следующей информации:
– информация о выполненных операциях по установке и обновлению средств антивирусной защиты;
– информация о выполненных операциях по обновлению сигнатурных баз средств антивирусной защиты;
– информация о фактах обнаружения и удаления (в том числе неуспешных) компьютерных вирусов;
– информация о выполненных операциях по отключению антивирусных средств;
– информация о выполненных операциях по проверке отсутствия компьютерных вирусов;
– информация о сбоях в работе средств антивирусной защиты;
– информация о результатах выполнения проверок целостности программных средств антивирусной защиты;
– информация о случаях выявления использования технологии мобильного кода (Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии).

7.15. Для событий ИБ, связанных с выполнением криптографических преобразований, аналитику может быть рекомендовано рассмотрение следующей информации:
– информация о выполненных операциях по криптографическому преобразованию информации при осуществлении переводов денежных средств;
– информация о выполненных операциях проверки электронной подписи в рамках осуществления переводов денежных средств;

7.16. Для событий ИБ, связанных с функционированием средств защиты от несанкционированного доступа, аналитику может быть рекомендовано рассмотрение следующей информации:

– информация о запуске программных процессов и сервисов;
– информация об установке, обновлении и (или) изменении состава программного обеспечения;
– информация о результатах выполнения доверенной загрузки операционных систем;
– информация о результатах выполнения операций по контролю состава, целостности программного обеспечения, контроля состава программного обеспечения, запускаемого при загрузке операционной системы.

7.17. Для событий ИБ, связанных с осуществлением информационного взаимодействия на всех уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91, аналитику может быть рекомендовано рассмотрение следующей информации:

протоколы (журналы) регистрации телекоммуникационного оборудования, средств межсетевого экранирования, средств обнаружения и предотвращения атак и данные сетевого трафика:

– информация аппаратного (физического) и канального уровней по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:
  • MAC-адреса сетевых карт источника и получателя данных;
  • данные о протоколе канального уровня (EtherType value);
  • информация об изменениях состояния сетевого интерфейса на аппаратном (физическом) и канальном уровне, в том числе подключение к вычислительной сети, изменение параметров, отключение от вычислительной сети, физическое отсоединение от сети;
– информация сетевого уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:
  • IP-адреса источника и получателя данных;
  • дата, время и результаты обработки сетевых пакетов;
  • идентификатор и информация о протоколе сетевого и транспортного уровня (IP protocol number, например, TCP, UDP, ICMP);
  • базовая информация используемого протокола (например, номер порта TCP или UDP, ICMP-тип и код);
  • информация о результатах выполнения операций адресации и маршрутизации (status information) и возникающих при этом ошибках (error information);
  • информация об адресах, портах и результатах выполнения NAT-преобразований;
  • информация о результатах установления и отклонения PROXY-соединений;
  • информация о назначении IP-адресов DHCP и DNS-сервисов, в том числе дата и время обработки назначения (высвобождения) IP-адреса, MAC-адреса средств вычислительной техники, результаты назначения IP-адреса, информация о соответствии MAC-адресов и IP-адресов;
  • информация VPN-шлюзов об установлении взаимодействия на сетевом уровне, в том числе IP-адреса источника и получателя данных, дата и время обработки сетевых пакетов;
  • информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;
  • информация о результатах применения правил фильтрации информационных потоков;
– информация транспортного уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:
  • информация об установке и окончании соединений по протоколам TCP, UDP, ICMP;
  • информация о номерах сетевых портов (ports) источника и получателя данных протоколов TCP и UDP, которые потенциально могут указывать на программное обеспечение, используемое для обмена данными;
  • информация о состоянии интерфейсов транспортного уровня взаимодействия (сокетов), в том числе создание сокета, переход в режим ожидания соединения, отправка и прием запроса на соединение, завершение соединения, удаление сокета;
  • информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;
  • информация о результатах применения правил фильтрации информационных потоков;
– информация сеансового и прикладного уровня по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:
  • данные, передаваемые по протоколу NetFlow;
  • информация об установке и окончании сессии взаимодействия на сеансовом уровне;
  • идентификатор и информация о протоколе прикладного уровня;

- информация об использованных идентификаторах субъектов доступа;
- информация о выполняемых операциях и командах, результатах их выполнения;
- информация о возможных реализациях вторжений (атак), в том числе информация о типе реализуемой атаки (например, атака типа “переполнение буфера”, SQL-инъекция), об использованной уязвимости, результативности реализации атаки;
- информация о создании, активации, деактивации, удалении правил фильтрации информационных потоков;
- информация о результатах применения правил фильтрации информационных потоков;
- информация о создании, изменении, удалении доверительных отношений между доменами;

протоколы (журналы) регистрации и данные почтовых серверов, средств контентной фильтрации электронной почты:

– информация “заголовков” почтовых сообщений:
  - информация о почтовых адресах отправителя и получателя почтового сообщения;
  - информация о дате и времени отправления почтовых сообщений;
  - информация о “теме” почтового сообщения;
  - информация об идентификационных номерах почтовых сообщений (message ID);
  - информация о типе почтового клиента, использованного для формирования почтового клиента;
  - информация о “степени важности” почтового сообщения;
  - информация о маршрутизации почтового сообщения (перечень транзитных почтовых серверов прохождения почтового сообщения, дата и время приема почтового сообщения указанными почтовыми серверами);
– информация “тела” почтового сообщения:
  - содержание почтового сообщения;
  - информация о типе содержимого почтового сообщения (например, простой текст, наличие графики, наличие прикрепленных файлов);
  - информация о наличии прикрепленных файлов и содержание прикрепленных файлов;
  - информация о наличии и содержании гиперссылок.

протоколы (журналы) регистрации и данных web-серверов, средств контентной фильтрации web-протоколов:

– информация о дате и времени получения запроса, результате выполнения запроса (status code);
– информация об IP-адресе инициатора запроса;
– информация о СВТ, с использованием которого сформирован запрос:
  - информация о web-браузере, сформировавшем запрос;
  - информация об операционной системе средства вычислительной техники, использованного для формирования запроса;
– информация о типе запроса (получение данных, запись данных);
– информация о ресурсе доступа, в отношении которого выполнен запрос.

7.18. Особое внимание при анализе аналитику рекомендуется уделять следующей содержательной (семантической) информации.

Инциденты ИБ, связанные с НСД к объектам информационной инфраструктуры клиентов или информационной инфраструктуры целевых систем:

– информация о попытках подбора пароля, заключающаяся в наличии существенного количества попыток доступа с использованием “привилегированных” учетных записей, в том числе “встроенных” учетных записей (например, root, Administrator), результатом которых может являться успешная авторизация;
– информация о попытках осуществления доступа в нетипичное время (например, ночью). При этом следует учитывать различия в возможных часовых поясах нахождения аналитика и места сбора технических данных;
– информация о нетипичном поведении субъектов доступа при осуществлении доступа (в том числе наличие существенного количества сбоев авторизации, слишком ранняя или слишком поздняя попытка доступа и авторизации, нехарактерная для данного пользователя активность при осуществлении доступа);
– информация о попытках осуществления доступа субъектами доступа к системам и ресурсам, которые не требуются ему для выполнения служебных обязанностей;
– информация о существенном изменении состава внешних IP/DNS-адресов либо наличии постоянного сетевого трафика на IP/DNS-адреса, находящиеся вне территории РФ, что может свидетельствовать о заражении средства вычислительной техники компьютерными вирусами;

– информация о попытках установления входящих соединений с IP-адресами, находящимися вне территории РФ;
– информация о попытках установления входящих соединений в обход эксплуатируемого VPN-шлюза;
– информация о доступе к протоколам (журналам), содержащим информацию о событиях ИБ.

Инциденты ИБ, связанные с реализацией атак типа “отказ в обслуживании” (DDOS-атаки), реализуемые применительно к информационной инфраструктуре клиентов, систем ДБО и систем фронт-офиса организации БС РФ:

– информация о предварительных признаках DDOS-атак в виде кратковременных, нетипичных “всплесков” сетевого трафика, которые могут свидетельствовать о проведении злоумышленниками тестирования устойчивости информационной инфраструктуры организации БС РФ к DDOS-атакам;
– сравнительная информация о составе IP-адресов в период осуществления DDOS-атаки и IP-адресов за определенный период до реализации DDOS-атаки, позволяющая идентифицировать реальные IP-адреса лиц, осуществляющие атаки;
– информация о наличии угроз (вымогательств), связанных с предполагаемым началом DDOS-атаки. Такие угрозы могут попадать в организацию БС РФ через общедоступные (информационные) почтовые ящики, официальных представителей (пресс-службы) организации БС РФ, а также через работников организации БС РФ, адреса которых есть у злоумышленника.

Инциденты ИБ, связанные с деструктивным воздействием компьютерных вирусов на информационную инфраструктуру организации БС РФ и клиентов:

– информация о дате и времени появления компьютерных вирусов на СВТ организации БС РФ;
– информация о выявлении антивирусными средствами компьютерных вирусов, о наличии “в карантине” антивирусного средства зараженных файлов за интересующий период времени и (или) диапазон дат;
– информация о классификации производителем антивирусного средства компьютерных вирусов и исходном местоположении выявленных компонентов компьютерных вирусов на СВТ организации БС РФ;
– информация о наличии постоянного и (или) периодического исходящего или входящего сетевого трафика небольшого объема на сетевые адреса за пределами РФ либо сетевые адреса, находящиеся в РФ, но не принадлежащие списку IP-адресов, с которыми организация ведет разрешенный обмен данными;
– информация о нетипичных маршрутах прохождения сетевого трафика и нетипичных маршрутных таблицах сетевого оборудования;
– информация о наличии посторонних программных процессов, похожих на системные программные процессы, но запущенные либо из нетипичного места (временные папки, папки перемещаемых профилей), либо программных процессов, имеющих схожее название с системными;
– информация о наличии файлов и папок, похожих на “системные” файлы и папки, но находящихся в отличном от стандартного размещения местоположении в файловой системе (например, папка Windows Update в корне папки Windows);
– информация о наличии нехарактерного для организации БС РФ программного обеспечения, запускаемого при запуске операционной системы СВТ, в том числе в папках автозагрузки, в службах, в системных драйверах, в системном реестре операционной системы Windows, в планировщике задач, в иных специфических местах, определяемых типом операционной системы;
– информация о наличии в протоколах (журналах) регистрации операционных систем или специализированного программного обеспечения данных о подключении устройств;
– информация о наличии в протоколах (журналах) регистрации серверов электронной почты входящих электронных сообщений с адресов электронной почты, имеющих схожее написание с доменами государственных учреждений, либо с доменов, переписка с которыми не характерна для деятельности организации БС РФ.

7.19. Для проведения анализа содержательной (семантической) информации аналитику могут быть рекомендованы следующие общие стратегии.

Стратегия анализа в определенном временном диапазоне, которая может быть использована в случае наличия у аналитика сведений о дате и времени исходного (базового) интересующего события ИБ или их группы. Аналитику могут быть рекомендованы следующие методы анализа:

– анализ содержательной информации об атрибутах файлов данных с целью определения состава файлов данных и последующего анализа содержания файлов данных, созданных и (или) модифицированных за временной диапазон, связанный с инцидентом ИБ;
– анализ состава и содержания протоколов (журналов) регистрации за временной диапазон, связанный с инцидентом ИБ.

Стратегия анализа умышленно скрытых данных, которая предусматривает:
- проведение сравнительного анализа и расхождений содержания заголовков файлов данных (file header), расширений и структур файлов данных;
- анализ структуры и содержания зашифрованных файлов данных, файлов данных, защищенных паролями, в том числе архивов, файлов данных, содержимое которых сформированно с использованием методов “стеганографии”;
- анализ информации из скрытых областей накопителей на жестких магнитных дисках (host-protected area HPA):
- анализ внедренных объектов в файлы данных (например, в файлы документов);
- анализ возможного размещения файлов данных в нестандартных местах файловой системы.

Стратегия сравнительного (корреляционного) анализа файлов данных и приложений, которая предусматривает:
- сопоставление состава файлов данных с установленными приложениями;
- сравнительный анализ состава и целостности исполняемых файлов данных на основе вычисления значений хэш-функций и эталонных значений;
- анализ возможной связи между файлами данных и (или) приложениями, например, соотнесение:
  - данных журналов (протоколов) использования сети Интернет с кеш-файлами:
  - файлов данных и файлов, содержащихся во вложении электронных почтовых сообщений;
- идентификация неизвестных типов файлов данных.

7.20. С целью идентификации субъектов, реализующих угрозы ИБ, аналитику может быть рекомендовано:
- определение владельца и места регистрации IP/DNS-адреса, с которого зафиксирована реализация угрозы ИБ или который был использован для реализации угрозы ИБ;
- проведение анализа атрибутов подозрительных или вредоносных файлов данных;
- проведение анализа временных параметров реализации угрозы ИБ (в том числе время наибольшей активности);
- проведение анализа временных параметров создания вредоносного кода и его отдельных компонентов;
- проведение анализа программного кода, использованного для реализации угрозы ИБ (например, вредоносного кода в файле данных, вредоносного скрипта, содержания “тела” почтового сообщения);
- проведение лингвистического (стилометрического) анализа текстов, сопровождающих реализацию угрозы ИБ (например, требование выкупа или шантажа);
- проведение анализа (пути) до потенциального нарушителя на следующих уровнях модели взаимодействия открытых систем, определенной в ГОСТ 28906-91:
  - сетевом (трассировка или traceback);
  - прикладном (например, путем анализа заголовков почтовых сообщений);
  - уровне маршрутизации (путем анализа таблиц маршрутизации);
- проведение анализа получателей несанкционированных переводов денежных средств или денежных средств, в отношении которых совершено покушение на хищение.

При проведении идентификации субъектов, реализующих угрозы ИБ, аналитик должен учитывать наличие следующих особенностей:
- потенциальная возможность использования для реализации угроз ИБ промежуточных узлов (прокси-серверов или abuse-устойчивый хостинг), которые могут находиться в различных юрисдикциях;
- потенциальная возможность целенаправленного изменения нарушителями ИБ служебных заголовков в трафике на сетевом или прикладном уровне (например, в сообщениях почтовых серверов или сервисов) для цели сокрытия нарушителями своего реального местоположения;
- отсутствие в большинстве современных сетевых и прикладных протоколов способов достоверного определения источника отправления данных;
- отсутствие реализации проверки идентификационных данных при регистрации IP/DNS-адресов;
- использование подставных лиц для выполнения отдельных операций в рамках реализации угрозы (например, в качестве получателей переводов денежных средств).

7.21. Для обеспечения возможности проведения выделения и анализа содержательной (семантической) информации организации БС РФ рекомендуется обеспечить в распоряжении аналитика следующих технических средств и инструментов:
- технические средства и инструменты анализа данных файловых систем, позволяющие:
  - проводить поиск, выделение и анализ содержательной (семантической) информации в составе подозрительных файлов данных, удаленных файлов данных, скрытых директориях файловых систем,

в неиспользуемых областях в пределах логических модулей выделения файлового пространства (file slack space), в неиспользуемом пространстве файловой системы (free space);
- устанавливать типы обрабатываемых файлов данных по содержанию заголовков файлов данных (file header) и их структуре;
- просматривать содержимое файлов данных разных форматов;
- осуществлять извлечение файлов данных из архивов;
- просматривать структуру директорий файловой системы, в том числе в графическом виде;
- проводить контроль состава и целостности исполняемых файлов данных на основе вычисления значений хэш-функций и эталонных значений, содержащихся в соответствующих справочниках, в том числе разрабатываемых организацией БС РФ. В качестве справочных данных организацией БС РФ может использоваться информация о вычисленных эталонных значениях хэш-функций, размещенная в справочнике NIST's National Software Reference Library (NSRL) [2];
- осуществлять полнотекстовый поиск по "ключевым словам" и поиск по "шаблонам" в содержимом файлов данных;
- осуществлять поиск и анализ информации в атрибутах файлов данных;

– технические средства и инструменты анализа данных оперативной памяти СВТ, позволяющие:
- просматривать содержимое, осуществлять поиск на основе текстовых и цифровых "шаблонов", ключевых слов и проводить анализ больших массивов неструктурированной информации (hex editors);

– технические средства и инструменты анализа данных протоколов (журналов) сетевого оборудования и данных сетевого трафика, позволяющие:
- осуществлять централизованный сбор, хранение и анализ данных протоколов (журналов) сетевого оборудования;
- осуществлять реконструкцию действий и событий для отдельных сессий сетевого взаимодействия и (или) всех сессий сетевого взаимодействия за определенный временной период;
- осуществлять визуализацию сетевого взаимодействия между СВТ (хостами) и иными элементами информационной инфраструктуры целевых систем;
- осуществлять построение шаблонов и профилей "типовой" сетевой активности и выявлять существенные отклонения сетевой активности от построенных шаблонов и профилей;
- осуществлять поиск в данных сетевого трафика на основе текстовых и цифровых "шаблонов", ключевых слов, аномалий.

Рекомендации по составу технических средств выделения из технических данных содержательной (семантической) информации и ее анализа приведены в приложении В к настоящему стандарту.

7.22. При проведении выделения и анализа содержательной (семантической) информации аналитик должен учитывать наличие следующих возможных технических ограничений:
– хранение содержимого файлов данных в зашифрованном виде;
– парольная защита архивов файлов данных;
– сокрытие файлов содержимого файлов данных с использованием методов "стеганографии" и "обфускации";
– использование вредоносного кода в содержимом архивных файлов, реализующего атаку типа "бомба разархивирования", предполагающую выполнение множественной повторяющейся операции разархивирования;
– использование вредоносного кода, реализующего выполнение множественной повторяющейся операции записи посторонних данных (шума) в оперативную память;
– использование вредоносного кода, обнаруживающего факт его анализа и пытающегося реализовать деструктивное воздействие на СВТ по факту своего обнаружения (например, перезаписать или уничтожить MBR-запись или зашифровать системные файлы на жестком магнитном диске);
– использование уникальных проприетарных форматов файлов данных;
– отсутствие должной синхронизации системного времени объектов информационной инфраструктуры – источников технических данных;
– использование накопителей на жестких магнитных дисках совместно с флеш-памятью, на которой сохранен пароль, необходимый для осуществления доступа к данным накопителя, в том числе в случаях, когда накопитель был извлечен из СВТ;
– шифрование или маскирование сетевого трафика;
– использование нетиповых номеров портов (ports) в рамках сетевого взаимодействия;
– сокрытие злоумышленником IP-адресов (spoofed IP addresses);
– регулярная смена злоумышленником IP/DNS-адресов;
– использование специальных алгоритмов генерации доменных имен;

– использование промежуточных узлов (в том числе нетипичных, например, принтеров), осложняющих идентификацию субъектов, реализующих угрозы ИБ. При этом необходимо учитывать, что угроза может быть реализована через узлы-посредники, владельцы которых не связаны с реализацией угрозы ИБ;
– сокрытие (инкапсуляция) вредоносной активности в разрешенных протоколах информационного взаимодействия (например, в DNS или HTTP/HTTPS).

7.23. Результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации должны быть документированы. Организации БС РФ рекомендуется формализовать правила документирования результатов выделения и анализа содержательной (семантической) информации. В правилах рекомендуется определить необходимость документирования:
– описания инцидента ИБ и его классификацию, выполненную с учетом содержания пункта 6.1 настоящего стандарта;
– описания состава собранных (используемых) технических данных;
– описания цели проведенного анализа собранных технических данных из числа определенных в пункте 7.1 настоящего стандарта;
– описания собранной первичной содержательной (семантической) информации, потенциально связанной с исходными (базовыми) событиями ИБ или их группой;
– описания использованных технических средств и инструментов, выполненных процедур и сервисных команд, связанных с обработкой технических данных. При этом описание должно обеспечивать возможность повторного выполнения указанных процедур и сервисных команд с исходными техническими данными;
– даты и времени выполнения процедур и сервисных команд по выделению и анализу содержательной (семантической) информации;
– содержания выделенной семантической информации;
– результатов анализа с максимально возможно подробным описанием:
  • технических способов и схем реализаций угроз ИБ;
  • результатов идентификации субъектов, реализующих угрозы ИБ;
  • результатов выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры;
– рекомендаций по сбору дополнительных технических данных с объектов информационной инфраструктуры, не принадлежащей организации БС РФ, например, протоколов (журналов) регистрации провайдеров сети Интернет или мобильных операторов связи;
– описания возможных вариантов интерпретации результатов анализа в случае отсутствия у аналитика однозначного вывода относительно инцидента ИБ;
– подробных выводов и рекомендаций, направленных на:
  • совершенствование обеспечения ИБ организации БС РФ;
  • устранение последствий инцидентов ИБ;
  • устранение выявленных уязвимостей ИБ;
  • инициирование взаимодействия с правоохранительными органами и (или) FinCert Банка России, а также иными организациями, проводящими мероприятия по реагированию на инциденты ИБ.

7.24. При определении содержания и детализации документов, содержащих результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации, организации БС РФ рекомендуется учитывать состав целевых получателей информации. Организации БС РФ рекомендуется рассматривать следующих потенциальных целевых получателей информации:
– руководство организации БС РФ, которому целесообразно обеспечить предоставление сводных аналитических отчетов обо всех выявленных инцидентах ИБ без указания детальных технических данных;
– технические подразделения организации БС РФ, служба ИБ, правоохранительные органы, FinCert Банка России, которым целесообразно обеспечить предоставление максимально подробных отчетов, содержащих подробное описание технических аспектов, связанных с инцидентом ИБ;
– подразделения по связям с общественностью или подразделения по работе с клиентами организации БС РФ, которым целесообразно обеспечить предоставление сводной информации без указания детальных технических данных, но направленной на повышение осведомленности в части возможных причин инцидента ИБ, которые могут быть интересны средствам массовой информации или клиентам организации БС РФ.

8. Рекомендации к распространению (передаче) выделенной и оформленной содержательной (семантической) информации

8.1. С целью получения методической и практической помощи в рамках выполнения процедур реагирования на инциденты ИБ организации БС РФ рекомендуется:

– обратиться в МВД России либо его территориальное подразделение с заявлением об оказании содействия в реализации процедур реагирования на инцидент ИБ. Для подачи заявления в МВД России следует подготовить пакет следующих документов:
  - заявление в свободной форме, к которому прилагается обзорная информация об инциденте ИБ – профиль инцидента ИБ, сформированный в соответствии с пунктом 6.1 настоящего стандарта. Заявление юридического лица пишется руководителем или уполномоченным лицом, действующим на основании соответствующей доверенности;
  - выписка по расчетному или лицевому счету, подвергшемуся фактическому несанкционированному списанию денежных средств;
  - для юридического лица – комплект правоустанавливающих документов юридического лица;
– обратиться в FinCert Банка России (контактные данные указаны на официальном сайте Банка России).

8.2. Организации БС РФ следует обеспечить возможность предоставления по запросам МВД России и (или) FinCert Банка России:

– документов, содержащих результаты выполнения аналитиком процедур и сервисных команд по выделению и анализу содержательной (семантической) информации, сформированных в соответствии с положениями пункта 7.13 настоящего стандарта;
– эталонных копий собранных исходных технических данных, сформированных в соответствии с положениями раздела 6 настоящего стандарта.

8.3. Организации БС РФ рекомендуется использование сервисов FinCert Банка России с целью:

– получения актуальной аналитической информации технического характера о выявленных в БС РФ инцидентах ИБ;
– использования полученной аналитической информации для цели своевременного выявления маркеров “скрытого” несанкционированного управления объектами информационной инфраструктуры в рамках процедур анализа содержательной (семантической) информации, проводимых в соответствии с положениями раздела 7 настоящего стандарта.

9. Рекомендации по распределению зон ответственности подразделений организации БС РФ в рамках процесса обработки технических данных

9.1. В рамках реализации процессов обработки технических данных рекомендуется участие следующих подразделений организации БС РФ:

– подразделение информатизации в части:
  - обеспечения наличия технических данных путем должной настройки объектов информационной инфраструктуры для ведения протоколов (журналов) регистрации;
  - обеспечения хранения протоколов (журналов) регистрации в течение как минимум трех лет;
  - обеспечения необходимых технических средств для сбора и обработки технических данных;
  - участия при необходимости в сборе технических данных;
  - участия при необходимости в выделении и анализе содержательной (семантической) информации;
  - предоставления содействия и информации, необходимых для проведения полноценного сбора технических данных, выделения и анализа содержательной (семантической) информации;
– служба ИБ в части:
  - организации и проведения сбора технических данных;
  - организации и проведения выделения и анализа содержательной (семантической) информации;
  - разработки планов (регламентов) сбора технических данных, реализуемого в случае выявления инцидентов ИБ;
  - формирования предложений по привлечению сторонних специалистов, а также по взаимодействию с правоохранительными органами, обращению в МВД России, FinCert Банка России;
  - обеспечения и координации взаимодействия с правоохранительными органами и FinCert Банка России;
  - обеспечения взаимодействия с клиентами организации БС РФ для получения технических данных, собранных клиентами;
  - контроля обеспечения наличия технических данных;

– юридическая служба – в части привлечения представителей, которых целесообразно обеспечить при документировании результатов выделения и анализа содержательной (семантической) информации, предполагаемых к передаче в правоохранительные органы;
– подразделение, ответственное за операционную деятельность, обслуживание банковских карт – в части участия при необходимости в анализе содержательной (семантической) информации при выявлении инцидентов ИБ, связанных с переводами денежных средств, а также принятии решений о возможности отключения и (или) выведения из штатного режима объектов информационной инфраструктуры целевых систем;
– подразделение внутренней (физической) безопасности – в части сопровождения при необходимости работников организации БС РФ при сборе технических данных с информационной инфраструктуры клиентов;
– подразделение по связям с общественностью – в части обеспечения взаимодействия со средствами массовой информации.

9.2. Ответственных за выполнение ролей в рамках реализации процессов обработки технических данных рекомендуется включать в группу реагирования на инциденты ИБ, создаваемую в соответствии с РС БР ИББС-2.5.

9.3. Организации БС РФ рекомендуется выделение и назначение работникам службы ИБ отдельной функциональной роли (или выделение отдельного функционального подразделения), связанной с выполнением функций, определенных в пункте 9.1 настоящего раздела.

10. Рекомендации по взаимодействию с клиентами организации БС РФ в рамках процесса обработки технических данных

10.1. В случаях, когда в результате реализации инцидента ИБ пострадали клиенты – физические лица, организации БС РФ не рекомендуется определять для них существенный объем выполняемых процедур, связанных с обработкой технических данных.

10.2. Рекомендуемым решением является доведение до клиента – физического лица плана (регламента) действий, содержащего:
– условия возникновения необходимости выполнения плана (регламента), в том числе:
  • спам-рассылки, реализуемые в рамках реализации методов “социального инжиниринга”;
  • деструктивное воздействие компьютерных вирусов;
  • обнаружение сайтов-двойников организации БС РФ (“фишинговых” сайтов) в информационно-телекоммуникационной сети Интернет;
  • несанкционированный перевод денежных средств;
– описание следующего порядка действий:
  • фиксация и описание СВТ (настольные компьютеры, ноутбуки), используемого клиентом для осуществления доступа к системам ДБО, осуществляемые с учетом содержания пункта 6.6 настоящего стандарта;
  • отключение СВТ, используемого клиентом для осуществления доступа к системам ДБО, путем прерывания питания[1] с последующим возможным извлечением запоминающих устройств;
  • передачей запоминающего устройства в адрес организации БС РФ с обеспечением их безопасной упаковки, хранения и транспортировки, осуществляемых с учетом содержания пункта 6.7 настоящего стандарта.

10.3. Сбор технических данных с объектов информационной инфраструктуры клиентов юридических лиц может осуществляться самостоятельно клиентами организации БС РФ. В этом случае организации БС РФ рекомендуется разработать детальный план (регламент) действий клиентов – юридических лиц по сбору и передаче организации БС РФ технических данных и обеспечить возможность доступа клиентов к содержанию указанного плана.

Выделение из технических данных, собранных клиентами, семантической (содержательной) информации и ее анализ рекомендуется выполнять организации БС РФ.

[1] Прерывание питания осуществляется с учетом описанных в разделе 6 особенностей данной операции.

10.4. Выполнение клиентами – юридическими лицами сбора технических данных должно обеспечивать:
- реализацию принципов обработки технических данных, определенных в пункте 5.2 настоящего стандарта;
- реализацию рекомендаций по сбору технических данных, определенных в разделе 6 настоящего стандарта, в части сбора технических данных с информационной инфраструктуры клиентов.

В плане (регламенте) действий клиентов – юридических лиц по сбору и передаче организации БС РФ технических данных рекомендуется включать:
- перечень собираемых технических данных;
- приоритеты (последовательность) сбора технических данных;
- описание правил документирования выполненных процедур и сервисных команд при сборе технических данных;
- описание правил документирования места сбора технических данных;
- детальные инструкции по использованию технических средств, описание процедур и сервисных команд, необходимых для сбора технических данных;
- описание процедур и сервисных команд, в том числе технических, проверки (контроля) целостности собранных данных;
- требования к количеству создаваемых копий собираемых технических данных;
- описание правил маркирования безопасной упаковки, хранения и передачи в адрес организации БС РФ носителей собранных технических данных.

10.5. Для всех категорий клиентов организации БС РФ рекомендуется регламентировать и обеспечить возможность применения:
- формы обращения клиента с целью передачи носителей собранных технических данных;
- правил и формы актирования факта передачи носителей собранных технических данных;
- контактной информации для возможной передачи носителей собранных технических данных;
- требований к составу передаваемой документации совместно с носителями технических данных;
- условий принятия организацией БС РФ собранных технических данных.

10.6. Сбор технических данных с информационной инфраструктуры клиентов работниками организации БС РФ следует осуществлять только при наличии уверенности организации БС РФ в их безопасности.

11. Рекомендации к компетенции персонала организации БС РФ и (или) иных внешних организаций, задействованных в процессах обработки технических данных

11.1. Организации БС РФ рекомендуется обеспечить наличие должной компетенции работников и (или) привлеченных специалистов для выполнения деятельности по сбору технических данных, поиску (выделению) содержательной (семантической) информации и анализу. Работники организации БС РФ, задействованные в сборе и обработке технических данных, должны:
- получить необходимые знания своих функций, прав и обязанностей, связанных со сбором и обработкой технических данных в рамках реагирования на инциденты ИБ;
- получить необходимые технические знания в части:
  - возможного состава собираемых технических данных;
  - условий возникновения необходимости сбора технических данных;
  - возможного состава объектов информационной инфраструктуры организации БС РФ, являющихся объектами сбора технических данных;
  - реализации технологических и технических процедур обработки технических данных в рамках реагирования на инциденты ИБ, использования необходимых технических средств и инструментов;
  - установленных ограничений на выполнение отдельных процедур и сервисных команд, способных повредить и (или) уничтожить собираемые технические данные;
- получить необходимые знания в части состава и содержания принципов и процедур сбора и обработки технических данных, направленных на обеспечение относимости собранных и обрабатываемых технических данных к конкретному инциденту ИБ;
- получить необходимые знания в части состава и содержания принципов и процедур сбора и обработки технических данных, направленных на обеспечение сохранности (нераспространение) информации, защищаемой в соответствии с требованиями законодательства РФ, в том числе содержащей банковскую тайну и персональные данные.

Отдельное внимание организации БС РФ должно быть уделено вопросам регламентации и доведения до соответствующих работников организации БС РФ правил сбора технических данных с объектов информационной инфраструктуры, критичных для обеспечения непрерывности деятельности организации БС РФ, в том числе условиям возможного отключения и (или) выведения из штатного режима функционирования указанных объектов.

11.2. Организации БС РФ рекомендуется обеспечить наличие следующих знаний и компетенции аналитиков, выполняющих поиск (выделение) и анализ содержательной (семантической) информации:

– глубокое знание и понимание способов организации хранения технических данных в файловых системах для разных типов носителей информации (разделение на логические тома, логическое форматирование файловых систем, способов организации хранения файлов и директорий), которые потенциально могут быть источниками значимой (семантической) информации. К таким носителям информации могут быть отнесены:
  - накопители на жестких магнитных дисках;
  - накопители на гибких магнитных дисках (флоппи-диски);
  - носители информации портативных компьютеров (планшетов), мобильных телефонов;
  - CD-диски, DVD-диски;
  - флеш-карты;
  - оптические накопители;
  - карты памяти (в том числе SD, PC Card, CF, MMC, Memory Stick).

  Для получения дополнительной информации о составе возможных носителей информации и соответствующих файловых системах возможно использование рекомендаций, определенных в разделах 4.1.1 “File Storage Media” и 4.1.2 “FileSystems” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3];
– глубокое знание и понимание способов организации хранения как минимум в следующих файловых системах:
  - операционные системы Windows и их файловые системы: FAT16, FAT32, NTFS;
  - операционные системы Unix, Linux и их файловые системы: Unix File System (UFS), Second Extended Filesystem (ext2fs), Third Extended Filesystem (ext3fs), ReiserFS;
  - операционная система MacOs и ее файловая система: Hierarchical File System (HFS), HFS Plus;
  - CD-диски: Compact Disc File System (CDFS), ISO 9660, Joliet;
  - DVD-диски: Universal Disc Format (UDF);
– глубокое понимание сетевых протоколов передачи данных TCP/IP и принципов их инкапсуляции:
  - протоколов прикладного уровня, в том числе протоколов DNS, FTP, HTTP, SMTP, POP3, IMAP, SNMP;
  - протоколов транспортного уровня, в том числе протоколов TCP, UDP, ICMP;
  - протоколов сетевого уровня, в том числе протоколов IPv4, IPv6, IPSec;
  - протоколов маршрутизации, в том числе протоколов RIP, OSPF, BGP;
  - протоколов канального и физического уровня, в том числе протокола Ethernet и семейства протоколов 802.11;
  - знание и понимание угроз ИБ, связанных с использованием вычислительных сетей, способов и техник реализации сетевых атак;
– знание и понимание организации вычислительных сетей (сетевой топологии) организации БС РФ, в том числе знание и понимание:
  - сетевой архитектуры организации БС РФ;
  - используемого организацией БС РФ сетевого и телекоммуникационного оборудования;
  - IP-адресов ключевых (критических) программных сервисов, в первую очередь используемых для осуществления переводов денежных средств;
  - номера используемых сетевых портов (ports) ключевых (критических) программных сервисов, в первую очередь используемых для осуществления переводов денежных средств;
– глубокое знание и понимание возможного содержания данных операционных систем, эксплуатируемых в пределах информационной инфраструктуры организации БС РФ:
  - порядка загрузки операционных систем Windows, Linux и мобильных операционных систем;
  - состава и возможного содержания конфигурационных файлов данных операционных систем;
  - состава и возможного содержания протоколов (журналов) регистрации операционных систем;
  - структуры и информации реестра операционной системы Windows;
  - состава и возможного содержания информации, содержащейся в неиспользуемых областях в пределах логических страниц или блоков выделения пространства оперативной памяти (memory slack space);

- состав и возможное содержание информации, расположенной в неиспользуемом пространстве оперативной памяти (memory free space, garbage);
- состав и возможное содержание информации о сетевых конфигурациях, сетевых соединениях, запущенных программных процессах, открытых сессиях доступа;

– знание и понимание организации и правил эксплуатации информационной инфраструктуры организации БС РФ:
  - состава СВТ и серверного оборудования;
  - состава, правил размещения, возможного содержания протоколов (журналов) регистрации операционных систем, системного программного обеспечения, СУБД, почтовых серверов, web-серверов;
  - состава, правил размещения, возможного содержания протоколов (журналов) регистрации средств защиты информации;
  - состава, правил размещения, возможного содержания протоколов (журналов) регистрации программного обеспечения целевых систем.

11.3. Организации БС РФ как минимум следует обеспечить наличие должной компетенции работников и (или) привлеченных специалистов для выполнения деятельности по обеспечению наличия, хранения и сбора технических данных. В случае существенных инцидентов ИБ и отсутствия должной компетенции работников организации БС РФ к проведению необходимого выделения и анализа содержательной (семантической) информации организации БС РФ может быть рекомендовано обращение в FinCert Банка России. Соответствующий запрос с описанием инцидента ИБ – профиля инцидента ИБ, сформированного в соответствии с пунктом 6.1 настоящего стандарта, следует направить на электронный адрес fincert@cbr.ru.

12. Рекомендации по обеспечению наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры

12.1. Для обеспечения наличия и сохранности технических данных для цели реагирования на инциденты ИБ организации БС РФ рекомендуется:

– установить ограничения и организовать контроль использования административных учетных записей для объектов информационной инфраструктуры, являющихся источниками технических данных;
– установить ограничения на совмещение одним лицом полномочий по использованию административных учетных записей разных объектов информационной инфраструктуры, являющихся источниками технических данных, в том числе установить ограничения на выполнение одним лицом функций администратора операционных систем, СУБД, целевых систем;
– принятие мер по мониторингу сообщений о выявленных уязвимостях объектов информационной инфраструктуры, являющихся источниками технических данных, и по реагированию на них в соответствии с РС БР ИББС-2.6, направленных на обеспечение невозможности использования уязвимостей для несанкционированного отключения протоколирования и повреждения технических данных, сокрытия нарушителем своих действий;
– принятие мер по контролю фактического состава технических средств и систем – источников технических данных путем применения средств инвентаризации и оценки защищенности целевых систем;
– протоколирование всех действий с данными протоколов (журналов) регистрации, в том числе действий по отключению ведения и (или) очистке протоколов (журналов);
– принятие организационных мер по ограничению использования “непротоколируемых” административных учетных записей, например, путем разделения административного пароля на две части для цели реализации принципа “двойного контроля”;
– обеспечение постоянного формирования и контроля формирования технических данных – протоколов (журналов) регистрации, являющихся потенциальной содержательной (семантической) информацией, состав которой определен в пунктах 7.10–7.17 настоящего стандарта. Обеспечение ведения протоколов (журналов) регистрации реализуется путем соответствующего выбора, настройки и (или) создания следующих источников технических данных:
  - операционные системы;
  - целевые системы;
  - средства (системы) аутентификации, авторизации и разграничения доступа;
  - средства антивирусной защиты информационной инфраструктуры;
  - средства криптографической защиты информации;
  - средства защиты от несанкционированного доступа;
  - маршрутизаторы и средства межсетевого экранирования, в том числе средства межсетевого экранирования прикладного уровня;

- DHCP- и DNS-сервисы;
- средства обнаружения вторжений и сетевых атак в информационную инфраструктуру;
- средства, используемые для предоставления удаленного доступа (VPN-шлюзы);
- почтовые серверы и средства контентной фильтрации электронной почты;
- web-серверы и средства контентной фильтрации web-протоколов;
- СУБД;

– обеспечить периодическое тестирование ведения протоколов (журналов) регистрации, например, путем периодического проведения тестирования на проникновение с имитацией возможных действий нарушителя по реализации инцидентов ИБ;
– обеспечивать адаптацию содержания протоколов (журналов) регистрации, состава источников технических данных, формирующих протоколы (журналы) регистрации, с учетом появления новых инцидентов ИБ, опыта организации БС РФ по реагированию на них.

12.2. Организации БС РФ рекомендуется учитывать, что разные технические средства и системы – источники технических данных могут формировать разный состав сведений об одном и том же инциденте ИБ. К примеру, целевая система может регистрировать факт выполнения несанкционированной операции, но не идентифицировать источник сообщения, инициировавшего операцию, на сетевом уровне взаимодействия. Средства защиты сетевого уровня могут регистрировать факт поступления сообщения и его источник, но не регистрировать операцию, инициированную сообщением. Таким образом, рекомендуется обеспечивать формирование, сбор и сопоставление всех возможных технических данных об инциденте ИБ с максимально возможной избыточностью.

12.3. Организации БС РФ рекомендуется обеспечить применение для всех целевых систем унифицированного состава технических средств и систем – источников технических данных, а также реализовать систему централизованного сбора и хранения протоколов (журналов) регистрации (например, SIEM систему).

При реализации системы централизованного сбора и хранения протоколов (журналов) регистрации рекомендуется обеспечить:

– централизованный сбор и хранение технических данных протоколов (журналов) регистрации, формируемых источниками технических данных, указанных в пункте 12.1 настоящего стандарта;
– реализация сбора технических данных путем комбинации следующих способов:
  - путем периодического автоматического копирования протоколов (журналов) регистрации;
  - путем получения данных, передаваемых с помощью протоколов аудита и диагностики (в том числе SYSLOG, SNMP);
  - путем периодического сбора данных о фактическом составе технических средств и систем – источников технических данных путем использования средств инвентаризации и оценки защищенности, протоколов удаленного администрирования (системного сканирования);
  - путем копирования сетевого трафика;
– контроль работоспособности технических средств, применяемых для сбора протоколов (журналов) регистрации;
– хранение собранных технических данных, в том числе архивное хранение, обеспечивающее:
  - контроль и протоколирование доступа к собранным техническим данным;
  - реализация защитных мер, направленных на обеспечение конфиденциальности, целостности и доступности собранных технических данных;
  - обеспечение запрета единоличного изменения и (или) удаления собранных технических данных;
  - возможность установления сроков оперативного хранения технических данных;
  - архивное хранение по истечении срока оперативного хранения, реализуемое при необходимости внешними системами архивного хранения;
  - возможность доступа к архивным данным о событиях информационной безопасности для цели анализа в течение трех лет;
– реализацию защиты собранных технических данных от несанкционированного доступа, двустороннюю аутентификацию при использовании общедоступных вычислительных сетей, в том числе информационно-телекоммуникационной сети Интернет, для цели передачи указанных данных;
– гарантированную доставку данных о событиях информационной безопасности;
– приведение однотипных технических данных, формируемых разными источниками технических данных, к унифицированному формату;
– возможность объединения и корреляции технических данных, сформированных разными источниками технических данных, в пределах одного общего инцидента ИБ;

– приведение (синхронизация) временных меток записей электронных журналов событий ИБ к единому часовому поясу и единому эталонному времени, для чего рекомендуется:
  - использование в качестве основного сигнала точного времени спутниковой системы “ГЛОНАСС”[1];
  - использование в информационной инфраструктуре специального оборудования, содержащего в своем составе приемники сигналов спутниковой системы “ГЛОНАСС” – сервер времени информационной инфраструктуры (Time Server);
  - осуществление синхронизации системного времени технических средств, являющихся источниками технических данных, с сервером времени информационной инфраструктуры с одновременным документированием выполнения этой операции;
  - осуществление синхронизации системного времени видеорегистраторов, установленных в корпусах технических средств, являющихся источниками технических данных, систем видеонаблюдения и систем контроля доступа, с одновременным документированием выполнения этой операции.

[1] Допустимо использование интернет-сервисов точного времени, погрешность которых должна быть достаточной для целей выявления и анализа событий ИБ.

Приложение А
(справочное)

Структура протокола обработки технических данных

1. **Дата и время начала выполнения процедур обработки технических данных**:
   [дд.мм.гггг], [чч.мм];

2. **Место проведения процедур обработки технических данных**:
   [Полное наименование организации БС РФ];
   [Полный адрес места выполнения процедур];

3. **Идентификационные данные лиц, выполнивших процедуры обработки технических данных:**
   [Полное наименование организации, работники которой выполнили процедуры];
   [Фамилия, имя, отчество работников];
   [Должности работников];

4. **Описание каждой выполненной процедуры и (или) сервисной команды:**
   [Цель выполнения процедуры и (или) сервисной команды];
   [Идентификаторы запоминающих устройств исходных технических данных];
   [Идентификаторы запоминающих устройств полученных технических данных или содержательной (семантической) информации];
   [Полное название организации – владельца запоминающего устройства полученных технических данных или содержательной (семантической) информации];
   [Точное описание выполненных сервисных команд];
   [Идентификаторы использованных технических средств];
   [Результаты выполнения процедур контроля целостности (неизменности) технических данных, в том числе значения вычисления хэш-функций];

5. **Дата и время окончания выполнения процедур обработки технических данных:**
   [дд.мм.гггг], [чч.мм];

6. **Описание мер, принятых для обеспечение безопасной упаковки и хранения собранных данных:**
   [Точное описание выполненных мер для обеспечения безопасной упаковки и хранения];
   [Идентификация и описание мест, использованных для хранения запоминающих устройств исходных и полученных технических данных или содержательной (семантической) информации];

7. **Подписи лиц, выполнивших процедуры обработки технических данных.**

Приложение Б
(справочное)

Пример протокола выполнения криминалистической копии (создания образа) накопителя на жестких магнитных дисках

г. [Город]

[Дата начала копирования] в *[Время начала копирования]*, работниками *[Наименование организации] [Фамилия, имя, отчество работников]* в офисе организации *[Наименование организации]* расположенном по адресу: *[Полный адрес]*, был начат процесс снятия аутентичной посекторной копии накопителя на жестких магнитных дисках (НЖМД), производитель _____, модель _____, серийный номер _____.

Снятие посекторной копии производилось в режиме _____ с использованием устройства дупликации носителей информации _____, обеспечивающего защиту от изменений оригинала.

Аутентичная копия диска-источника была сохранена на НЖМД, производитель _____, модель _____, серийный номер _____, принадлежащий *[Наименование организации]*. Все секторы были предварительно очищены.

Значение хэш-функций, посчитанных на основе данных диска-оригинала и криминалистической копии: _____.

1. Диск-источник

(производитель _____, модель _____, серийный номер _____)
SHA256: _____
MD5: _____

2. Аутентичная посекторная копия

(производитель _____, модель _____, серийный номер _____)
SHA256: _____
MD5: _____

Диск-источник НЖМД, производитель _____, модель _____, серийный номер _____, после снятия с него образа (точной копии) был помещен в антистатический пакет и опечатан бумажной биркой с подписями от имени _____ и оттиском печати *[Наименование организации]* способом, предотвращающим его использование без нарушения целостности упаковки.

Опечатанный диск-источник НЖМД, производитель _____, модель _____, серийный номер _____ передан в *[Наименование организации]*.

НЖМД, производитель _____, модель _____, серийный номер _____, содержащий образ (точную копию) диска-источника, был помещен в антистатический пакет и опечатан бумажной биркой с подписями от имени _____ и оттиском печати *[Наименование организации]* способом, предотвращающим его использование без нарушения целостности упаковки.

Опечатанный НЖМД, производитель _____, модель _____, серийный номер _____, образ (точная копия) диска-источника, был предоставлен в лабораторию компьютерных экспертиз *[Наименование организации]* для исследования.

_____
_____

[Подписи присутствующих]

[Дата]

Приложение В
(справочное)

Примеры технических средств сбора и обработки технических данных, имеющих отдельные функциональные возможности

1. Примеры технических средств выполнения криминалистической копии (создания образа) запоминающих устройств.

В качестве программных средств выполнения криминалистической копии (создания образа) возможно использовать:

- программы (утилиты) **dd** и **dc3dd** для UNIX-систем;
- программы **FTK Imager, EnCase Forensic Imager** или **Redline** для Windows-систем;
- программу **Belkasoft Evidence Center** для Windows, Linux, MacOS, iOS, Android, Windows Phone, Blackberry-систем;
- программу **The Sleuth Kit** для Windows, MacOS, Linux, Solaris, OpenBSD, FreeBSD-систем;
- рекомендации, определенные в разделе 4.2.1 “Copying File from Media” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3];
- программные средства, описанные в разделе “Копирование содержимого энергонезависимых носителей информации” Инструкции по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания ООО “Группа информационной безопасности” (GROUP-IB) [4].

В качестве программных средств вычисления значений хэш-функций возможно использовать:

- программы **md5sum** или **sha256sum** для Linux-систем;
- программы **Memoryze** для Windows и MacOS-систем;
- программу **dff** для Windows и Linux-систем.

В качестве специализированных программных средств – “write-blocker” – возможно использовать:

- программу **dff** для Windows и Linux-систем;
- рекомендации, определенные в разделе 4.2.2 “Data File Integrity” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

2. Примеры технических средств выполнения копирования содержимого оперативной памяти СВТ и получения данных операционных систем.

В качестве технических средств выполнения копирования содержимого оперативной памяти СВТ возможно использовать:

- программы **FTK Imager, Redline, MoonSols Windows Memory Toolkit** и **Memoryze** для Windows-систем;
- программу **Belkasoft Evidence Center** для Windows, Linux, MacOS, iOS, Android, Windows Phone, Blackberry-систем;
- программу **Memoryze** для MacOS-систем;
- программу **dff** для Windows и Linux-систем;
- программные средства, описанные в разделе “Копирование энергозависимых данных, лог-файлов сетевого оборудования и сетевого трафика” Инструкции по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания ООО “Группа информационной безопасности” (GROUP-IB) [4].

В качестве технических средств получения данных операционных систем о сетевых конфигурациях возможно использовать:

- команды **ifconfig** и **arp** для UNIX и MacOS-систем;
- команду **ipconfig, netstat, arp** и **route** для Windows-систем;
- набор утилит **Sysinternals** для Windows-систем;
- программы **Rekall Memory Forensic Framework** и **Volatility Framework** для Windows, MacOS, Linux-систем;
- рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

В качестве технических средств получения данных операционных систем о сетевых соединениях возможно использовать:

- программу **netstat** для UNIX, Windows и MacOS-систем;
- команды **nbstat** и **net** для Windows-систем;
- набор утилит **Sysinternals** для Windows-систем;
- программы **Rekall Memory Forensic Framework** и **Volatility Framework** для Windows, MacOS, Linux-систем;

– рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

В качестве технических средств получения данных операционных систем о запущенных процессах возможно использовать:

– команды **ps, top** и **w** для UNIX и MacOS-систем;
– программу (утилиту) **Task Manager**, программу **Memoryze** и набор утилит **Sysinternals** для Windows систем;
– программу **Memoryze** для MacOS-систем;
– программы **Rekall Memory Forensic Framework** и **Volatility Framework** для Windows, MacOS, Linux-систем;
– программу **dff** для Windows и Linux-систем;
– рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

В качестве технических средств получения данных операционных систем об открытых файлах возможно использовать:

– команду **lsof** для UNIX и MacOS систем;
– программы **Rekall Memory Forensic Framework** и **Volatility Framework** для Windows, MacOS, Linux-систем;
– набор утилит **Sysinternals** для Windows-систем;
– рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

В качестве технических средств получения данных операционных систем об открытых сессиях доступа возможно использовать:

– команду **w** для UNIX и MacOS-систем;
– команду **netstat** для Windows-систем (с параметром – anorse);
– программы **Rekall Memory Forensic Framework** и **Volatility Framework** для Windows, MacOS, Linux-систем;
– набор утилит **Sysinternals** для Windows-систем;
– рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

В качестве технических средств получения данных о зарегистрированных пользователях, времени их последней аутентификации возможно использовать:

– команды **last, who** и **w** для UNIX и MacOS-систем;
– команду **lastlog** для Linux-систем;
– команду **net** для Windows-систем;
– набор утилит **Sysinternals** для Windows-систем.

В качестве программных средств получения системных даты и времени операционной системы возможно использовать:

– команду **date** для UNIX и MacOS-систем;
– команду **date, time, nlsinfo** для Windows-систем;
– программы **Rekall Memory Forensic Framework** или **Volatility Framework** для Windows, MacOS, Linux-систем;
– набор утилит **Sysinternals** для Windows-систем;
– рекомендации, определенные в разделе 5.2.1.2 “Types of Volatile OS Data” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [3].

3. В качестве технических средств получения данных об атрибутах и структуре файлов операционной системы возможно использовать:

– команду **file** для UNIX и MacOS-систем;
– программу **Belkasoft Evidence Center** для Windows, Linux, MacOS, iOS, Android, Windows Phone, Blackberry-систем;
– программу **dff** для Windows и Linux-систем;
– программу **The Sleuth Kit** для Windows, MacOS, Linux, Solaris, OpenBSD, FreeBSD-систем;
– для анализа исполняемых файлов – программы **packerid, pescanner, exescan, PEiD, PeStudio, CFF Explorer;**
– для анализа PDF-файлов – программы **PeePDF, PDFiD, AnalyzePDF, pdfextract, pdfwalker, pyew, pdf-parser, pdf.py, pdfsh, Malzilla;**

– для анализа файлов MS Office – программы **OfficeMalScanner, Offvis, peOLEScanner;**
– для анализа графических файлов – программы **Photo Investigator, Adroit Photo Forensics, Exiftool;**

4. Для анализа протоколов (журналов) регистрации web-серверов и прокси-серверов возможно использовать программу Log Analysis Tool Kit (LATK).

5. В качестве технических средств копирования и анализа сетевого трафика возможно использовать:
– программы **tcpdump** и **Wireshark** для систем Windows или Linux;
– программы **Network Miner** и **Foremost** для Linux-систем;
– программу **Kismet** (для анализа беспроводных сетей) для Linux-систем;
– программу **ntop** (для анализа высокопроизводительных сетей) для Windows, Linux и MacOS-систем;
– программу **ssldump** (для анализа SSL/TLS-трафика);
– программу **DINO** (для визуализации сетевых соединений и геолокации IP адресов);
– технические средства, указанные в разделе 6.2.1 “Packet Sniffer and Protocol Analyzers” NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response [2];
– технические средства, описанные в разделе “Копирование энергозависимых данных, лог-файлов сетевого оборудования и сетевого трафика” Инструкции по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания ООО “Группа информационной безопасности” (GROUP-IB) [4].

6. В качестве технических средств анализа аномальных или вредоносных действий, совершаемых файлами[1], возможно использовать программу **Cockoo Sandbox**.

7. В качестве технических средств анализа сетевого и телекоммуникационного оборудования Cisco возможно использовать команду **show** (с ключами clock detail, version, running-config, startup-config, users, who, log, debug, processes, ip route, ip ospf, ip bgp, cdp neighbors, ip arp, interfaces, ip sockets, tcp brief all, ip nat translations, ip cef, snmp).

8. В качестве технических средств анализа мобильных устройств возможно использовать программы **Belkasoft Evidence Center, .XRY** для iOS, Android, Windows Phone, Blackberry-систем.

9. В качестве программных средств определения владельца IP/DNS-адреса возможно использовать:
– web-сервис **whois;**
– команду **traceroute** для Linux-систем или **tracert** для Windows-систем;
– команду **ip source-track** на маршрутизаторах Cisco определенных моделей.

10. В качестве платформы для проведения анализа собранных технических данных возможно использовать платформы **REMnux, PALADIN Forensic Suite,** которые содержат ряд программных средств, указанных в настоящем приложении, которые позволяют проводить анализ вредоносных и подозрительных файлов, создание криминалистических копий оперативной памяти, запоминающих устройств и сетевого трафика.

[1] Указанные технические средства имеют общее наименование “Песочница”.

Библиография

[1] ГОСТ Р 34.11-2012 “Информационные технологии. Криптографическая защита информации. Функция хэширования”.

[2] Офиц. сайт. URL: http://www.nsrl.nist.gov/ (дата обращения: 25.12.2015).

[3] NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response.

[4] Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания ООО “Группа информационной безопасности” (GROUP-IB). Офиц. сайт URL: http://www.group-ib.ru/brochures/Group-IB_dbo_instruction.pdf (дата обращения: 25.12.2015).

В качестве дополнительных источников информации в части сбора и анализа технических данных организации БС РФ могут использоваться следующие источники:

[5] NIST 800-150 Guide to Cyber Threat Information Sharing.

[6] NIST 800-92 Guide to Computer Security Log Management.

[7] ISO/IEC 27037:2012 Information technology –- Security techniques –- Guidelines for identification, collection, acquisition and preservation of digital evidence.

Ключевые слова: банковская система Российской Федерации, инцидент информационной безопасности.